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

БГУИР КП 1-40 02 01 01 1 26 ПЗ

Выполнил:

студент гр. 950501

Рябинин С. В.

Руководитель проекта:

Глецевич. И. И.

Минск 2022

|  |  |
| --- | --- |
| Вариант | 26 |
| Объект | Кафедра государственного университета, на которой обучают физике |
| Форма здания, этажи, суммарная площадь помещений в квадратных метрах | Квадратная, 1-3, 95 |
| Количество стационарных пользователей (ПК), количество стационарных подключений, количество мобильных подключений | 60, 60+?,5 -- площадь может быть распределена по этажам поразному |
| Сервисы (дополнительные подключения) | Файловый сервер NTFS/SMB для внутреннего использовани |
| Прочее оконечное оборудование (дополнительные подключения) | принтеры, видеонаблюдение |
| Подключение к Internet | 10 Gigabit Ethernet: оптоволокно |
| Внешняя адресация IPv4, внутренняя адресация IPv4, адресация IPv6 | непосредственного подключения к провайдеру нет -- использовать первую из подходящих подсетей из своего варианта лабораторных работ,  публичная подсеть -- использовать одну из подходящих подсетей из своего варианта лабораторных работ (если возможно), доступ в Internet,  использовать подсеть из блока адресов для Беларуси |
| Безопасность | IPsec-VPN для удаленного подразделения |
| Надежность | защита от сильных перепадов напряжения |
| Финансы | полноценная коммерческая сеть |
| Производитель сетевого оборудования | Cisco |
| Дополнительное требование заказчика | нет |

**СОДЕРЖАНИЕ**

[ВВЕДЕНИЕ 4](#_Toc121246798)

[1 ОБЗОР ЛИТЕРАТУРЫ 5](#_Toc121246799)

[1.1 Оптоволокно 5](#_Toc121246800)

[1.2 Безопасность сети 5](#_Toc121246801)

[1.3 Файловый сервер 6](#_Toc121246802)

[2 СТРУКТУРНОЕ ПРОЕКТИРОВАНИЕ 8](#_Toc121246803)

[3 ФУНКЦИОНАЛЬНОЕ ПРОЕКТИРОВАНИЕ 9](#_Toc121246804)

[1.4 Обоснование выбора активного сетевого оборудования 9](#_Toc121246805)

[1.4.1 Обоснование выбора маршрутизатора 9](#_Toc121246806)

[1.4.2 Обоснование выбора коммутатора 9](#_Toc121246807)

[1.4.3 Обоснование выбора точки доступа 9](#_Toc121246808)

[1.5 Обоснование выбора камеры видео наблюдения 10](#_Toc121246809)

[1.6 Обоснование выбора пользовательских станций 10](#_Toc121246810)

[1.7 Обоснование выбора принтера 10](#_Toc121246811)

[1.8 Обоснование выбора мобильных устройства 10](#_Toc121246812)

[1.9 Расчет качества покрытия беспроводной сетью 10](#_Toc121246813)

[1.10 Схема адресации 12](#_Toc121246814)

[1.11 Настройка виртуальных сетей 12](#_Toc121246815)

[1.12 Настройка маршрутизации 12](#_Toc121246816)

[1.13 Настройка точки беспроводного доступа 12](#_Toc121246817)

[1.14 Настройка принтера 12](#_Toc121246818)

[1.15 Настройка файлового сервера 12](#_Toc121246819)

[1.16 Настройка подключения к Интернету 12](#_Toc121246820)

[4 ПРОЕКТИРОВАНИЕ СТРУКТУРНОЙ КАБЕЛЬНОЙ СИСТЕМЫ 13](#_Toc121246821)

[ЗАКЛЮЧЕНИЕ 14](#_Toc121246822)

[СПИСОК ИСПОЛЬЗУЕМЫХ ИСТОЧНИКОВ 15](#_Toc121246823)

[ПРИЛОЖЕНИЕ А 16](#_Toc121246824)

[ПРИЛОЖЕНИЕ Б 17](#_Toc121246825)

[ПРИЛОЖЕНИЕ В 18](#_Toc121246826)

[ПРИЛОЖЕНИЕ Г 19](#_Toc121246827)

[ПРИЛОЖЕНИЕ Д 20](#_Toc121246828)

ВВЕДЕНИЕ

В качестве курсовой работы необходимо создать локальную компьютерную сеть организации, занимающаяся торговлей бытовой химией, обладающей лицензией и на продажу агрессивных моющих средств, то есть предоставить соответствующую документацию. Инфраструктура объекта должна быть приближена к реальности. Проектируемая сеть должна включать как проводную, так и беспроводную составляющие, с возможностью выхода в Internet.

Локальные компьютерные сети используются повсеместно: на заводах и предприятиях, в школах, научных лабораториях, в игровых студиях. Список можно продолжать долго. Именно благодаря сетям наш мир способен бесперебойно работать. Использование локальной сети позволяет создать надлежащие условия для быстрой передачи информации, будь то текстовые сообщения, изображения, аудио или видеофайлы и так далее.

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 и т. д. Сегодня эффективность построения локальной сети предприятия не вызывает сомнения, поскольку обеспечивает пользователей непрерывным доступом к корпоративным ресурсам: файлам, хранилищам данных, совместным пользованием дорогостоящей оргтехникой (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

Перед выполнением курсовой работы необходимо актуализировать уже имеющиеся знания и изучить дополнительный материал, для более точного понимания требований заказчика.

* + 1. Подключение ко внешней СРПД

По заданию доступ к сети Internet осуществляется через оптоволокно. В качестве оптоволоконного кабеля для шнура используется zip-cord. Также указан тип оптического разъёма и полировки: LC и UPC соответственно.

Оптический коннектор LC — это малогабаритный вариант SC коннектора. Он имеет прямоугольное сечение корпуса. Конструкция исполняется на пластмассовой основе и снабжена защелкой, подобной защелке, применяющейся в модульных коннекторах медных кабельных систем. Вследствие этого и подключение коннектора производится схожим образом.

