

Вариант	42
Объект	Организация, занимающаяся торговлей бытовой химией (есть лицензия и на продажу агрессивных моющих средств)
Форма здания, этажи, суммарная площадь помещений в квадратных метрах	Прямоугольная, 0, 110
Количество стационарных пользователей (ПК), количество стационарных подключений, количество мобильных подключений	10, ?, 20
Сервисы (дополнительные подключения)	Нет
Прочее оконечное оборудование (дополнительные подключения)	Принтеры, сканеры.
Подключение к Internet	Gigabit Ethernet: оптоволокно
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	Программная усиленная безопасность в отношении администратора и пользователей.
Надежность	Надежность хранения данных.
Финансы	Полноценная коммерческая сеть.
Производитель сетевого оборудования	Cisco
Доп требования	задействовать уже имеющийся системный блок (Core 2 Quad Q8300, PC2-6400 4 GB, GeForce 7600GS 256 MB GDDR2, HD Audio, Gigabit Ethernet, DVD-RAM Drive)

СОДЕРЖАНИЕ

ВВЕДЕНИЕ.....	5
1 ОБЗОР ЛИТЕРАТУРЫ.....	6
1.1 Gigabit Ethernet:	6
1.2 Оптоволокно	7
1.3 Требование надежности хранения данных (RAID)	7
1.4 Программная усиленная безопасность в отношении администратора и пользователей	8
1.4.1 Cisco port-security	8
1.4.2 Межсетевой экран	8
1.5 Прочее оконечное оборудование.....	9
2 СТРУКТУРНОЕ ПРОЕКТИРОВАНИЕ	10
3 ФУНКЦИОНАЛЬНОЕ ПРОЕКТИРОВАНИЕ	12
3.1 Обоснование выбора сетевого оборудования	12
3.1.1 Обоснование выбора маршрутизатора.....	12
3.1.2 Обоснование выбора конвертера сигнала	13
3.1.3 Обоснование выбора коммутатора.....	13
3.1.4 Обоснование выбора точки доступа	14
3.1.5 Обоснование выбора рабочих станций.....	14
3.1.6 Обоснование выбора дата сервера	15
3.1.7 Обоснование выбора сканера.....	17
3.1.8 Обоснование выбора принтера	17
3.2 Расчёт покрытия помещений предприятия беспроводной сетью	18
3.3 Схема адресации	19
3.5 Настройка маршрутизатора.....	20
3.5 Настройка коммутатора.....	22
3.6 Настройка дата сервера	23
3.7 Настройка беспроводной точки доступа.....	24
3.8 Настройка стационарных компьютеров.....	25
4 ПРОЕКТИРОВАНИЕ СТРУКТУРНОЙ КАБЕЛЬНОЙ СИСТЕМЫ	27
СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ.....	29
ПРИЛОЖЕНИЕ А	30
ПРИЛОЖЕНИЕ Б.....	31

ПРИЛОЖЕНИЕ В	32
ПРИЛОЖЕНИЕ Г	33
ПРИЛОЖЕНИЕ Д	34

ВВЕДЕНИЕ

Для современных организаций и предприятий остро становится вопрос об организации и передаче рабочей информации между работниками. Эту проблему решает создание и настройка локальной компьютерной сети, которая, объединяет все персональные компьютеры и возможные периферийные устройства. Достоинства компьютерных сетей обусловили их широкое распространение в информационных системах финансовой сферы, органов управления, предприятий и организаций.

Стоит сказать, что в наше время каждая организация так или иначе имеет в своём распоряжение высокотехнологичное оборудование, для создания локальной сети и выхода в глобальную сеть интернет, данный факт обусловлен следующими факторами:

1) Во-первых это помогает улучшить и облегчить работу на всех уровнях, упростить процесс обмена информацией, избежать путаницы в работы и утечки секретной информации. Если система правильно настроена, то работники будут быстрее решать поставленные задачи, находить нужную информацию, избежать путаницы в работы и утечки секретной информации.

2) Возможность работы над одним проектом с разных устройств, имея доступ к файлам в рамках сети. Это используется для увеличения производительности, а также в целях обеспечения большей надежности при хранении информации в сети.

3) Возможность использования корпоративного программного обеспечения, лицензия на которое будет доступна в рамках локальной сети.

Таким образом, построение локальной сети является на сегодняшний день наилучшим способом создания на предприятии единой информационной среды, обусловленного современными требованиями быстрого обмена информацией между пользователями, совместного использования различных ресурсов. Сегодня эффективность построения локальной сети предприятия не вызывает сомнения, поскольку обеспечивает пользователей непрерывным доступом к корпоративным ресурсам: файлам, хранилищам данных, совместным использованием дорогостоящей оргтехники (принтеры, сканеры, факсы), быстрым и простым перемещением и добавлением новых рабочих мест и оборудования, обеспечением дополнительной безопасности корпоративных данных особой секретности и другими.

1 ОБЗОР ЛИТЕРАТУРЫ

Для успешного выполнения курсового проекта, учитывая условия заказчика, потребовалось изучить новые или углубить уже имеющиеся знания по средствам изучения дополнительных материалов.

1.1 Gigabit Ethernet:

Технология Gigabit Ethernet представляет собой дальнейшее развитие стандартов 802.3 для сетей Ethernet с пропускной способностью 10 и 100 Мбит/с. Основная цель Gigabit Ethernet состоит в значительном повышении скорости передачи данных с сохранением совместимости с уже установленными сетями на базе Ethernet. Необходимо обеспечить возможность пересылки данных между сегментами, работающими на разных скоростях, что, помимо всего прочего, позволило бы упростить архитектуру существующих мостов и коммутаторов, применяющихся в больших промышленных сетях.

