**ВВЕДЕНИ**

В современном мире компьютерные технологии играют огромную роль и внедряются во все сферы жизни обычных людей. Невозможно вообразить современную квартиру, рабочее пространство без компьютера, принтера и прочих устройств. В прошлом веке технологии были дорогостоящими, персональный компьютер могли позволить лишь единицы. Но на сегодняшний день практически каждый может приобрести многофункциональное устройство, которое позволяет просматривать медиаконтент, создавать рисунки, музыку, программировать и даже играть. В связи с ростом спроса на высокие технологии появляется все большее количество специалистов в разных сферах IT.

Одна из основных технологий – компьютерные сети. Действительно, нельзя представить дом, офис без интернета и локальной сети, ведь глобальная сеть увеличивает эффективность большинства устройств, а некоторые из них и вовсе не будут работать без подключения к интернету. Ни одно государство, ни один бизнес не может существовать без интернета, ведь быстрая передача огромного количества данных крайне важна.

Как и многие современные технологии, компьютерные сети изначально использовались в военных целях, а первая компьютерная сеть была создана в 1956 году. Но вскоре компьютерные сети стали использовать и в гражданских целях. В основном это были локальные сети, которые использовались в больших офисах и так популярных раньше компьютерных клубах.

Основная цель данного курсового проекта – построение компьютерной сети с полным описанием принципа ее работы. Для работы потребуется изучить информацию о работе с локальными сетями, ее настройкой и обеспечением безопасности. Вся работа будет сделана в программе Cisco Packet Tracer, предназначенная для моделирования компьютерных сетей.

**1 АНАЛИЗ ИСХОДНЫХ ДАННЫХ ДЛЯ ПРОЕКТИРОВАНИЯ СЕТИ**

В любом виде работы нужен ясный и понятный план, который будет являться основой, базой всего проекта. А в условиях реального проекта исполнителю требуется согласовывать план с заказчиком.

Для начала требуется узнать всю нужную информацию о компании, не забывая и о мелочах, которые могут в корне изменить подход к работе. И обязательный пункт – это план помещения, в котором и будет разворачиваться сеть.

В данном курсовом проекте будет создаваться компьютерная сеть для компании «Document Company». Она занимается продажей офисной бумаги, принтеров и сканеров. Также компания занимается и технической поддержкой клиентов по вопросам, связанными с эксплуатацией проданных товаров. Компания также помогает своим сотрудникам улучшить свои навыки, например, в обслуживании принтеров.

Именно на основе всех этих факторов была выстроена система, по которой компания работает.

У компании есть чёткая иерархия, она разбита на 7отделов, которые обладают разными правами доступа к информации:

1 Дирекция – главный отдел компании, директор в любое время имеет доступ ко всем данным. Имеет четыре рабочих места, одно из них выделено для секретаря.

2 Отдел продаж – занимается продажей принтеров и бумаги. Десять рабочих мест.

3 Отдел сервисной поддержки – работа с клиентами, предоставляет помощь в эксплуатации продукции. Пять рабочих мест.

4 Бухгалтерия – из-за направленности компании необходимо обрабатывать большое количество договоров. Шесть рабочих мест.

5 Отдел управления проектами – работа с ключевыми заказчиками компании, приносящими стабильный и основной доход компании. Десять рабочих мест.

6 Отдел повышения квалификации – из-за направленности компании требуется подготовка новых специалистов по обслуживанию печатных устройств. Пятнадцать рабочих мест.

Таблица 1.1 – Отделы компании

|  |  |  |
| --- | --- | --- |
| Отдел | Рабочие места | Оборудование |
| Директорский | 4 | 4 ПК, кофемашина, 2 принтера |
| Сервисной поддержки | 5 | 5 ПК |
| Продаж | 10 | 10 ПК, кофемашина, принтер |
| Бухгалтерия | 6 | 6 ПК, 3 принтера, кофемашина |
| Управления проектами | 10 | 10 ноутбуков, кофемашина |
| Повышения квалификации | 15 | 15 ПК, 3 веб-камеры, 1 принтер |

Для нужд данной организации необходимо 6серверов, указанных ниже:

1 *DHCP (Dynamic Host Configuration Protocol)*, нужен для того, чтобы избавить от необходимости присваивать *IP*-адрес вручную каждому компьютеру, он делает это автоматически. Так как в данной компании много портативных ПК, без него не обойтись.