UPC ¬ это сокращение от Ultra Physicalt, который является улучшением PC оптического разъема с Контактом. UPC имеет лучше отделку поверхности после продолжительной полировки и возвратных потерь, чем PC структура, почти -50 дБ или выше. Хотя он имеет относительно низкое обратное отражение по сравнению с PC разъемом, он недостаточно прочно.

Наконечник изготавливается из керамики и имеет диаметр 1,25 мм. Применяется так же дуплексный вариант LC коннектора — два коннектора объединяются полимерным зажимом.

Исходя из приведенного выше, ввиду большей простоты прокладки сетевой инфраструктуры коммуникацию сетевого оборудования внутри офиса организации выгодно организовывать через витую пару. Следовательно, требуется некоторая аппаратура для преобразования оптического сигала в электрический для коммуникации между оптоволокном и витой парой. В данном случае можно воспользоваться, например, медиаконвертером или GPON-модемом.

* + 1. Требования к безопасности сети

В задании в качестве требования к безопасности проектируемой сети указано использования технологий VPN и протоколов шифрования SSL и TLS для обеспечения безопасного удалённого подключения пользователей к сети организации.

VPN — это совокупность технологий, позволяющая организовать защищённую виртуальную сеть, объединяющую доверенные сети и узлы, поверх открытой сети с низким уровнем доверия путём использования криптографических способов защиты данных.

VPN создает «туннель», по которому вы можете безопасно отправлять данные, используя инструменты шифрования и аутентификации. Предприятия часто используют VPN-подключения для обеспечения сотрудникам удаленного доступа к частным корпоративным сетям, даже если они работают вне офиса.

VPN позволяет удаленным устройствам, таким как ноутбуки, работать так, как будто они находятся в одной локальной сети. Многие маршрутизаторы VPN могут одновременно поддерживать десятки туннелей с помощью простых инструментов настройки, обеспечивая всем сотрудникам доступ к данным компании, где бы они ни находились.

SSL и TSL — криптографические протоколы, обеспечивающие защищённую передачу данных между узлами в сети Интернет. TLS и SSL используют асимметричное шифрование для аутентификации, симметричное шифрование для конфиденциальности и коды аутентичности сообщений для сохранения целостности сообщений.

SSL — Secure Socket Layer, уровень защищенных сокетов. TLS — Transport Layer Security, безопасность транспортного уровня. SSL является более ранней системой, TLS появился позднее и он основан на спецификации SSL 3.0, разработанной компанией Netscape Communications. Тем не менее, задача у этих протоколов одна — обеспечение защищенной передачи данных между двумя компьютерами в сети Интернет.

Безопасная передача обеспечивается при помощи аутентификации и шифрования передаваемой информации. TLS является преемником SSL, хотя они и могут использоваться одновременно, причем даже на одном и том же сервере. Такая поддержка необходима для того, чтобы обеспечить работу как с новыми клиентами (устройствами и браузерами), так и с устаревшими, которые TLS не поддерживают. Принцип работы SSL и TLS: поверх протокола TCP/IP устанавливается зашифрованный канал, внутри которого передаются данные по прикладному протоколу, например HTTP, FTP. Пакеты прикладного протокола шифруются TLS/SSL, далее уже зашифрованный пакет инкапсулируется в TCP/IP. Также TSL/SSL являются частью протокола HTTPS.

Принцип работы SSL состоит из двух фаз: фаза рукопожатия и фаза передачи данных. Во время фазы рукопожатия клиент и сервер используют шифрование открытым ключом для того, чтобы определить параметры секретного ключа, используемого клиентом и сервером для шифрования во время фазы передачи данных.

Клиент инициирует рукопожатие посылая «hello»-сообщение серверу. Такое сообщение содержит список алгоритмов симметричного шифрования, поддерживаемых клиентом. Сервер отвечает похожим «hello»-сообщением, выбрав при этом наиболее подходящий алгоритм шифрования из полученного списка. Далее сервер отправляет сертификат, который содержит его публичный ключ.

Сертификат — это набор данных, который подтверждает подлинность. Подтвержденная третья сторона, известная как центр сертификации (CA), генерирует сертификат и проверяет его подлинность. Чтобы получить сертификат, сервер должен использовать безопасные каналы для отправки своего публичного ключа в центр сертификации. Он генерирует сертификат, который содержит его собственный ID, ID сервера, публичный ключ сервера и другую информацию. А также центр сертификации создает отпечаток (digest) сертификата, который, по сути, является контрольной суммой. Далее центр сертификации создает подпись сертификата (certificate signature), которая формируется путем шифрования отпечатка сертификата приватным ключом центра сертификации.

Для проверки сертификата сервера клиент использует публичный ключ центра сертификации для расшифровки подписи. Затем клиент самостоятельно считает отпечаток сертификата сервера и сверяет с расшифрованным. Если они не совпадают, то сертификат был подделан. Естественно, для расшифровки подписи у клиента должен быть публичный ключ центра авторизации. Поэтому клиент хранит у себя список публичных ключей подтвержденных центров сертификации. Когда клиент установил подлинность сервера, сервер использует шифрование открытым ключом для определения секретного ключа для обмена информацией.

Фаза рукопожатия завершается отправкой «finished»-сообщений, как только обе стороны готовы начать использование секретного ключа. Начинается фаза передачи данных, в ходе которой каждая сторона разбивает исходящие сообщения на фрагменты и прикрепляет к ним коды авторизации сообщений MAC (message authentication code). Код авторизации сообщения это зашифрованный отпечаток, вычисленный на основе содержимого сообщений. Для получения полноценного SSL пакета каждая из сторон объединяет данные фрагмента, код авторизации сообщения, заголовки сообщения и шифруют с использованием секретного ключа. При получении пакета, каждая из сторон расшифровывает его и сверяет полученный код авторизации сообщения со своим. Если они не совпадают, то пакет был подделан.

* + 1. Прочее оконечное оборудование

В задании указанно наличие принтеров и цветных принтеров в качестве прочего оконечного оборудования разрабатываемой сети.