Разработка технологии Gigabit Ethernet началась в ноябре 1995 года, когда была сформирована рабочая группа (IEEE 802.3z), рассматривающая возможность развития Fast Ethernet до гигабитных скоростей. После утверждения полномочий этой группы работа над стандартом стала продвигаться быстрыми темпами. При разработке этой технологии были поставлены следующие задачи :

- Достичь скорости передачи 1 Гбит/с.
- Использовать формат кадра Ethernet 802.3.
- Соответствовать функциональным требованиям стандарта 802.
- Предусмотреть простое взаимодействие между сетями со скоростями 10, 100 и 1000 Мбит/с.
- Сохранить неизменными минимальный и максимальный размер кадра согласно существующему стандарту.
- Предоставить поддержку полу- и полнодуплексного режима работы.
- Поддерживать топологию "звезда".
- Использовать метод доступа CSMA/CD с поддержкой по крайней мере одного повторителя в домене коллизий (под доменом коллизий понимается область, в пределах которой кадры от различных станций могут конфликтовать друг с другом).
- Поддерживать спецификации ANSI Fibre Channel FC-1 и FC-0 (оптоволоконный кабель) и, если возможно, медный кабель.
- Предоставить семейство спецификаций физического уровня, которые поддерживали бы канал длиной не менее: 500 метров на многомодовом оптоволоконном кабеле, 25 метров на медном проводе, 3000 метров на одномодовом оптоволоконном кабеле

1.2 Оптоволокно

Оптическое волокно — диэлектрическая направляющая среда, предназначенная для канализации электромагнитных волн оптического и инфракрасного диапазонов. Оптическое волокно коаксиальной конструкции и состоит из сердцевины, оболочки и первичного акрилатного покрытия и характеризуется профилем показателя преломления. Существует два основных типа оптических волокон: многомодовое и одномодовое, преобладающие на рынке с 70-х годов и используемые в широком диапазоне сетевых технологий. В многомодовом волокне распространяющийся по сердцевине оптический сигнал представлен множеством мод, в то время как одномодовое волокно в нормальном режиме работы поддерживает распространение только одной моды.

В многомодовых волокнах время распространения сигнала вдоль волокна различно для разных мод, что выражается в уширении импульсов на выходе волокна — межмодовой дисперсии. Разность между временем распространения различных мод называется дифференциальной модовой задержкой (Differential Mode Delay, DMD). Межмодовая дисперсия ограничивает пропускную способность многомодового волокна, то есть, с одной стороны, максимальную возможную скорость передачи, с другой — максимальное возможное расстояние.

Оболочка волокна — это слой, который окружает сердцевину. Когда свет, введенный в сердцевину, достигает границы с оболочкой, он испытывает внутреннее отражение. Условие полного внутреннего отражения (когда весь свет, распространяющийся в сердцевине, остается в сердцевине) зависит от угла, под которым свет подает на границу сердцевины и оболочки, и показателя преломления материалов, из которых они изготовлены. Чтобы свет оставался внутри сердцевины волокна, показатель преломления оболочки (n_2) должен быть меньше показателя преломления сердцевины (n_1).

Волокна можно классифицировать по размерам сердцевины и оболочки. У одномодовых волокон диаметр сердцевины не превышает 8 мкм, у многомодовых диаметр он значительно больше и равен 50 мкм или 62,5 мкм. Соответственно, два стандартных типа многомодового волокна принято обозначать как 50/125 и 62,5/125. Последняя цифра соответствует внешнему диаметру волокна, который одинаков для многомодовых и одномодовых волокон.

1.3 Требование надежности хранения данных (RAID)

В задании требуется спроектировать сеть с условием, что существует требование заказчика, связанное с надежностью хранения данных, то есть надежность должна быть направлена прежде всего на обеспечение низкой вероятности потери работоспособности. Быстрое реагирование на потерю или искажение данных и восстановление их достоверности и работоспособности

за время меньшее, чем порог между сбоем и отказом, обеспечивает высокую надежность.

RAID - избыточный массив независимых дисков — технология виртуализации данных для объединения нескольких физических дисковых устройств в логический модуль для повышения отказоустойчивости и производительности.

RAID позволяет превратить несколько физических дисковых накопителей в один большой логический. Его можно использовать в качестве хранилища данных с функцией автоматического резервного копирования или настроить как системный диск повышенной отказоустойчивости.

1.4 Программная усиленная безопасность в отношении администратора и пользователей

В отношении безопасности заказчиком было предъявлено требование программно усилить безопасно в отношении администратора и пользователей существующей сети. Мною был выбран вариант использования механизма cisco port-security для защиты административного доступа в сеть, а так же использование межсетевого экрана(firewall) для распределение интерфейсов маршрутизатора по зонам безопасности.

1.4.1 Cisco port-security

Port security — функция коммутатора, позволяющая указать MAC-адреса хостов, которым разрешено передавать данные через порт. После этого порт не передает пакеты, если MAC-адрес отправителя не указан как разрешенный. Кроме того, можно указывать не конкретные MAC-адреса, разрешенные на порту коммутатора, а ограничить количество MAC-адресов, которым разрешено передавать трафик через порт.

Используется для предотвращения:

- Несанкционированной смены MAC-адреса сетевого устройства или подключения к сети.
- Атак направленных на переполнение таблицы коммутации.

1.4.2 Межсетевой экран

Межсетевой экран или же firewall - это программное обеспечение или аппаратно-программные продукты, предназначенные для блокировки нежелательного трафика. Разрешение или запрет доступа межсетевым экраном осуществляется на основе заданных администратором параметров. В том числе могут использоваться следующие параметры и их комбинации:

- IP-адреса. При помощи Firewall можно предоставить или запретить получение пакетов с определенного адреса или задать перечень запрещенных и разрешенных IP-адресов.
- Доменные имена. Возможность установки запрета на пропуск трафика с определенных веб-сайтов.
- Порты. Задание перечня запрещенных и разрешенных портов позволяет регулировать доступ к определенным сервисам и приложениям. Например, заблокировав порт 80, можно запретить доступ пользователей к веб-сайтам.
- Протоколы. МСЭ может быть настроен таким образом, чтобы блокировать доступ трафика определенных протоколов.

1.5 Прочее оконечное оборудование

Еще одно требование, приуроченное к разрабатываемой локальной сети гласит, что мы должны задействовать уже имеющийся системный блок (Core 2 Quad Q8300, PC2-6400 4 GB, GeForce 7600GS 256 MB GDDR2, HD Audio, Gigabit Ethernet, DVD-RAM Drive), который мы будем использовать как административный ПК.