2 *DNS.* Необходим в организациях с большим количеством рабочих мест, позволяет централизованно управлять сетевыми и файловыми ресурсами.

3 *FTP*. Протокол передачи файлов по сети. В компании происходит постоянная передача данных между отделами, существенно облегчает работу с потоком этих данных.

4 *Web* – это сервер, принимающий *HTTP*-запросы от клиентов, обычно веб-браузеров, и выдающий им *HTTP*-ответы, как правило, вместе с *HTML*-страницей, изображением, файлом, медиа-потоком или другими данными. Большинство рабочего времени персонала уходит на мониторинг сети Интернет, без него работа компании остановится [1].

5 *E-mail.* Объединяет несколько протоколов, таких как *SMTP, POP3* и *IMAP*. Нужен для обмена данными между клиентами и заказчиками с помощью электронной почты.

6 *Print*. Программное обеспечение или устройство, позволяющее группе пользователей проводных и беспроводных сетей совместно использовать принтер дома или в офисе. В компании каждый день печатаются сотни бумаг, служит для обеспечения удобства этого процесса [2].

Почти все отделы будут иметь доступ ко всем сервисам, однако для отдела повышения квалификации доступ к некоторым из них будет ограничен.

Таблица 1.2 – Доступ отделов

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Отдел/ресурс | DHCP | DNS | FTP | Web | Email | Print |
| Директорский отдел | + | + | + | + | + | + |
| Продаж | + | + | + | + | + | + |
| Бухгалтерия | + | + | + | + | + | + |
| Сервисной поддержки | + | + | + | + | + | + |
| Управления проектами | + | + | + | + | + | + |
| Повышения квалификации | + | + | + | + | - | - |

Таким образом, было определено, какие отделы получат доступ к необходимым сервисам.

**2 ОБОСНОВАНИЕ ТОПОЛОГИИ КОМПЬЮТЕРНОЙ СЕТИ И СТРУКТУРЫ ИНФОРМАЦИОННЫХ РЕСУРСОВ**

Для того, чтобы построить эффективную сеть, требуется изучить основные типы сетевых топологий и выбрать наиболее оптимальную. Сетевая топология может быть использована для того, чтобы отразить основные свойства различных физических систем. Например, коммунальных сетей, сетей автомобильных дорог, железнодорожных путей, сетей передачи электроэнергии, связи и, разумеется, интернета. На более высоком уровне сетевые топологии могут отражать определенные абстракции, такие, как, например, возможности или функции, которые должны быть обеспечены, и, как утверждалось ранее, могут затем составить основу при выборе способов физической реализации системы. Такие физические или абстрактные системы обычно разрабатываются с учетом возможных изменений, то есть топология меняется с течением времени по мере добавления или устранения узлов и/или связей.

Типы топологий:

1 Звезда – базовая топология компьютерной сети, в которой все компьютеры сети присоединены к центральному узлу (обычно коммутатор), образуя физический сегмент сети. Подобный сегмент сети может функционировать как отдельно, так и в составе сложной сетевой топологии (как правило, «дерево»). Весь обмен информацией идет исключительно через центральный компьютер, на который таким способом возлагается очень большая нагрузка, поэтому ничем другим, кроме сети, он заниматься не может. Как правило, именно центральный компьютер является самым мощным, и именно на него возлагаются все функции по управлению сетью [3].

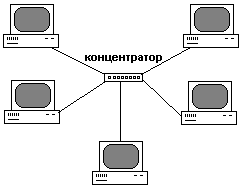


Рисунок 2.1 – Топология «Звезда»

2 Шина – Особенность сети, построенной по топологии «общая шина», заключается в передаче сигнала сразу всем компьютерам. Чтобы определить, какой из них должен их принять, используется МАС-адрес, который соответствует данной машине, точнее, ее сетевой карте. Адрес зашифровывается в каждый из пакетов, передаваемых по сети. Кроме того, данные в каждый конкретный момент времени может передавать только один компьютер. Это является слабым местом данной топологии, так как с возрастанием количества подключенных компьютеров и устройств, желающих одновременно передавать данные, скорость сети заметно падает [4].