В зависимости от возможностей принтера его подключение к локальной сети может происходить по-разному. Существуют принтеры со встроенным Wi-Fi адаптером, осуществляющим беспроводное подключение к сети. Также принтеры со встроенным Ethernet интерфейсами, для проводного подключения. Данные типы принтеров не требуют дополнительного сетевого оборудования для подключения их к сети. Самый распространённый и дешёвый вариант — принтер с USB портом, не адаптированный ни аппаратно, ни программно для подключения его в КС. Такого рода устройства требуют устройства-адаптера для подключения к сети.

2 СТРУКТУРНОЕ ПРОЕКТИРОВАНИЕ

В данном разделе будет рассмотрена структура локальной сети.

Данный раздел сопровождает чертеж схемы СКС структурной (приложение «А»).

Для уточнения структуры подсети требуется рассмотреть структуру помещений офиса. По заданию офис находится на площади цокольного этажа здания, обладает квадратной площадью в 110 квадратных метров. Помещение обладает высокой влагозащитой и защитой о погодных условиях. В помещении поддерживается комнатная температура. Офис состоит из комнат, каждая из которых закреплена за определённым отделом. Всего в офисе есть 9 комнат, где будет использоваться конечные устройства для подключения к сети:

* склад;
* отдел закупок;
* бухгалтерия;
* отдел сбыта;
* комната руководителя предприятия;
* отдел кадров;
* отдел снабжения.

Также есть отдельное выделенное помещение для размещения сетевого оборудования.

Исходя из вышесказанного, не требуется осуществлять дополнительных мер защиты физической инфраструктуры прокладываемой сети от высоких перепадов температуры и влажности.

Подключение к корпоративной локальной сети к Internet осуществляется через маршрутизатор. К маршрутизатору будет подключен корневой коммутатор, к которому в свою очередь подключены коммутаторы для обеспечения достаточного количества стационарных подключений. Также 2 коммутатора будут использованы для подключения к web-серверам для повышения надёжности сегмента сети. К ряду коммутаторов будут подключены точки беспроводного доступа для обеспечения требуемого количества мобильных подключений.

3 ФУНКЦИОНАЛЬНОЕ ПРОЕКТИРОВАНИЕ

В данном разделе пояснительной записки описывается и проводится функциональное проектирование заданной локальной компьютерной сети. Здесь даётся более подробное описание функционирования программной и аппаратной составляющих разрабатываемой сети, а именно: приведены конфигурации для настройки устройств, входящих в локальную сеть, дано обоснование выбора сетевого оборудования и его конфигурирования, приведена схема IP-адресации устройств в локальной сети.

Более детально изучить компоненты разрабатываемой локальной сети можно в приложении Б.

* + 1. Обоснование выбора активного сетевого оборудования

При выборе сетевого оборудования требуется, чтобы оно распространялось официальными дилерами на момент окончания курсового проектирования. В случае, если у нескольких рассматриваемых аналогов характеристики полностью удовлетворяют требованиям к искомому оборудованию, выбор осуществляется на основе рекомендуемой производителем цены в пользу наименьшего её значения.

* + 1. Обоснование выбора маршрутизатора

Для выбора маршрутизатора необходимо определится с требуемой скоростью интернет-соединения, так как требования не оговаривают эту характеристику. Так как по заданию в сети присутствует web-сервер для внутреннего и внешнего использования.

Ввиду малого количества конечных устройств и малой нагрузки при interVLAN маршрутизации для организации виртуальных локальных сетей используется Router-on-Stick. Тогда к маршрутизатору требуется подключить и web-сервер для внешнего пользования.

Для нормального функционирования корпоративной сети выбрана технология 10Gb. Подключение к оптоволокну осуществляется через медиа конвертер, для которого требуется sfp+ порт для поддержки стандарта 10Gbase-t. Также требуется один sfp+ порт для подключения к коммутатору при помощи оптоволоконного кабеля для обеспечения скорости соединения 10 Гбит. Также требуется поддержка TCL-VPN.

Поскольку аппаратные решения Cisco IOS SSL VPN на момент выполнения работы устарели, для обеспечения SSL VPN потребуется приобретение и установка лицензии. По этой причине критерий поддержки SSL VPN снимается выбираемого роутера. Тогда требуется только поддержка IPSec протокола.

В качестве маршрутизатора был выбран A901-6CZ-FS-A.

Таблица 3.1 – Сравнение маршрутизаторов

|  |  |  |  |
| --- | --- | --- | --- |
| Маршрутизатор | A901-6CZ-FS-A | A901-6CZ-F-A | RV160-K8-RU |
| Поддержка IPSec | Да | Нет | Да |
| Ethernet порты | 8 x 100/1000 RJ-45 Gigabit Ethernet ports  8 x 1 SFP Gigabit Ethernet ports  2 x 10 SFP+ Gigabit Ethernet ports | 8 x 100/1000 RJ-45 Gigabit Ethernet ports  8 x 1 SFP Gigabit Ethernet ports  2 x 10 SFP+ Gigabit Ethernet ports | 4 x RJ-45 Gigabit Ethernet ports  1 RJ-45 SFP Gigabit Ethernet combination port |
| Потребляемая мощность, Вт | 58 | 57 | 18 |
| Тип слота расширения | SFP+  SFP (mini-GBIC) | SFP+  SFP (mini-GBIC) | SFP |
| Поддержка IPv6 | Да | Да | Да |
| Поддержка IPsec VPN | Да | Нет | Да |
| Доступен для продажи | Да | Да | Нет |
| Техническая поддержка осуществляется | Да | Да | Да |

После анализа и сравнения моделей был сделан выбор в пользу маршрутизатора ASR 901-6CZ-FS-A, как наиболее соответствующего требованиям.

* + 1. Обоснование выбора коммутатора

При выборе коммутатора стоит учесть надобность в резервировании портов для дальнейшего расширения сети организации. Предполагается резервирование портов в размере равном требующимся на момент проектирования сети.