2 СТРУКТУРНОЕ ПРОЕКТИРОВАНИЕ

В данном разделе описан этап разработки структурной схемы локальной компьютерной сети для организации по торговлей бытовой химией, находящейся на цокольном этаже.

Данный раздел сопровождается структурной схемой(приложение “А”)

В таблице 2.1 приведено описание помещений организации с перечислением находящихся там устройств.

Таблица 2.1–Описание помещений

Помещение	Площадь, м ²	Список устройств	Беспроводной доступ интернет
Склад	14	Нет подключений	нет
Серверная	10	Подключены серверы для хранения данных, телекоммуникационный шкаф	да
Служебное помещение 1	22	пять ПК, десять мобильных подключений, принтер, сканер	да
Служебное помещение 2	10	два ПК, четыре мобильных подключения, принтер, сканер	да
Служебное помещение 3	12	четыре ПК, восемь мобильных подключений, принтер, сканер	да
Уборная	4	нет	да

По заданию офисное помещение предприятия находится на площади цокольного этажа здания, обладает прямоугольной площадью в 110(7.5 на 15 метров) квадратных метров. Поскольку дополнительных требований связанных с микроклиматом внутри помещения не было предъявлено, мы предполагаем, что особых проблем в этом направлении не наблюдается и внутри помещения поддерживается комнатная температура, нет излишней влажности, и эти факторы не зависят от внешних условий. Исходя из вышесказанного, не требуется осуществлять дополнительных мер защиты физической инфраструктуры прокладываемой сети от высоких перепадов температуры и влажности.

Говоря о структуре комнат, наше офисное помещение будет подразделяться на несколько сегментов: склад, серверная, три служебных помещения и одна уборная.

Подключение к корпоративной локальной сети к Internet осуществляется через маршрутизатор. К маршрутизатору будет подключен корневой коммутатор, к которому будут подключены рабочие станции, точка доступа и сервер для базы данных с поддержкой технологии RAID.

3 ФУНКЦИОНАЛЬНОЕ ПРОЕКТИРОВАНИЕ

На этапе функционального проектирования в данном разделе описывается функционирование программной и аппаратной составляющей проектируемой локальной компьютерной сети. В разделе приведены конфигурации для настройки используемых устройств, входящих в локальную сеть, дано краткое пояснение выбора устройств, приведена схема IP-адресации устройств в локальной сети.

3.1 Обоснование выбора сетевого оборудования

В данном подразделе курсового проектирования рассматривается и обосновывается выбор того или иного оборудования, кроме того проводится сравнение выбранного оборудования с другими представленными на рынке(см. Приложение В):

1. Маршрутизатор Cisco ISR4431/K9
2. Конвертер сигнала Cisco CWDM-SFP-1470-100
3. Коммутатор Cisco C1000-24P-4G-L
4. Точка доступа Cisco C9115AXI-EWC-I
5. Персональный компьютер HP 200 G3
6. Сервер базы данных Dell EMC PowerEdge T440
7. Сканер Canon Scan LiDE 120
8. Принтер HP LaserJet Pro M404dw

3.1.1 Обоснование выбора маршрутизатора

Отталкиваясь от условий задания, для выбора маршрутизатора нам следует учесть, что требуется использовать оптоволокно в качестве среды передачи данных, для достижения этой задачи мы можем использовать либо внешний модем, либо маршрутизатор с встроенным модемом, либо же использовать медиаконвертер. Говоря о последнем варианте, выбранный нами маршрутизатор должен иметь sfp порт с поддержкой технологии 1000Base-t, куда мы будем подключать медиаконвертер для преобразования оптического сигнала в электрический.

Выбор маршрутизатора остановился на модели Cisco ISR4431/K9. Выбранный маршрутизатор из коробки имеет 2 sfp порта, которые поддерживает технологию Gigabit ethernet, куда и будет подключаться соответствующий медиаконвертер. Так же данный маршрутизатор поддерживает функцию брандмауэра зональной политики, что поможет нам защитить административный компьютер и сервер с базой данных от внешнего воздействия. Так же от маршрутизатора требуется наличие свободного GigabitEthernet порта для дальнейшего подключения коммутатора и построения сети.

Таблица 3.1 – Спецификация маршрутизатора ISR4431/K9

Характеристика	Описание
USB порты(type A)	2
WAN порты	2 GE / SFP; 2 GE
USB интерфейс	USB 2.0
SSL VPN	Нет
Производительность	1 Gbps
Флеш память	8Gb
Оперативная память	4Gb
Zone-based firewall	Есть

3.1.2 Обоснование выбора конвертера сигнала

Так как по требованиям заказчика подключение к глобальной сети интернет должно происходить по средствам оптоволокна, нам требуется использовать конвертер оптического сигнала в электронный, данного эффекта можно добиться с помощью использования модема, либо маршрутизатора со встроенным модулем, либо отдельного медиаконвертера. Мною был выбран вариант с использованием медиаконвертером , поскольку в этом случае список маршрутизаторов, которые мы можем использовать, в разы увеличивается и не привязывается к наличию конкретного модуля, а зависит от наличия так называемого sfp порта. В нашем же случае будет использоваться конвертер Cisco CWDM-SFP-1470-100, поскольку он позиционируется, как самая доступная модель поддерживающая технологию Gigabit Ethernet, представленная на официальном сайте производителя.

3.1.3 Обоснование выбора коммутатора

Таблица 3.2 – Сравнение коммутаторов

Коммутатор	C1000-24P-4G-L	C1000-16P-E-2G-L
Поддержка PoE+	Да	Да
Ethernet порты	24 x Ge RJ-45	16 x Ge RJ-45
Потребляемая мощность PoE, Вт	195	120
Доступен для продажи	Да	Да
Техническая поддержка осуществляется	Да	Да

В ходе выбора коммутатора стоит учитывать возможность дальнейшего расширения нашей корпоративной сети, а так же наличие технологии PoE+ для питания точки доступа. В ходе сравнения мною был выбран коммутатор C1000-24P-4G-L, поскольку он удовлетворяет всем требованиям, а так же

имеет достаточное количество портов, которые могут быть задействованы в случае расширения сети.