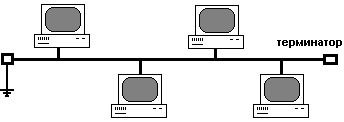


Рисунок 2.2 – Топология «Шина»

3 Кольцо – при таком подключении каждый компьютер вынужден передавать возникший сигнал по кругу, предварительно его усиливая. Это выглядит следующим образом. Когда одной рабочей станции нужно передать данные для другой, она формирует специальный маркер, содержащий адрес передающего и принимающего компьютера, и непосредственно данные. После этого сформированный маркер передается в сеть. Попадая в кольцо, сигнал переходит от одного компьютера к другому, пока не найдет адресата. Если адрес в маркере совпадает с адресом компьютера, то получившая эти данные машина посылает уведомление о получении. Таким образом, каждый компьютер принимает полученный маркер, проверяет адрес, в случае несовпадения усиливает его и передает дальше по кольцу [5].

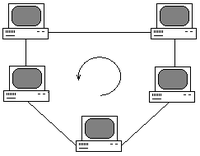


Рисунок 2.3 – Топология «Кольцо»

4 Ячеистая топология – сетевая топология компьютерной сети, построенная на принципе ячеек, в которой рабочие станции сети соединяются друг с другом и способны принимать на себя роль коммутатора для остальных участников. Данная организация сети является достаточно сложной в настройке, однако при такой топологии реализуется высокая отказоустойчивость. Как правило, узлы соединяются по принципу «каждый с каждым». Таким образом, большое количество связей обеспечивает широкий выбор маршрута следования трафика внутри сети – следовательно, обрыв одного соединения не нарушит функционирования сети в целом [6].

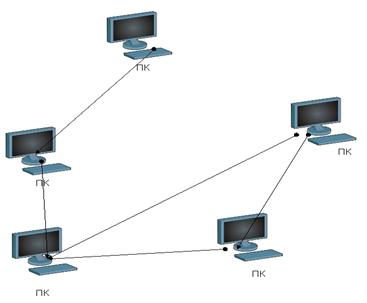


Рисунок 2.4 – Ячеистая топология

5 Древовидная топология – представляет собой особый тип структуры, в которой многие соединенные элементы расположены как ветви дерева. Они, как правило, используются для организации компьютеров в корпоративной сети или информации в базе данных.

Топология дерева базируется на двух топологиях – шины и звезды. Несмотря на то, что такая конфигурация не является широко используемой сетевой топологией, она все же применяется в определенных обстоятельствах, например, когда требуется масштабируемая иерархическая связь между двумя сетями.

В древовидной топологии между любыми двумя связанными узлами может быть только одно соединение. Поскольку любые два узла могут иметь только одну взаимную связь, такая структура образует единственную родительски-дочернюю иерархию. Например, в компьютерных сетях топология дерева также известна как топология звездной шины, потому что как уже было сказано выше, она включает в себя элементы как шинной, так и звездной конфигурации.

Древовидная топология – иерархическая структура, в которой каждый уровень связан со следующим уровнем, и находится он, как правило, выше текущего. Таким образом, в ней могут объединяться несколько звездообразных структур, что позволяет, например, если речь идет о сети, пользователям соединятся с большим количеством серверов. Такая иерархическая структура считается лучшим вариантом для подключения больших сетей [7].