От коммутаторов требуется обеспечивать количество подключений, равное удвоенному числу подключаемых к коммутатору устройств. В данном случае количество подключений равно 22. С учётом целей резервирования портов, два подключения должны поддерживать PoE+ для питания точки доступа. В данном случае был выбран коммутатор C1000-48P-4G-L ввиду наличия требуемого количества портов с учётом резервирования и поддержкой PoE+.

Таблица 3.3 – Сравнение коммутаторов второго уровня

|  |  |  |
| --- | --- | --- |
| Коммутатор | C1000-48P-4G-L | C1000-48P-4X-L |
| Количество портов | 48 x 10/100/1000 RJ45 Gigabit Ethernet ports  4 x 10 SFP+ Gigabit Ethernet ports | 48 x 10/100/1000 RJ45 Gigabit Ethernet ports  4 x 10 SFP Gigabit Ethernet ports |
| Максимальная потребляемая мощность, Вт | 400 | 400 |
| Поддержка PoE+ | Да | Да |
| Бюджет PoE, Вт | 370 | 370 |
| Пропускная способность | 52 Гб/с | 88 Гб/с |
| Скорость пересылки пакетов | 11.9 Mpps | 11.9 Mpps |
| Поддержка 802.1Q | Да | Да |
| Поддержка PoE | Да | Нет |

Обе модели обладают схожими характеристиками. Между коммутатором третьего уровня и коммутатором второго уровня будет проложено оптоволоконное соединение MMF со скоростью передачи данных 10 Гбит/сек. Исходя из вышеупомянутого факта необходима поддержка именно SFP+ порта, поэтому был сделан выбор в пользу модели C1000-48P-4G-L.

* + 1. Обоснование выбора медиаконвертера

Для подключения маршрутизатора к сети Интернет 10Gb через оптоволокно требуется конвертация оптического сигнала в электрический. Этого можно достичь использованием либо внешнего 10GPON модема, либо маршрутизатора со встроенным 10GPON модемом, либо медиаконвертером с подключением в SFP+. В отличие от PON модемов, медиаконвертеры представлены в более широком ассортименте. Найти требующийся медиаконвертер с учётом типа коннектора оптоволокна легче. Медиаконвертер соединяется с сетевым устройством при помощи SFP порта, что делает медиаконвертер более универсальным решением, отвязывая сетевое оборудования от типа присоединяемого коннектора.

Выбор остановился на использовании медиаконвертера ввиду большей гибкости при выборе маршрутизатора. Была выбрана модель SFP-10G-T-X. Выбор данной модели обусловлен соответствием требованием подключаемой внешний среды передачи данных.

* + 1. Обоснование выбора точки доступа

Для снижения нагрузки на коммутатор и отказа от покупки контроллера точек доступа решено использовать точки доступа со встроенным контроллером. Это также объясняется малым количеством точек доступа, требуемого для развёртывания WLAN организации. Требование к точке доступа, исходя из расчета затухания сигнала в пункте 3.1. – это мощность излучения более 20 дБ. Также из соображений безопасности требуется обеспечить аутентификацию мобильных пользователей. Предполагается питание точки доступа как PoE устройства.

Имеет смысл рассматривать точки доступа из серий, рекомендованных Cisco для развёртывания BSS для малого бизнеса. Из наиболее распространённых решено рассмотреть серии Cisco Catalyst 9115 и Cisco Aironet 1815m. С учётом вышеописанных требований из данных семейств подходят по требованиям модели C9115AXI-EWC-I и AIR-AP1815m-I-K9.

В таблице приведён анализ требуемых характеристик вышеуказанных точек доступа. В данном случае ля модели C9115AXI-EWC-I не специфицировано максимальное количество подключений, поэтому в качестве точки доступа выбрана модель AIR-AP1815m-I-K9.

Таблица 3.Х – сравнение характеристик рассматриваемых точек доступа.

|  |  |  |
| --- | --- | --- |
| Наименование | C9115AXI-EWC-I | AIR-AP1815m-I-K9 |
| Мощность, W | 20.4 | 13.9 |
| Максимальная мощность передачи 2.4 GHz, дБм | 23 | 27 |
| Максимальное количество подключений | Не указана в спецификации | 200 |
| Поддержка PoE |  |  |
| Протокол безопасности | 802.11i, Wi-Fi Protected Access 3 (WPA3), WPA2, WPA | 802.11i, WPA3, WPA2, WPA |

* + 1. Обоснование выбора пользовательских станций

По заданию требуется обеспечить компьютерную сеть десятью 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.

Предполагается подключение пользовательских станций к локальной компьютерной сети при помощи витой пары с разъёмом RJ45 по стандарту 1000BASE-T. Это налагает ограничения на установленную сетевую карту.

В качестве стационарной пользовательской станции была выбрана Dell OptiPlex Micro 5090-286316.

Данная модель имеет следующие характеристики:

1. Процессор: Intel Core i5 10500T.
2. Оперативная память: 8 Гб DDR4 SO-DIMM.
3. Накопитель: SSD 256 Гб
4. Сетевой интерфейс GigabitEthernet.
5. Операционная система: Windows 10 Pro

Такая комбинация комплектующих обеспечит достаточный уровень вычислительной мощности для решения поставленных задач.

* + 1. Обоснование выбора Web-сервера

В соответствии с заданием в локальной сети требуется присутствие web-сервера для внутреннего и внешнего использования. Из соображений оптимизации доступа к ресурсу сервера предполагается использование сервера с двум сетевыми картами, одна из которых будет нацелена на использование со стороны внутренней подсети, другая – со стороны внешней.

* + 1. Обоснование выбора принтера

В задании оговорено наличие принтеров и цветных принтеров в качестве прочего оконечного оборудования. В данном случае стоит выбор между принтерами, подключающимися к другому оконечному оборудованию, выступающему в роли принт-сервера, принтера со встроенной сетевой картой для подключения к сети через витую пару, беспроводным принтером и принтером со встроенным программным обеспечением, не требующего подключения управляющего оборудования.