3.1.4 Обоснование выбора точки доступа

Таблица 3.3 – Сравнение точек доступа

Наименование	C9115AXI-EWC-I	Cisco WAP150
Мощность, W	20.4	23
Память	2048 MB DRAM 1024 MB flash	256 MB RAM 128 MB flash
Максимальная мощность передачи 2.4 GHz, дБм	23	27
Максимальное количество подключений	150	120
Протокол безопасности	802.11i, Wi-Fi Protected Access 3 (WPA3), WPA2, WPA	802.11i, WPA3, WPA2, WPA
Wifi 6 (802.11ax)	да	нет

Среди приведенных выше моделей была выбрана первая модель, поскольку данная модель является более новой и имеет сертификат wifi 6, что определенно положительно скажется на стабильности и производительности, из-за нового механизма доставки пакетов. Должен отметить, что данная технология требует от принимающей стороны соответствующего модуля, но если учесть, что многие мобильные устройства уже сейчас имеют у себя поддержку данной технологии, а так же что в будущем 802.11ax станет стандартом де-факто, можно сказать, что установка данного оборудования имеет прикладной смысл.

Минусом же выбранной модели является её дороговизна, но благодаря тому, что по заданию требуется создать полноценную коммерческую сеть, мы можем не акцентировать внимание на данной проблеме.

3.1.5 Обоснование выбора рабочих станций

В связи с тем, что предприятие никак не связано с какого-либо рода большими компьютерными вычислениями, основной упор при выборе рабочих станций ставился на практичность, компактность и доступность. Мой выбор остановился на покупке моноблока из-за простоты перемещения и наличия встроенного монитора, что освобождает нас от покупки дополнительного оборудования.

Таблица 3.4 – Сравнение рабочих станций

Наименование	HP 200 G3	Lenovo V410z
Процессор	Intel Core i3-8130U	Intel Core i5-7400T
Память	4-16 GB RAM 1000 GB ROM	8-16 GB RAM 1000 GB ROM
Экран	21,5 дюйм, разрешение 1920x1080 точек	21,5 дюйм, разрешение 1920x1080 пикселей
Интерфейсы	1xGbE, 802.11ac	1xGbE, 802.11ac
В продаже	да	нет

Мною был выбран HP 200 G3 в связи с тем, что он всё ещё находится в свободной продаже и имеет достаточную вычислительную мощность для выполнения всех прикладных задач.

3.1.6 Обоснование выбора дата сервера

Перед тем, как выбрать нужный дата сервер, ознакомится с преимуществами и недостатками разных спецификаций технологии RAID, представленными в таблице 3.5 . При этом стоит учитывать, что выбор той или иной технологии по своей сути будет являться компромиссным, поскольку добиться определенного результата в производительности или в защите хранения данных, без потери при этом свободного места на диске невозможно или потери в производительности невозможно.

Таблица 3.5 – Таблица преимуществ и недостатков уровней RAID

Уровень RAID	Преимущества	Недостатки
0	Максимальная производительность при полной полезной емкости	Нет защиты от потери данных
1	Высокая производительность чтения и записи и данных защита (выдерживает отказ одного диска) с быстрым временем восстановления.	Наибольшая потеря полезной емкости (половина от всей емкости) с ограниченным количеством дисков (2 диска).
5	Высокая производительность чтения и защита данных (выдерживает отказ одного диска) с наименьшими потерями в полезной емкости.	Низкая производительность записи и медленное время восстановления.
6	Высокая производительность чтения и максимальная	Низкая производительность записи и медленное восстановление.

	защита данных (выдерживает сбой двух дисков).	
10	Высокая производительность чтения и записи, достаточная защита данных(допускает отказ одного диска в массиве), быстрое восстановление.	Наибольшая потеря полезной емкости (половина всей ёмкости) с ограниченным количеством дисков (до 16 дисков).
50	Высокая производительность чтения и большая емкость массива(масштабируется более чем на 32 диска) с защитой данных(допускает отказ одного диска на пролет).	Низкая производительность записи и медленное время восстановления.
60	Высокая производительность чтения и большая емкость массива (масштабируется более 32 дисков) с самыми высокими данными защита (допускает два отказа привода на пролет).	Низкая производительность записи и медленное время восстановления.

Исходя из изложенного заказчиком требования, самым подходящим для нас будет использование технологии RAID 6, поскольку насчёт производительности системы заказчик ничего не упомянул, к тому же спецификация предприятия не предполагает использования большой вычислительной мощности. Исходя из вышеперечисленных причин, будем выбирать сервер в первую очередь с учетом наличия возможности использования там RAID 6.

Поскольку при выборке дата-сервера, мы не учитывали вариант покупки собственной конфигурации сервера, а выбирали среди готовых вариантов, подходящим вариантом оказался дата сервер Dell EMC PowerEdge T440.

Таблица 3.6 – Dell EMC PowerEdge T440 спецификация

Характеристика	Описание
Корпус	tower-корпус
Процессор	Intel Xeon® Silver 4110
Оперативная память	16 ГБ памяти ECC DDR4 2400 МГц
Контроллер	контроллер PERC H730P
Поддержка RAID	поддержка RAID 0, 1, 10, 5, 6
Винчестер	SATA-винчестер на 2 ТБ
Интерфейсы	2x 1000 Mbit/s Ethernet
Блок питания	495 Вт
Габариты	175 x 435 x 376 мм

3.1.7 Обоснование выбора сканера

При выборе сканера, я отталкивался от представленного функционала и наличия подключения через USB, поскольку в требованиях заказчика не наблюдается наличия беспроводных интерфейсов. Выбор пал на сканер Canon Scan LiDE 120, так как он является неплохим вариантом если сравнивать его по параметрам цены и качества, это обосновывается небольшой ценой, маленьким весом, незначительными габаритами и достаточным функционалом.