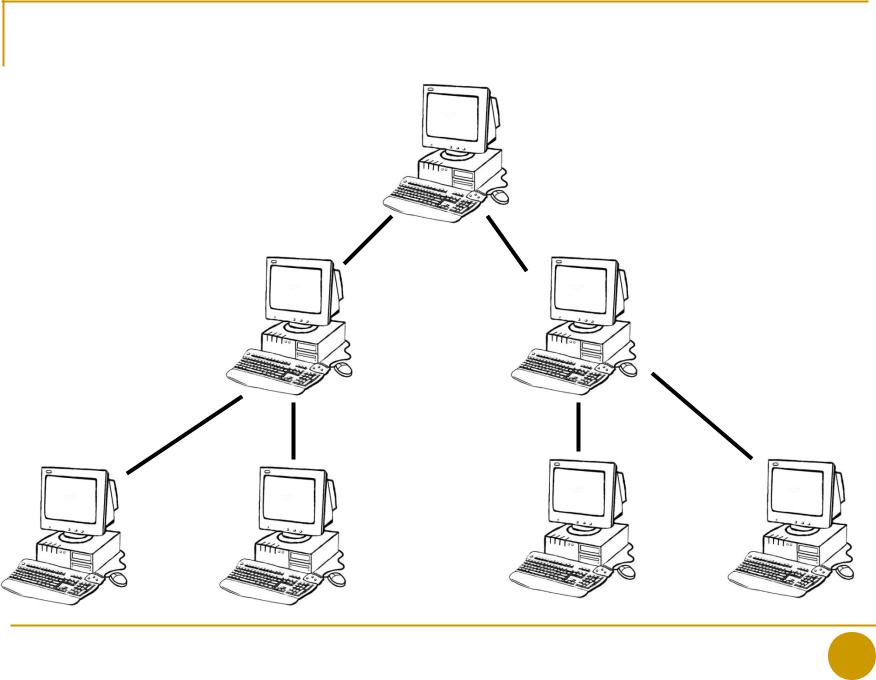


Рисунок 2.5 – Древовидная топология

В данной сети будет разумно выбрать древовидную топологию, так как в компании есть чёткая иерархия, что идеально вписывается в концепцию. У этой топологии есть как свои плюсы, так и минусы.

Из преимуществ особенно выделяют:

1 Гибкость. В древовидную топологию можно легко добавлять новые узлы (компьютеры), просто подключив к ней концентратор. Это фактически позволяет добавлять несколько компьютеров в сеть одновременно.

2 Масштабируемость. Она очень масштабируема, потому что конечные узлы могут концентрировать в себе несколько подключений от новых узлов. Такое разветвление с каждым новых подключением множит количество потенциальных подключений.

3 Доступ. Поскольку древовидная топология представляет собой большую сеть, все компьютеры будут иметь лучший доступ к сети. Это фактически делает ее наиболее эффективным способом подключения нескольких компьютеров к одному дереву.

4 Надежность. В древовидной топологии другие иерархические сети не затрагиваются, если одна из них повреждена. Это делает ее очень надежной и эффективной.

5 Позволяет использовать несколько серверов. Топология дерева также позволяет пользователям подключаться к нескольким серверами. Это фактически делает ее расширяемой и способной одновременно вместить множество компьютеров.

6 Обмен информацией. Она также позволит обмениваться информацией по крупной сети, что очень удобно для крупных корпораций.

Не стоит забывать и о недостатках:

1 Необходимы огромные кабели. Поскольку в древовидной топологии имеется несколько точек подключения, наверняка понадобятся, большое количество длинных кабелей, а это довольно затратно.

2 Длина сети ограничена типом кабеля. При такой конфигурации длина сети ограничена типом кабеля, который будет использоваться. Таким образом, потребуется использовать высококачественные кабели для расширения, иначе сигнал не будет проходить.

3 Одна точка отказа. Если магистраль всей сети выходит из строя, то ее отдельные части не смогут взаимодействовать друг с другом.

4 Обслуживание. Подобные структуры нуждаются в постоянном мониторинге и обслуживании. Причина состоит в том, что большое количество точек подключения, подразумевает относительно регулярный выход из строя того или иного узла.

**3 ВЫБОР И ОБОСНОВАНИЕ АКТИВНОГО И ПАССИВНОГО СЕТЕВОГО ОБОРУДОВАНИЯ**

Для получения доступа в сеть, необходимо иметь установленное и правильно настроенное сетевое оборудование, которое бывает как активным, так и пассивным.

Главной задачей активного сетевого оборудования является обеспечение устойчивой передачи данных от компьютера к компьютеру. Типичным примером такого сетевого оборудования являются маршрутизаторы, благодаря которым подключенные к ним компьютеры имеют возможность выходить в интернет. Любой представитель активного сетевого оборудования оперирует пакетной передачей данных. При этом каждый пакет несёт полную информацию о местонахождении, целостности содержащихся данных и иные важные сведения. Всё это даёт возможность надёжно и в полном объёме доставить данные к пункту назначения.

Помимо функции передачи данных сетевое оборудование может создавать каналы передачи данных. Это необходимо по той причине, что в сети существует множество способов пересылки данных, прямо зависящих как от текущей нагрузки на сеть, так и занятых или свободных устройств.

Чтобы создать единую сеть между несколькими компьютерами, используют специальные сетевые устройства, вроде коммутаторов и концентраторов. При этом распределением пакетов данных между компьютерами и сегментами сети занимаются маршрутизаторы [8].

Рассмотрим их подробнее, начиная с маршрутизатора. Маршрутизатор (роутер) – сетевое устройство, необходимое для перенаправления пакетов данных в одной или нескольких подсетях с помощью того или иного принципа. Маршрутизатор может анализировать данные, определяет адресата и выбирает маршрут уже исходя из полученной информации. Отчасти устройство напоминает компьютер, что, в общем-то, так и есть. Если коммутатор (свитч) может создать локальную сеть между несколькими компьютерами, то маршрутизатор способен соединить несколько сетей одновременно, причем с разными *IP*-адресами [9].