Принтеры без встроенной сетевой карты не будут иметь возможность функционировать без принт-сервера. В качестве принт-сервера может использоваться как рабочая станция или отдельное одноимённое сетевое устройство. Использование рабочей станции не удобно в контексте организации, так как отдельная станция используется работниками организации также как основное рабочее устройство и, как следствие, подвержено различного рода уязвимостям в случае некорректного использования, что повлечёт и прекращение работы принтера. Использование принт-сервера куда более надёжно, однако его использование требует источника питания, что приводит либо к увеличению количества требуемых PoE портов коммутатора, либо к большему количеству требуемых силовых розеток. В случае сетевого принтера, подключаемого витой парой, вышеперечисленных проблем не возникает, однако это требует прокладки дополнительных кабелей для подключения. Беспроводной вариант требует наличия WLAN в месте работы принтера и его функционирование будет зависеть от функционирования точек доступа. Также усложняется построение виртуальной сети для беспроводных устройств. Принтеры со встроенным по наиболее удобны, так как на их работоспособность не влияют ни состояние управляющей машины, ни локальной сети в целом. Для такого рода принтеры требуется только подключение к питанию для функционирования. Недостатком такого рода устройств является их стоимость.

Ввиду достаточного бюджета и простоты использования организацией был выбран вариант принтера со встроенным программным обеспечением.

Выбранная модель – Epson WorkForce WF-7015 в качестве цветного принтера и Epson WorkForce Pro WF-M5299 в качестве чёрно-белого.

* + 1. Обоснование выбора мобильных устройства

В данное время мобильные телефоны являются распространенными устройствами в повседневной жизни, поэтому не подразумевается покупка дополнительных мобильных устройств. Большинство современных моделей имеют возможность подключение к Wi-Fi.

* + 1. 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 конструкционных элементов здания.

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

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

Так как форма здания квадратная, предположим размещение точки в центре на потолке. Высота потолка – 2,5 м. Рассчитаем затухание у наиболее удалённых точек помещений.

Расстояние до самых удалённых точек помещений (углов этажа):

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

Рассчитанное затухание сигнала удовлетворительно с учётом мощности излучения точки доступа 20 дБ. Тогда стоит рассмотреть затухание на конструкционных элементах здания. Наиболее серьёзное препятствие для распространения сигнала представляется в виде трёх стен из гипсокартона. Суммарно, такое препятствие даёт затухание:

.

Также стоит учесть возможное затухание за счёт взаимного размещения оборудования .

Тогда максимальное затухание сигнала в помещениях организации составляет:

Тогда минимальная мощность сигнала в помещении будет равна:

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

* + 1. Схема адресации

По заданию внешняя адресация представлена статическим публичным IPv4-адресом и белым IPv6-адресом, выдаваемыми провайдером. Внутренняя адресация представлена публичной подсетью IPv4, выданной провайдером. Ввиду этого сеть не будет нуждаться в настройке NAT ввиду видимости со стороны сети Internet всех сетевых интерфейсов. Однако этот факт ставит задачу настройки брандмауэра для защиты интерфейсов, которые не должны быть доступны вне локальной сети, например интерфейса web-сервера для внутреннего использования.

В проектируемой сети подразумевается использования виртуальных сетей для создания виртуальных доменов для стационарных пользователей, беспроводных устройств, сервера и сетевого администрирования.

Так как внутренняя IPv4 адресация представляет собой публичную подсеть, то подсеть требуется запросить у провайдера. Диапазоны адресов виртуальных подсетей получаются делением предоставляемой провайдером подсети на участки, кратные степени двойки.

Всего в сети используется:

* 9 адресов стационарными пользователями без учётом станции администратора;
* 21 адрес мобильными пользователями с учётом адреса шлюза для беспроводных устройств;
* 2 адреса web-сервером;
* 4 адреса для администрирования сетевого оборудования с учётом станции администрирования;
* 1 адрес шлюза локальной сети;
* 4 адреса виртуальными интерфейсам на подинтерфейсах маршрутизатора для interVLAN маршрутизации, адрес для административного VLAN пересекается с адресом для администрирования маршрутизатора;
* 25 удалённых пользователей.

Удалённые пользователи входят в VLAN StatUser в количестве 24 и Admin в количестве 1.

Для каждого VLAN трбуется адрес для подинттерфейса на маршрутизаторе. Он же будет являться шлюзом по умолчанию для всех устройств VLAN.

Также требуется учесть собственно адреса подсети и broadcast-адреса для подсети, выданной провайдером и используемых виртуальных подсетей и резервирование адресов в двойном объёме. Адрес шлюза удобно выдать провайдеру из области адресов подсети. Минимальный размер подсети, требуемый каждым VLAN вычисляется по формуле:

,

где – количество требуемых адресов в виртуальной подсети X.

Тогда минимальные размеры подсетей равны:

Так как размер подсети равняется степени двойки, то итоговый размер подсети, запрашиваемой у провайдера равен общему числу адресов виртуальных подсетей с учётом также адреса шлюза локальной компьютерной сети и собственно адреса и broadcast-адреса выделяемой подсети. Собственно адрес или broadcast адрес выделяемой подсети будет совпадать с одним из соответствующих адресов из диапазона одной из виртуальных сетей. Тогда размер запрашиваемого диапазона адресов провайдера равен:

Стоит отметить, что данная цифра является большой и заказ такого количества адресов у провайдера нетривиален. Резервирование такого количества публичных адресов крайне затратно с финансовой точки зрения. Однако данное решение не противоречит техническому заданию.

Провайдером была выдана подсеть публичных IPv4-адресов 154.234.0.0/24 и статический адрес 165.246.110.227. Тогда деление выданного диапазона адресов на требуемые адресные пространства VLAN удобно произвести методом последовательного отсечения наибольших сетей VLAN.

Провайдером была выдана подсеть публичных IPv6-адресов 2a00:1760:2::/64 и статический адрес 2a00:1760:0:2b4c:cccd:25a/128.