Таблица 3.7 – Спецификация сканера Canon Scan LiDE 120

Характеристика	Описание
Тип сканера	Планшетный
Дисплей	Нет
USB интерфейс	USB 2.0
Поддержка Wifi	Нет
Поддержка	Windows, MacOS
Потребляемая мощность	2.5 Вт
Габариты(ширина, длинна, высота)	25см, 4см, 37см
Вес	1.6 кг

3.1.8 Обоснование выбора принтера

В качестве принтера мною был выбран HP LaserJet Pro M404dw, выбор был сделан в пользу данного оборудования в связи относительно небольшой стоимостью относительно конкурентов и возможностью подключения через USB порт. Так же стоит отметить, что данный принтер лазерного типа, что в случае предприятия заказчика имеет смысл, поскольку лазерные принтеры в отличие от струйных имеют большую скорость печати. При условии, что нет индивидуального принтера на каждого сотрудника, определенно будет не лишней.

Таблица 3.8 – Спецификация сканера HP LaserJet Pro M404dw

Характеристика	Описание
Скорость печати	38 стр/мин
Дисплей	Есть
USB	Есть
Поддержка	Windows, MacOS, Linux
Потребляемая мощность	22.5 Вт
Габариты(ширина, длинна, высота)	38, 64см, 23см
Вес	8.56 кг

3.2 Расчёт покрытия помещений предприятия беспроводной сетью

В соответствии с заданием требуется развернуть беспроводную сеть для обеспечения 20 мобильных подключений в помещениях организации. Для большинства современных точек доступа Cisco такое количество подключений может обслуживаться одним устройством. В помещениях организации отсутствуют ранее установленные WLAN. По периметру этажа помещения имеют железобетонные стены, обеспечивающие хорошую изоляцию от внешнего электромагнитного фона. Как следствие, влияние расположенных поблизости WLAN можно не рассматривать.

Так, как стены между помещениями организации преимущественно являются стенами из гипсокартона и силикатобетона, имеет смысл рассмотреть возможность размещения точек доступа, покрывающих более 1 помещения. Для этого требуется теоретически рассчитать места расположения точек для покрытия всех помещений организации с учётом влияния конструктивных элементов здания.

Для расчёта затухания радиоволн в беспрепятственной воздушной среде используется упрощённая формула:

$$L = 32,44 + 20 * \lg(F) + 20 * \lg(D), \text{ дБ}$$

F – частота сигнала в GHz, D – расстояние в метрах от точки доступа. Чувствительность устройств обычно находится в пределах от -65 до -75 dB.

Высота потолка – 2,5 м. Рассчитаем затухание у наиболее удалённых точек помещений.

Расстояние до самых удалённых точек помещений (углов этажа):

$$r = \sqrt{7.5^2 + 3.75^2 + 2.5^2} = 8.75 \text{ м}$$

Пусть частота точки будет 5 GHz как наиболее быстро затухающая, тогда затухание на таких точках:

$$L_{\text{макс. уд.}} = 32,44 + 20 * \lg(5) + 20 * \lg(8.75) = 65.26 \text{ дБ}$$

Рассчитанное затухание сигнала удовлетворительно с учётом мощности излучения точки доступа 20 дБ. Тогда стоит рассмотреть затухание на конструктивных элементах здания. Наиболее серьёзное препятствие для распространения сигнала представляется в виде одной стены из гипсокартона:

$$L_{\text{макс.конст.}} = L_{\text{гипс. ст.}} = 3 \text{ дБ.}$$

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

Тогда максимальное затухание сигнала в помещениях организации составляет:

$$L_{\text{макс.}} = L_{\text{макс.конст.}} + L_{\text{макс. уд.}} + L_{\text{обор.}} = 3 \text{ дБ} + 65.26 \text{ дБ} + 5 \text{ дБ} = 73,26 \text{ дБ}$$

Тогда минимальная мощность сигнала в помещении будет равна:

$$S_{\text{мин}} = S_{\text{маршрутизатора}} - L_{\text{макс}} = 20 \text{ дБ} - 73,26 \text{ дБ} = -53,26 \text{ дБ}$$

Такой показатель сигнала является удовлетворительным, что позволяет воспользоваться одной точкой доступа с мощностью излучения не менее 20 дБ для покрытия всех помещений WLAN.

3.3 Схема адресации

По заданию внешняя адресация представлена динамическим IPv4-адресом и белым IPv6-адресом, выдаваемыми провайдером. Внутренняя адресация представлена публичной подсетью IPv4, выданной провайдером. Подводя итоги вышесказанного наша сеть не нуждается в настройке NAT, но при этом является незащищенной, что противоречит условиям заказчика, поэтому данная сеть также нуждается в настройке встроенного в маршрутизатор брандмауэра для защиты тех интерфейсов, которые не должны быть достигаемы вне нашей локальной сети.

Адресация осуществляется по протоколу IPv4 и IPv6. Всего в сети используется: 10 адресов стационарными пользователями без учёта станции администратора, 21 адрес мобильными пользователями с учётом адреса шлюза для беспроводных устройств, 1 адрес сервера базы данных.

Для каждого VLAN требуется адрес для подинтерфейса на маршрутизаторе, он же будет являться шлюзом по умолчанию для всех устройств VLAN, кроме того стоит обратить внимание на наличие broadcast-адреса для каждой подсети. При резервировании адресов так же стоит учесть, возможность подключения новых устройств, в таком случае резервация адресов будет происходить в двойном объеме.

Провайдером была выдана подсеть публичных IPv4-адресов 13.127.128.0/17, так же провайдером была выдана подсеть публичных IPv6-адресов 2a02:d247:9000::/64.

Для деления, выданного провайдером адресного пространства на подсети посчитаем минимальный размер подсети исходя из формулы:

$$A_x = 2^{\lceil \log_2 (N_x * 2 + 2) \rceil},$$

где N_x – количество требуемых адресов в виртуальной подсети X.

Тогда минимальные размеры подсетей равны:

$$A_2 = 2^{\lceil \log_2 (1 * 2 + 3) \rceil} = 2^3 = 8 \text{ адреса};$$

$$A_3 = 2^{\lceil \log_2 (1 * 2 + 3) \rceil} = 2^3 = 8 \text{ адреса};$$

$$A_4 = 2^{\lceil \log_2 (20 * 2 + 3) \rceil} = 2^6 = 64 \text{ адреса};$$

$$A_5 = 2^{\lceil \log_2 (10 * 2 + 3) \rceil} = 2^6 = 32 \text{ адреса};$$

Диапазоны адресов, наименования, номера и назначения VLAN сведены в таблицы 3.9 — 3.13.