Для данной сети был выбран маршрутизатор *Cisco* 2911 [10], так как он является проверенным вариантом, единственным недостатком которого является цена.



Рисунок 3.2 – Внешний вид маршрутизатора Cisco 2911

В качестве более дешёвого аналога можно сделать выбор в пользу *TP-Link TL-R480T+* [11], который имеет 4 порта и межсетевой экран при значительно более низкой цене. Однако продукция компании *TP-Link* славится своей ненадёжностью и ориентированностью на нижний сегмент рынка, так что такой вариант лучше подойдёт для небольших компаний.



Рисунок 3.3 – Внешний вид маршрутизатора *TP-Link TL-R480T+*

В качестве аналога можно выбрать маршрутизатор *Mikrotik Hex* []. По заверениям пользователей, данный маршрутизатор надежнее ранее названного *TP-Link,* но имеет особенности, в частности непривычный интерфейс настройки устройства.Далее приведено сравнение трех выбранных маршрутизаторов (Таблица):

Таблица 3.1 – Сравнение маршрутизаторов

|  |  |  |  |
| --- | --- | --- | --- |
|  | *Cisco 2911* | *TP-Link TL-R480T+* | *Mikrotik Hix* |
| Количество портов | 3 | 4 | 5 |
| Поддержка фильтрации трафика | + | + | + |
| Брандмауэр | + | + | + |
| Динамическая маршрутизация | + | + | + |
| Цена | 1000 BYN | 159 BYN | 445 BYN |

Рисунок 3.4 – Сравнение выбранных маршрутизаторов

Маршрутизатор от компании *Cisco* имеет ряд преимуществ: поддержка *IGMP*, *PoE*, наличие *USB*-порта. Но основная причина выбора этого маршрутизатора – его стабильность и надежность.

Теперь необходимо подобрать коммутатор. Сетевой коммутатор – это устройство обеспечивающее соединение узлов компьютерной сети для организации единой системы доступа пользователей к программным, техническим и информационным ресурсам. Узлом сети считается любое устройство с *IP*-адресом способное совершать обмен данными. Основой для разработки коммутаторов послужила технология сетевого моста, которая подразумевают последовательную передачу пакетов информации. Коммутаторы, как устройства следующего поколения, обеспечивают одновременную передачу пакетов данных для всех своих портов [12].

Не изменяя самим себе, выберем коммутатор от компании Cisco, а именно *Cisco* 2960 [13]:



Рисунок 3.6 – Внешний вид коммутатора *Cisco* 2960

Дешёвым аналогом может стать коммутатор *TP-Link TL-SG2210P* [14]. Он имеет те же характеристики, однако профессиональные пользователи не рекомендуют его покупать в качестве основного оборудования по причине некачественной сборки и частых браков. Можно приобрести и использовать только в качестве резервного коммутатора.

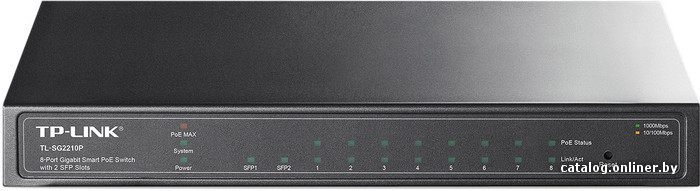


Рисунок 3.7 – Внешний вид *TP-Link TL-SG2210P*

В качестве третьего варианта можно выбрать коммутатор *Mikrotik CSS326-24G-2S+RM*. Данный коммутатор находится в средней ценовой категории и является прекрасным решением для малого бизнеса.

Далее приведена таблица сравнения всех выбранных коммутаторов уровня 2:

Таблица 3.2 – Сравнение коммутаторов *L2*

|  |  |  |  |
| --- | --- | --- | --- |
|  | *Cisco 2960* | *TP-Link TL-SG2210P* | *Mikrotik CSS326-24G-2S+RM* |
| Количество записей в таблице *MAC*-адресов | 8000 | 8000 | 16000 |
| Количество портов | 24 | 8 | 24 |
| Поддержка 802.1*q VLAN* | + | + | - |
| Поддержка питания *PoE* для *Wi-Fi* точек | - | + | + |
| Цена | 6000 BYN | 530 BYN | 1300 BYN |

Как видно исходя из таблицы сравнения, коммутатор от компании Cisco хотя и превосходит аналоги по цене, но также является самым функциональным и надежным вариантом.