Диапазоны адресов, наименования, номера и назначения VLAN сведены в таблицу.

Таблица 3.3 – Проектируемые VLAN

|  |  |  |  |
| --- | --- | --- | --- |
| Номер | Назначение | IPv4 подсеть | IPv6 подсеть |
| 10 | Стационарные и удалённые пользователи | 154.234.0.96/27 | 2a00:1760:2::10:0/123 |
| 20 | Мобильные пользователи | 154.234.0.192/26 | 2a00:1760:2::20:0/122 |
| 30 | Сервер, внутреннее использование | 154.234.0.72/29 | 2a00:1760:2::30:0/125 |
| 40 | Удалённые пользователи | 154.234.0.128/26 | 2a00:1760:2::50:0/122 |
| 100 | Сетевое администрирование | 154.234.0.80/28 | 2a00:1760:2::40:0/124 |

Адреса для конечных стационарных, мобильных и удалённых пользователей назначаются динамически.

Таблица 3.3 – Адресация административной подсети

|  |  |  |
| --- | --- | --- |
| Устройство | IPv4 Адрес | IPv6 Адрес |
| Маршрутизатор | 154.234.0.81 | 2a00:1760:2::100:1 |
| VLAN на корневом коммутаторе | 154.234.0.82 | 2a00:1760:2::100:2 |
| Станция администратора | 154.234.0.83 | 2a00:1760:2::100:3 |
| Точка доступа | 154.234.0.84 | 2a00:1760:2::100:4 |

Таблица 3.3 – Адресация удалённых пользователей

|  |  |  |
| --- | --- | --- |
| Устройство | IPv4 Адрес | IPv6 Адрес |
| Маршрутизатор | 154.234.0.129 | 2a00:1760:2::40:1 |
| VLAN на корневом коммутаторе | 154.234.0.130 | 2a00:1760:2::40:2 |
| Станция администратора | 154.234.0.131-181 | 2a00:1760:2::40:3-35 |

Таблица 3.3 – Адресация стационарных пользователей

|  |  |  |
| --- | --- | --- |
| Устройство | Адрес IPv4 | Адрес IPv6 |
| Маршрутизатор | 154.234.0.97 | 2a00:1760:2::10:1 |
| VLAN | 154.234.0.98 | 2a00:1760:2::10:2 |
| ПК | 154.234.0.99- 117 | 2a00:1760:2::10:3-15 |

Таблица 3.3 – Адресация внутренней беспроводной сети

|  |  |  |
| --- | --- | --- |
| Устройство | Адрес IPv4 | Адрес IPv6 |
| Маршрутизатор | 154.234.0.193 | 2a00:1760:2::20:1 |
| VLAN интерфейс коммутатора | 154.234.0.194 | 2a00:1760:2::20:2 |
| Точка доступа | 154.234.0.195 | 2a00:1760:2::20:3 |
| Мобильные устройства | 154.234.0.196- 236 | 2a00:1760:2::20:4-2С |

Таблица 3.3 – Адресация внутренней подсети web-сервера

|  |  |  |
| --- | --- | --- |
| Устройство | Адрес IPv4 | Адрес IPv6 |
| Маршрутизатор | 154.234.0.73 | 2a00:1760:2::30:1 |
| VLAN | 154.234.0.74 | 2a00:1760:2::30:2 |
| Web сервер | 154.234.0.75 | 2a00:1760:2::30:3 |

* + 1. Настройка маршрутизатора

Настройка маршрутизатора осуществляется при помощи интерфейса командной строки. Для обеспечения доступа к интерфейсу командной строки маршрутизатора требуется при помощи кабеля, идущего в комплекте подключить маршрутизатор к компьютеру через консольный порт.

После чего при помощи клиентского приложения, поддерживающего работу через последовательный порт, например, PuTTY осуществляется подключение к оболочке командной строки.

На маршрутизаторе необходимо настроить инкапсуляциюVLAN, access-lists и присвоить все необходимые IP адреса.

Согласно техническим требованиям, требуется обеспечить SSL VPN для удалённых пользователей. В рамках деятельности организации в качестве VPN клиента выбран Cisco AnyConnect VPN. Выбранный маршрутизатор по умолчанию не поддерживает AnyConnect VPN. Для активации требуемого функционала требуется установить соответствующую лицензию. Была выбрана лицензия.

В качестве Cisco AnyConnect VPN лицензии выбрана Cisco AnyConnect Plus Perpetual License AC-PLS-P-25-S. Это обеспечит систему маршрутизатора необходимым функционалом на неограниченный период времени.