Таблица 3.9 – Проектируемые VLAN

Номер	Назначение	IPv4 подсеть	IPv6 подсеть
2	Административная сеть	13.127.128.0/29	2a02:d247:9000::2:0/125
3	Серверная сеть	13.127.128.8/29	-
4	Беспроводная сеть	13.127.128.16/26	2a02:d247:9000::4:0/122
5	Стационарная сеть	13.127.128.80/27	2a02:d247:9000::5:0/123

Адреса для конечных стационарных, и мобильных пользователей назначаются динамически, исключая станцию администратора.

Таблица 3.10 – Адресация административной подсети

Устройство	IPv4 Адрес	IPv6 Адрес
Маршрутизатор	13.127.128.1	2a02:d247:9000::2:1
VLAN	13.127.128.2	2a02:d247:9000::2:2
Станция администратора	13.127.128.3	2a02:d247:9000::2:3

Таблица 3.11 – Адресация внутренней подсети дата-сервера

Устройство	Адрес IPv4	Адрес IPv6
Маршрутизатор	13.127.128.9	2a02:d247:9000::3:1
VLAN	13.127.129.10	-
Дата сервер	13.127.129.11	-

Таблица 3.12 – Адресация внутренней беспроводной сети

Устройство	Адрес IPv4	Адрес IPv6
Маршрутизатор	13.127.128.17	2a02:d247:9000::4:1
VLAN	13.127.128.18	2a02:d247:9000::4:2
Точка доступа	13.127.128.19	2a02:d247:9000::4:3
Мобильные устройства	13.127.128.20-40	2a02:d247:9000::4:4

Таблица 3.13 – Адресация стационарных пользователей

Устройство	Адрес IPv4	Адрес IPv6
Маршрутизатор	13.127.131.1	2a02:d247:9000::5:1
VLAN	13.127.131.2	2a02:d247:9000::5:2
ПК	13.127.131.3-13	2a02:d247:9000::5:3-13

3.5 Настройка маршрутизатора

Для работы с IPv6 на маршрутизаторе мы должны настроить инкапсуляцию.

На маршрутизаторе необходимо настроить инкапсуляцию VLAN для того, чтобы трафик доходил в разные VLAN при этом используя один и тот же канал, кроме того необходима настройка access-lists и присвоение всех необходимых IP адресов. Стоит настроить пароль для администрирования коммутатора через telnet.

Начальная настройка роутера:

```
R1(config-if)#conf t
R1(config-if)#int gigabitethernet 0/1
R1(config-if)#enable secret 3256
R1(config-if)#ip address dhcp
R1(config-if)#exit
```

Настройка VLAN:

```
R1(config-if)# int gigabitethernet 0/2.1
R1(config-subif)# encapsulation dot1Q 2
R1(config-subif)# ip addr 13.127.128.1 255.255.255.248
R1(config-subif)# ipv6 addr 2a02:d247:9000::2:1/125
R1(config-subif)# int gigabitethernet 0/2.2
R1(config-subif)# encapsulation dot1Q 3
R1(config-subif)# ip addr 13.127.128.9 255.255.255.248
R1(config-subif)# int tengigabitethernet0/2.3
R1(config-subif)# encapsulation dot1Q 4
R1(config-subif)# ip add 13.127.128.17 255.255.255.192
R1(config-subif)# ipv6 add 2a02:d247:9000::4:1/122
R1(config-subif)# int gigabitethernet 0/2.4
R1(config-subif)# encapsulation dot1Q 5
R1(config-subif)# ip add 13.127.128.80 255.255.255.224
R1(config-subif)# ipv6 add 2a02:d247:9000::5:1/123
```

Настройка брандмауера:

```
R1(config)#ip access-list standard OUTER_BLOCK
R1(config-std-nacl)#deny ip any 13.127.128.1 0.0.127.255
R1(config-std-nacl)#deny ip any 13.127.129.1 0.0.127.255
R1(config-std-nacl)#permit any
R1(config)#ip access-list standard IN_ADMIN_BLOCKIN
R1(config-std-nacl)#deny ip any 13.127.128.1 0.0.127.255
R1(config-std-nacl)#permit any
R1(config)#int gigabitethernet0/1
R1(config-if)#ip access-group OUTER_BLOCK in
R1(config)#int tengigabitethernet0/2.1
R1(config-if)#ip access-group INNER_BLOCKIN in
```

Настройка маршрутизации по протоколу eigrp:

```
R1(config)#ipv6 unicast-routing
R1(config)#router eigrp 1
R1(config-router)#network 13.127.128.0
R1(config-router)#network 13.127.129.8
R1(config-router)#network 13.127.130.16
R1(config-router)#network 13.127.131.80
R1(config-router)#no shutdown
R1(config-router)#router-id 1.1.1.1
R1(config-router)#exit
```

Настройка DHCP:

```
R1(config)#ip dhcp pool POOL-v4
R1(dhcp-config)#network 13.127.128.80 255.255.255.248
R1(dhcp-config)#default-router 13.127.128.81
R1(dhcp-config)#exit
```

```

R1(config)ip dhcp excluded 13.127.128.81
R1(config)ip dhcp excluded 13.127.131.82
R1(config)#ipv6 dhcp pool POOL-v6
R1(dhcp-config)#network 2a02:d247:9000::5:0/123
R1(dhcp-config)#default-router 2a02:d247:9000::5:1
R1(dhcp-config)#exit
R1(config)ipv6 dhcp excluded 2a02:d247:9000::5:1
R1(config)ipv6 dhcp excluded 2a02:d247:9000::5:2

```

3.5 Настройка коммутатора

Настройка администрирования:

```

Switch>enable
Switch#conf terminal
Switch(config)#hostname switch1
Switch(config)#enable password strongPassword3256