Также выберем коммутатор третьего уровня. Коммутатор 3 уровня — устройство, которое пересылает трафик на основе информации уровня 3 (главным образов через *MAC*-адрес). Коммутатор 3 уровня поддерживает все функции коммутации, а также имеет некоторые функции маршрутизации между *VLAN*. Он задуман, как технология ля повышения производительности сетевой маршрутизации в больших локальных сетях. Для коммутатора 3 уровня перенаправление уровня выполняется специализированными *ASIC*, это быстрее, чем маршрутизаторы, но им обычно не хватает расширенных возможностей маршрутизаторов. В отличие от маршрутизаторов, коммутатор 3 уровня менее подвержен задержке в сети, поскольку пакетам не нужно выполнять дополнительные действия через маршрутизатор. коммутатор 3 уровня выполняет функции, как и уровня 2, поэтому, его также называют «многоуровневым» коммутатором.

Среди множества коммутаторов третьего уровня у компании *Cisco* существует много конкурентов, например, *Mikrotik* и молодая американская компания *Ubiquiti*.



Рисунок 3.9 – Внешний вид коммутатора *Ubiquiti UniFi Switch 24 [US-24-250W]*



Рисунок 3.10 – Внешний вид коммутатора *Cisco 3560*



Рисунок 3.11 – Внешний вид коммутатора *Mikrotik CRS328*

Сравнение между тремя коммутаторами приведено ниже:

Таблица 3.3 – Сравнение коммутаторов *L3*

|  |  |  |  |
| --- | --- | --- | --- |
|  | *Cisco 3560* | *Ubiquiti UniFi Switch 24 [US-24-250W]* | *Mikrotik CRS328* |
| Поддержка *ACL* | + | + | + |
| Количество портов | 24 | 24 | 24 |
| Поддержка 802.1*q VLAN* | + | + | - |
| Динамическая маршрутизация | + | + | + |
| Цена | 1000 BYN | 1800 BYN | 800 BYN |

Выбор был сделан в пользу *Cisco*. У коммутатора Cisco выше скорость коммутационной матрицы, что является важным фактором при выборе такого устройства.

Из активного сетевого оборудования осталось выбрать только *Wi-Fi* точки. Авторитетным производителем является компания *Keenetic*, ей доверяет огромное количество пользователей во всем мире. Выбор упал на *Wi-Fi* точку *Keenetic Giga KN-1011.* Характеристики данного аппарата представлены ниже (Таблица):