Router>enable

Router#configuration terminal

Router#(config)int tengigabitethernet 0/0/0

Router(config-if)# ip add 165.246.110.227.0 255.255.0.0

Router#(config)int tengigabitethernet 1/1/1

Router(config-if)# ip add 165.246.110.227.0 255.255.0.0

Настройка инкапсуляции VLAN

Router(config-if)#int tengigabitethernet 1/1/1.1

Router(config-subif)# encapsulation dot1Q 10

Router(config-subif)# ip addr 154.234.0.97 255.255.255.224

Router(config-subif)# ipv6 addr 2a00:1760:2::10:1/64

Router(config-subif)#int tengigabitethernet 1/1/1.2

Router(config-subif)# encapsulation dot1Q 20

Router(config-subif)#ip addr 154.234.0.193 255.255.255.192

Router(config-subif)# ipv6 add 2a00:1760:2::20:1/64

Router(config-subif)#int tengigabitethernet1/1/1.30

Router(config-subif)# encapsulation dot1Q 30

Router(config-subif)# ip add 154.234.0.73 255.255.255.248

Router(config-subif)# ipv6 add 2a00:1760:2::30:1/64

Router(config-subif)#int tengigabitethernet1/1/1.4

Router(config-subif)# encapsulation dot1Q 40

Router(config-subif)# ip add 154.234.0.129 255.255.255.192

Router(config-subif)# ipv6 add 2a00:1760:2::40:1/64

Router(config-subif)#int tengigabitethernet1/1/1.5

Router(config-subif)# encapsulation dot1Q 100

Router(config-subif)# ip add 154.234.0.81 255.255.255.240

Router(config-subif)# ipv6 add 2a00:1760:2::100:1/64

Настройка access-list

Router(config)#access-list 4 permit tcp any 192.168.5.3 eq http

Router(config)#access-list 4 permit tcp any 192.168.5.3 eq https

Router(config)#access-list 4 permit tcp any 192.168.33.40

Router(config)#access-list 4 permit icmp any any

Router(config)#int Gig0

Router(config-if)#ip access-group 4 in

Настройка маршрутизации

Router(config)#ipv6 unicast-routing

Router(config)#router eigrp 1

Router(config-router)#network 154.234.0.96

Router(config-router)#network 154.234.0.72

Router(config-router)#network 154.234.0.128

Router(config-router)#network 154.234.0.80

Router(config-router)#network 154.234.0.192

Router(config-router)#exit

Router(config)#ip route 0.0.0.0 0.0.0.0 tengigabitethernet0/0/0

Настрока DHCP

Router(config)#ip dhcp pool DHCP\_STAT

Router(dhcp-config)#network 154.234.0.96 255.255.255.224

Router(dhcp-config)#default-router 154.234.0.97

Router(dhcp-config)#exit

Router(config)ip dhcp excluded 154.234.0.97

Router(config)ip dhcp excluded 154.234.0.98

Router(config)#ipv6 dhcp pool DHCPv6\_STAT

Router(dhcp-config)#network 2a00:1760:2::10:0/123

Router(dhcp-config)#default-router 2a00:1760:2::10:1

Router(dhcp-config)#exit

Router(config)ipv6 dhcp excluded 2a00:1760:2::10:1

Router(config)ipv6 dhcp excluded 2a00:1760:2::10:2

Router(config)#ip dhcp pool DHCP\_REMOTE

Router(dhcp-config)#network 154.234.0.128 255.255.255.192

Router(dhcp-config)#default-router 154.234.0.129

Router(dhcp-config)#exit

Router(config)ip dhcp excluded 154.234.0.129

Router(config)ip dhcp excluded 154.234.0.130

Router(config)#ipv6 dhcp pool DHCPv6\_REMOTE

Router(dhcp-config)#network 2a00:1760:2::20:0/122

Router(dhcp-config)#default-router 2a00:1760:2::20:1

Router(dhcp-config)#exit

Router(config)ipv6 dhcp excluded 2a00:1760:2::20:1

Router(config)ipv6 dhcp excluded 2a00:1760:2::20:2

Router(config)end

* + 1. Настройка SSL VPN

Далее необходимо передать лицензию в флэш-память маршрутизатора, например по средством SCP. Далее необходимо произвести установку лицензии.

Router# copy scp://user@linux-box.cisco.com/home/user/AC-PLS-P-25-S.lic bootflash:

Router# install license bootflash: PLS-P-25-S.lic

Для предоставления AnyConnect VPN также требуется загрузить и установить пакет AnyConnect Secure Mobility Client. Он может быть загружен в секции AnyConnect Secure Mobility Client электронного ресурса []. Далее необходимо передать пакет во флэш-память маршрутизатора, например по средством SCP. После этого необходимо произвести установку пакета.

Router#copy scp://user@linux-box.cisco.com/home/user/ anyconnect-win-3.1.08009-k9.pkg bootflash: /webvpn

Router#install license bootflash: PLS-P-25-S.lic

Router#crypto vpn anyconnect flash:/webvpn/anyconnect-win-3.1.08009-k9.pkg sequence 1

Генерируем RSA ключи для сертификатов.

Router#crypto key generate rsa label SSLVPN\_KEYPAIR modulus 2048

После успешного создания пары ключей RSA необходимо настроить точку доверия PKI с информацией о нашем маршрутизаторе и парой ключей RSA. Общее имя (CN) в имени субъекта должно быть настроено с IP-адресом, который пользователи используют для подключения к шлюзу AnyConnect.

Router#crypto pki trustpoint SSLVPN\_CERT

enrollment selfsigned

subject-name CN=fdenofa-SSLVPN.cisco.com

rsakeypair SSLVPN\_KEYPAIR crypto pki enroll SSLVPN\_CERT

После правильного определения точки доверия маршрутизатор должен сгенерировать сертификат.

crypto pki enroll SSLVPN\_CERT

Далее необходимо создать AAA список аутентификации и добавить в него пользователя.

aaa new-model

aaa authentication login SSLVPN\_AAA local

username VPNUSER password TACO

Локальный пул IP-адресов должен быть создан, чтобы клиентские адаптеры AnyConnect могли получить IP-адрес. Убедитесь, что вы настроили достаточно большой пул для поддержки максимального количества одновременных клиентских подключений AnyConnect.

По умолчанию AnyConnect будет работать в режиме полного туннеля, что означает, что любой трафик, генерируемый клиентским компьютером, будет отправляться через туннель. Поскольку это обычно нежелательно, можно настроить список управления доступом (ACL), который затем определяет трафик, который должен или не должен передаваться через туннель. Как и в других реализациях ACL, неявный запрет в конце устраняет необходимость в явном отказе; следовательно, необходимо настроить операторы разрешения только для трафика, который должен быть туннелирован.

* + 1. Настройка коммутатора

На центральном коммутаторе необходимо создать необходимые VLAN, настроить VLAN интерфейсы, перевести порты в trunk или access в зависимости от предназначения интерфейса.