```

Адресация VLAN:

```

Switch1(config)#vlan 2
Switch1(config-vlan)#name administrative
Switch1(config-if)#ip add 13.127.128.1 255.255.255.248
Switch1(config-if)#ipv6 add 2a02:d247:9000::2:2/125
Switch1(config-vlan)#exit
Switch1(config)#vlan 3
Switch1(config-vlan)#name data
Switch1(config-if)#ip add 13.127.128.9 255.255.255.248
Switch1(config)#vlan 4
Switch1(config-vlan)#name wireless
Switch1(config-if)#ip add 13.127.128.17 255.255.255.192
Switch1(config-if)#ipv6 add 2a02:d247:9000::4:2/122
Switch1(config-vlan)#exit
Switch1(config)#vlan 5
Switch1(config-vlan)#name stationary
Switch1(config-vlan)#ip add 13.127.128.81 255.255.255.224
Switch1(config-if)#ipv6 add 2a02:d247:9000::5:2/123
Switch1(config-vlan)#exit
Switch1(config-vlan)#ip default-gateway 13.127.128.1

```

Настройка портов:

```

Switch1(config)#int gigabitEthernet0/1
Switch1(config-if-range)#switchport mode trunk
Switch1(config-if-range)#switchport trunk allowed vlan 2,3,4,5
Switch1(config-if-range)#switchport trunk native vlan 1
Switch1(config)#int range gigabitEthernet0/2

```

```

Switch1(config)#switchport port-security
switch(config)#switchport port-security mac-address
0001.42EA.5CC4
switch1(config-if-range)#switchport mode access
switch1(config-if-range)#switchport access vlan 2
switch1(config)#int range gigabitEthernet0/3-12
switch1(config-if-range)#switchport mode access
switch1(config-if-range)#switchport access vlan 5
switch1(config-if-range)#spanning-tree portfast
switch1(config)#int gigabitEthernet0/14
switch1(config-if-range)#switchport mode access
switch1(config-if-range)#switchport access vlan 3
switch1(config-if-range)#spanning-tree portfast
switch1(config)#int gigabitEthernet0/15
switch1(config-if-range)#switchport mode access
switch1(config-if-range)#switchport access vlan 4
switch1(config-if-range)#spanning-tree portfast

```

3.6 Настройка дата сервера

Как уже было сказано наш дата-сервер работает под операционной системой RedHat Linux Enterprise 7. Проводить конфигурацию сервера будем с использованием встроенной консоли.

Для изменения IP-адреса gigabit ethernet порта сервера необходимо открыть для изменения следующий файл настроек интерфейса:

```
#vim /etc/sysconfig/network-scripts/ifcfg-eth0
```

Файл после редактирования:

```

ifcfg-eth0 configuration
type="Ethernet"
BOOTPROTO="NONE"
NAME="eth0"
IPADDR="13.127.129.11"
NETMASK="255.255.255.0"
GATEWAY="13.127.128.1"
DEVICE="eth0"
ONBOOT="yes"

```

Перезапустить NetworkManager с помощью команды:

```
# systemctl restart NetworkManager
```

Кроме этого, можно перезапустить сам интерфейс:

```
# nmcli con down eth0 && nmcli con up eth0
```

Часто происходит так, что внесенные изменения приводят в негодность описанную ранее сетевую логику и нужно быстро откатиться назад. Для надежности хранения данных было решено настроить Ваксир. Для этого напишем скрипт, который будет выполняться раз в неделю. Для корректного выполнения скрипта предварительно была создана папка backup в корне устройства.

```

/system scheduler add interval=7d name="Weekly-
Configuration" on-event=\

```

```
"/export file=backup/D.rsc\r\  
\n/system backup save name=backup/D"  
start-time=04:00:00
```

Скрипт создает два файла:

- D.rsc – полностью читаемый файл, который содержит наборы команд.
- D.backup – backup файл, который готов для повторной загрузки. Он используется для отката конфигурации или полного переноса на другое устройство.

Порядок настройки RAID 6:

1. Создать программное устройство RAID 6

```
sudo mdadm --create /dev/md1 --run --level=1 --raid-devices=2  
/dev/sdd1 /dev/sde1
```

2. Создать файловую систему на устройстве RAID 6

/dev/md1 (например, xfs файловую систему)

```
sudo mkfs.xfs /dev/md1
```

3. UUID каждого устройства можно получить с помощью следующей команды

```
sudo mdadm -D /dev/DEVICE | grep UUID
```

4. Далее необходимо отредактировать файл /etc/fstab, добавив запись для устройства RAID 1+0 /dev/md2

```
/dev/md1 /data xfs defaults 1 2
```

5. После этого следует смонтировать RAID устройство

```
sudo mount /data
```

3.7 Настройка беспроводной точки доступа

Для того чтобы упростить себе жизнь и должным образом сконфигурировать точку доступа, зададим ей для начала статический ip

```
AP1#conf t  
AP1(config)#interface bvl 1  
AP1(config-int)#ip address 13.127.128.19  
AP1(config-int)#no shutdown  
AP1(config-int)#end  
AP1#exit
```

Дальнейшее конфигурирование точки доступа будет происходить через встроенный в точку доступа веб-интерфейс, по средствам своего браузера пользователь может зайти в панель админа, сделав запрос [http:// 139.76.8.3](http://139.76.8.3), в результате этого действия в браузере начнет появляться веб-страничка и всплывающее окно, куда нужно будет ввести пароль по умолчанию – “Cisco” и подтвердить ввод данных формы при этом поле логина оставить пустым. В результате пользователю будут доступны настройки беспроводной точки доступа.

3.8 Настройка стационарных компьютеров

Одним из условий заказчика было программно защитить пользователя и администратора в таком случае при настройке конечного оборудования стоит установить сложный пароль, установить дополнительное антивирусное программное обеспечение.

Антивирусной защите подлежат все компоненты информационной системы, участвующие в транспортировке информации и её хранении:

- файл-серверы;
- рабочие станции;
- рабочие станции мобильных пользователей;
- сервера резервного копирования;
- почтовые сервера.