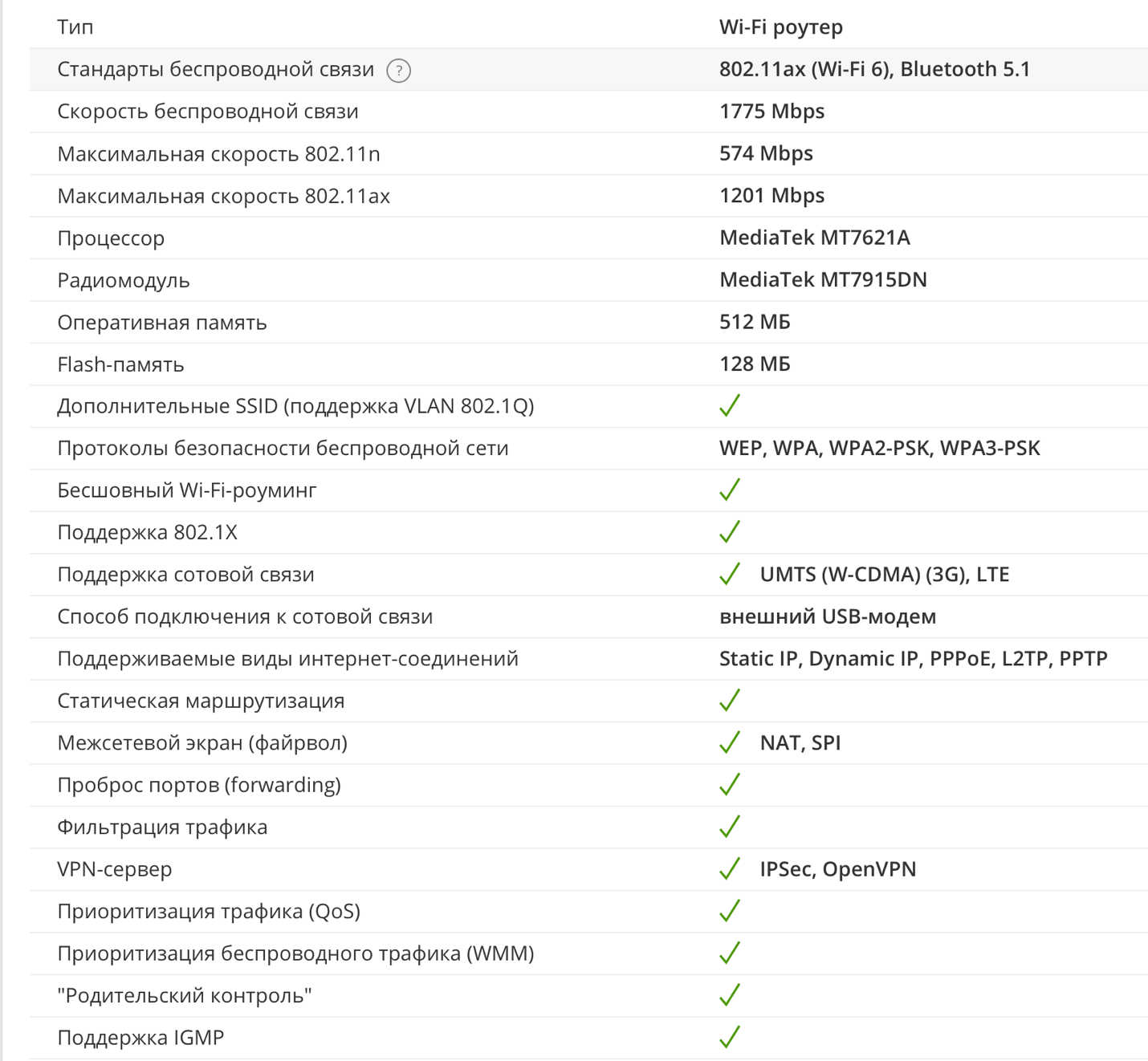


Рисунок 3.12 – Характеристики *Keenetic Giga KN-1011*

Пассивное оборудование отличается от активного в первую очередь тем, что не питается непосредственно от электросети и передает сигнал без его усиления. Пассивное сетевое оборудование делится условно на две группы. Первая группа включает в себя оборудование, являющееся трассой для кабелей: кронштейны, металлические лотки, закладные трубы, клипсы, и коммутационные шкафы. Во вторую группу входит оборудование, которое служит трактом передачи данных. Сюда относят розетки, кабели и коммутационные панели.

Подобранное пассивное оборудование приведено в таблице 3.4:

Таблица 3.4 – Пассивное оборудование

|  |  |  |  |
| --- | --- | --- | --- |
| Тип и модель оборудования | Количество | Назначение | Характеристика |
| Кабель *UTP Cat 5e* | 1000м | Соединение устройств | Неэкранированная витая пара, частотная полоса 125 МГц, скорость передачи – 1000 Мбит/с |
| Кабель-канал *SQ0408-0512 TDM ELECTRIC 60х40* | 990м | Прокладка кабеля, защита от пожара | Ширина 60 мм, высота 40 мм |
| Коннектор *RJ-45 8P8C SiPL* | 200 штук | Изготовление патч-кордов | Наконечники изготовлены из прочного и прозрачного пластика, контакты позолочены |
| Розетка *Rexant* *03-0121* | 100 штук | Подключение устройств | Количество портов: 1 |
| Коммутационный шкаф *RUN-12-60/50* | 1 штука | Размещение активного оборудования | Ёмкость для монтажа 50*U*, усиленное крепление |
| Патч-панель *RJ-45 CAT5e 19 REXANT* | 2 штуки | Упрощение монтажа сети | 48 гнёзд *RJ-45 CAT 5e, 19”* |

Всё активное оборудование было выбрано от компании *Cisco*. Также было подобрано пассивное оборудование от разных производителей.