Switch>enable

Switch#conf terminal

Switch(config)#hostname S0

Добавление VLAN

S0(config)#vlan 10

S0(config-vlan)#name stationary

S0(config-vlan)# exit

S0(config)#vlan 20

S0(config-vlan)#name wireless

S0(config-vlan)# exit

S0(config)#vlan 30

S0(config-vlan)#name server\_inner

S0(config-vlan)# exit

S0(config)#vlan 40

S0(config-vlan)#name remote

S0(config-vlan)# exit

S0(config)#vlan 100

S0(config-vlan)#name admin

S0(config-vlan)# exit

Настройка адресации VLAN

S0(config)#int vlan 10

S0(config-if)#ip add 154.234.0.98 255.255.255.224

S0(config-if)# ipv6 add 2a00:1760:2::10:2/64

S0(config)#int vlan 20

S0(config-if)#ip add 154.234.0.194 255.255.255.192

S0(config-if)# ipv6 add 2a00:1760:2::20:2/64

S0(config)#int vlan 30

S0(config-if)#ip add 154.234.0.130 255.255.255.248

S0(config-if)# ipv6 add 2a00:1760:2::30:2/64

S0(config)#int vlan 40

S0(config-if)#ip add 154.234.0.130 255.255.255.0

S0(config-if)# ipv6 add 2a00:1760:2::40:2/64

S0(config)#int vlan 100

S0(config-if)#ip add 154.234.0.82 255.255.255.240

S0(config-if)# ipv6 add 2a00:1760:2::100:2/64

S0(config-if)exit

S1(config)# ip default-gateway 192.168.33.1

Настройка портов

S0(config)int range gig1/0/3-4

S0(config-if-range)switchport mode access

S0(config-if-range)switchport access vlan 3

S0(config)int range gig1/0/5-6

S0(config-if-range)switchport mode access

S0(config-if-range)switchport access vlan 4

S0(config)int range gig1/0/7-8

S0(config-if-range)switchport mode access

S0(config-if-range)switchport access vlan 2

S0(config)int gig1/0/9

S0(config-if)switchport mode access

S0(config-if)switchport access vlan 5

S0(config)int range gig1/0/0-2

S0(config-if-range)switchport mode trunk

S0(config-if-range)switchport trunk allow vlan 2-5,33

* + 1. Настройка точки доступа
    2. Настройка принтера

Ввиду наличия к принтера предустановленного программного обеспечения настройка принтера не требуется.

* + 1. Настройка web – сервера

Для сервера была выбрана Windows Server 2016 и в качестве web-сервера будет настроена IIS.

Для завершения конфигурации сервера требуется выполнить следующие шаги:

1. Запустить «Мастер добавления ролей и компонентов», который можно найти в меню «Пуск» «Пуск->Диспетчер серверов->Управление->Добавить роли и компоненты».

Затем следуя инструкции жмем «Далее». На следующем этапе выбираем пункт «Установка ролей и компонентов».

Далее необходимо выбрать целевой сервер.

На шаге выбора роли выбираем «Веб-сервер (IIS)». Так же нам предложат остановить компонент «Консоль управления службами», соглашаемся.

После выбора роли жмем «Далее», проверяем выбранные роли и компоненты и ждем окончания установки (рисунок 3.11).

* + 1. Настройка подключения к Интернету

4 ПРОЕКТИРОВАНИЕ СТРУКТУРНОЙ КАБЕЛЬНОЙ СИСТЕМЫ

ЗАКЛЮЧЕНИЕ

СПИСОК ИСПОЛЬЗУЕМЫХ ИСТОЧНИКОВ

[1] Сергеев, А.Н. Основы локальных компьютерных сетей / А.Н. Сергеев – М.: Лань, 2016. – 184 с.

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

[3] Таненбаум, Э. Компьютерные сети / Э. Таненбаум, Д. Уэзеролл. – 5-е издание – Санкт-Петербург [и другие] : Питер, Питер Пресс, 2017. – 955 с.

[4] Семенов, A. Б. Волоконная оптика в локальных и корпоративных сетях. / А. Б. Семенов. – Москва : АйТи-Пресс, 2005. – 304 с.

[5] What Is Network Security? [электронный ресурс] – Режим доступа: https://www.cisco.com/c/en/us/products/security/what-is-network-security.html

[6] Guide to IPsec VPNs [электронный ресурс] – Режим доступа: https://csrc.nist.rip/library/alt-SP800-77.pdf

[7] Левицкий, Н. Д. Удаленный сервер своими руками. От азов создания до практической работы / Н. Лекицкий – Спб.: НАУКА и ТЕХНИКА, 2021. - 400 с. https://www.cisco.com/c/en/us/support/all-products.html

[8] Сетевые решения и оборудование Cisco [электронный ресурс]. – Режим доступа: https://www.cisco-parts.ru/catalog-cisco/setevye-resheniya-cisco.

[9] All products support [электронный ресурс]. – Режим доступа: https://www.cisco.com/c/en/us/support/all-products.html

[10] Cisco Servers - Unified Computing System (UCS) [электронный ресурс]. – Режим доступа: https://www.cisco.com/c/en/us/products/servers-unified-computing/index.html

[11] Cable and Connectors [электронный ресурс]. – Режим доступа: https://www.cisco.com/c/en/us/td/docs/switches/lan/cisco\_ie3000/hardware/installation/guide/IE3000HIG/HIGCABLE.pdf.

[12] VLAN [электронный ресурс] – Режим доступа: http://xgu.ru/wiki/VLAN.

[13] NTFS Documentation [электронный ресурс] – Режим доступа: https://dubeyko.com/development/FileSystems/NTFS/ntfsdoc.pdf.

[14] Server Message Block Overview [электронный ресурс] – Режим доступа: https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/hh831795(v=ws.11)

[15] NTFS (NT File System) [электронный ресурс] – Режим доступа: https://www.techtarget.com/searchwindowsserver/definition/NTFS

ПРИЛОЖЕНИЕ А

(обязательное)

Схема СКС структурная

ПРИЛОЖЕНИЕ Б

(обязательное)

Схема СКС функциональная

ПРИЛОЖЕНИЕ В

(обязательное)

Перечень оборудования

ПРИЛОЖЕНИЕ Г

(обязательное)

Схема СКС принципиальная (План монтажа здания)

ПРИЛОЖЕНИЕ Д

(обязательное)

Схема СКС принципиальная (План здания)