Как один из вариантов рассмотрим “Универсальный комплект Small Business” от компании Dr.WEB. Комплект Dr.Web Small Business универсальный включает в себя:

- Центр управления Dr.Web® Enterprise Security Suite;
- Dr.Web® Desktop Security Suite - комплексная антивирусная защита рабочих станций Windows либо Linux;
- Dr.Web® Server Security Suite — защита серверов Windows либо Unix, как 32-бит, так и 64-битные системы.

А также дополнительно предлагается для того же количества объектов, что и количество защищаемых рабочих станций в рамках лицензии:

- Dr.Web® Mobile Security Suite — защита мобильных устройств Windows Mobile, Android OS, Symbian OS;
- Dr.Web® Mail Security Suite - защита почтового сервера Unix, MS Exchange, Lotus, Kerio;
- Dr.Web® Gateway Security Suite - защита интернет-шлюза Kerio, Unix, Qbik Win gate, MIMESweeper;
- право на использование лечащей утилиты Dr.Web® CureNet!;
- право на использование лечащей утилиты Dr.Web® CureIt!.

универсальный включает в себя:

- Центр управления Dr.Web® Enterprise Security Suite;
- Dr.Web® Desktop Security Suite - комплексная антивирусная защита рабочих станций Windows либо Linux;
- Dr.Web® Server Security Suite — защита серверов Windows либо Unix, как 32-бит, так и 64-битные системы.

- А также дополнительно предлагается для того же количества объектов, что и количество защищаемых рабочих станций в рамках лицензии:
- Dr.Web® Mobile Security Suite — защита мобильных устройств Windows Mobile, Android OS, Symbian OS;
- Dr.Web® Mail Security Suite - защита почтового сервера Unix, MS Exchange, Lotus, Kerio;
- Dr.Web® Gateway Security Suite - защита интернет-шлюза Kerio, Unix, Qbik Win gate, MIMESweeper;
- право на использование лечащей утилиты Dr.Web® CureNet!;
- право на использование лечащей утилиты Dr.Web® CureIt!.

Причем, если учесть, что разрабатываемая сеть достаточно мала по своим размерам, покупка дополнительного оборудования может быть необязательной, а мониторинг и администрирование установленного антивирусного ПО будет производиться со станции администратора.

4 ПРОЕКТИРОВАНИЕ СТРУКТУРНОЙ КАБЕЛЬНОЙ СИСТЕМЫ

Кабельная система представляет собой неэкранированную витую пару, проложенную в кабельном коробе. В кабельном коробе кабель идет до информационной розетки, через которую происходит подключение конечных устройств. В качестве короба будет выбран короб 12х12. Короба, проводящие кабеля до розеток внутри помещения, будут располагаться над фальшпотолком, а сами розетки на расстоянии примерно 0,6 м от пола вблизи оконечных устройств. Для подключения оконечного оборудования используются однопортовые накладные розетки RJ-45 UTP. Прохождение кабелей через стену выполняется в ПВХ трубе через силикатобетонную стену и в стальной трубе через гипсокартонную стену.

Помещение предусматривает наличие серверной комнаты с серверным шкафом. Там будет находиться всё активное сетевое оборудование. Рядом будет стоять сервер для хранения данных, так же в серверной комнате будет установлен кондиционер, поскольку при долгой работе оборудование имеет свойство перегреваться, тем самым ухудшая производительность и увеличивая шанс выхода из строя.

Точка беспроводного доступа монтируется в коридоре в центре здания.

Принтеры и сканеры находятся в каждой комнате кроме склада и уборной

Со схемой плана здания можно ознакомиться в приложении Г. В плане здания можно увидеть, как прокладывается кабель и местоположение сетевого оборудования.

ЗАКЛЮЧЕНИЕ

Выполнив данную курсовую работу, была построена локальная компьютерная сеть небольшой организации, занимающейся торговлей мощных средств. Был проведен анализ предметной области во время проектирования локальной сети.

В пояснительной записке можно найти основные пояснения, которые можно использовать для понимания концепций и решений данной курсовой работы.

Был представлен план этажа, на котором можно наблюдать прокладку кабелей. Был проведен анализ и сравнение сетевого оборудования для выбора наиболее оптимального решения.

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

Локальная компьютерная сеть, спроектированная для организации, занимающейся торговлей мощными средствами, может существенно ускорить работу организации, начиная от ускоренного взаимодействия между сотрудниками и заканчивая быстрым доступом к общим данным компании, что теоретически может ускорить оформление заказов.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

- [1] Документация Cisco [Электронный ресурс]:
<http://www.justogroup.ru/cisco/dokumentacija>.
- [2] Cisco support [Электронный ресурс]:
<https://www.cisco.com/c/en/us/support>.
- [3] Cisco Port-security [Электронный ресурс]:
https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4000/8-2glx/configuration/guide/sec_port.html.
- [4] RAID Lenovo docs [Электронный ресурс]:
<https://lenovopress.lenovo.com/lp0578.pdf>.
- [5] Gigabit Ethernet [Электронный ресурс]:
<https://www.comnet.net/about/news/fast-ethernet-vs-gigabit-ethernet>.
- [6] Сетевые решения и оборудование Cisco [Электронный ресурс]. – Режим доступа: <https://www.cisco-parts.ru/catalog-cisco/setevye-resheniya-cisco>.
- [7] Каталог серверов Dell [Электронный ресурс]:
<https://www.dell.com/de-de/shop/poweredge-server>
- [8] ThinkServer TS150 User Guide and Hardware Maintenance Manual [Электронный ресурс]:
https://download.lenovo.com/pccbbs/thinkservers/ts150ughmm_en.pdf
- [9] Рожнова Н.Г. Вычислительные машины, системы и сети. Дипломное проектирование / Н.Г. Рожнова, Н.А. Искра, И.И. Глецевич – Минск БГУИР 2014.

ПРИЛОЖЕНИЕ А
(обязательное)

Схема структурная

ПРИЛОЖЕНИЕ Б
(обязательное)

Схема СКС функциональная

ПРИЛОЖЕНИЕ В
(обязательное)

Схема СКС. План этажа

ПРИЛОЖЕНИЕ Г
(обязательное)

Перечень оборудования, изделий и материалов

ПРИЛОЖЕНИЕ Д
(обязательное)

Ведомость документов