**4 АДРЕСАЦИЯ И МАРШРУТИЗАЦИЯ В ПРОЕКТИРУЕМОЙ СЕТИ**

Сетевые устройства, соединяющие сегменты, используют не только физическое разделение с помощью кабелей, но и логическое, возможное благодаря использованию *VLAN*. Это виртуальная локальная компьютерная сеть, которая представляет собой группу хостов с общим набором требований, которые взаимодействуют так, как если бы они были подключены к широковещательному домену независимо от их физического местонахождения. *VLAN* имеет те же свойства, что и физическая локальная сеть, но позволяет конечным членам группироваться вместе из разных мест.

Таблица 4.1 – Адресация в проектируемой сети

|  |  |  |  |
| --- | --- | --- | --- |
| Отделы | Адреса | *Vlan* | Количество устройств |
| Директорский | *Gateway*: 192.168.27.1\27  Диапазон: 192.168.27.2-7 | *Vlan10* | 6 |
| Сервисной поддержки | *Gateway*: 192.168.27.33\27  Диапазон: 192.168.27.34-38 | *Vlan20* | 5 |
| Продаж | *Gateway*: 192.168.27.65\27  Диапазон: 192.168.27.66-77 | *Vlan30* | 12 |
| Управления проектами | *Gateway*: 192.168.27.97\27  Диапазон: 192.168.27.98-108 | *Vlan40* | 11 |
| Серверная | *Gateway*: 192.168.27.129\27  Диапазон: 192.168.27.130-136 | *Vlan50* | 6 |
| Бухгалтерия | *Gateway*: 192.168.27.161\27  Диапазон: 192.168.27.162-170 | *Vlan60* | 9 |
| Повышения квалификации | *Gateway*: 192.168.27.225\27  Диапазон:  192.168.27.226-244 | *Vlan70* | 19 |

**5 РАСЧЕТ ОСНОВНЫХ ЧИСЛОВЫХ ХАРАКТЕРИСТИК ПРОЕКТРИУЕМОЙ СЕТИ**

Для того, чтобы обеспечить быстродействие и отказоустойчивость сети, необходимо знать её слабые места. Такими потенциально могут быть так называемые «узкие места». Это узлы сети, в которых нагрузка на узел очень большая, что приводит к очередям и сильному снижению пропускной способности. Поэтому при построении сети нужно учитывать возможное появление таких мест.

Чтобы найти «узкие места» нужно воспользоваться формулой:

*B=S/N*, (5.1)

где *B* – средняя пропускная способность узла; *S* – скорость канала; *N* – наибольшее вероятное количество узлов в *VLAN*.

В нашей сети самой загруженной *VLAN* является отдел младшего менеджмента, так как в нём находится наибольшее количество узлов (20). Значит в нём будет минимальная пропускная способность.

Пропускная способность каждого отдела равна 1 Гбит/с. Значит, при максимальной загруженности пропускная способность в «узких местах» будет равна минимуму – 50 Мбит/с.

Согласно расчёту, пропускная способность для каждого отдела:

Для *VLAN* 10 B = 1000/4 = 250 Мбит/с.

Для *VLAN* 20 B = 1000/4 = 250 Мбит/с.

Для *VLAN* 30 В = 1000/10 = 100 Мбит/с.

Для *VLAN* 40 В = 1000/4 = 250 Мбит/с.

Для *VLAN* 50 В = 1000/3 = 333.3 Мбит/с.

Для *VLAN* 60 В = 1000/5= 200 Мбит/с.

Для *VLAN* 70 В = 1000/5 = 200 Мбит/с.

Для *VLAN* 80 В = 1000/20 = 50 Мбит/с.

Потребляемая мощность сетевого оборудования определяется суммарным потреблением мощности каждого компонента. Формула для расчёта мощности:

*P = NS* · *S + NMS* · *MS + NR* ·*R,* (5.2)

где *P* – мощность; *NS* – количество коммутаторов второго уровня; *S* – потребляемая мощность коммутатором второго уровня; *NMS* – количество коммутаторов третьего уровн; *MS* – потребляемая мощность коммутатором третьего уровня; *NR* – количество маршрутизаторов; *R* – потребляемая мощность роутером.

Мощность маршрутизатора – 39.6 Вт, коммутатора *L3* – 40.5 Вт, коммутатора *L2* – 18.6 Вт.

Суммарная мощность равна:

*P* = 39.6 Вт · 2 + 40.5 Вт · 2 + 18.6 Вт · 8 = 309 Вт.

Также необходимо рассчитать портовую ёмкость по следующей формуле:

*G = NS* ·𝑆 *+ NMS* ·𝑀𝑆 *+ NR* ·𝑅, (5.3)

где *G* – портовая ёмкость; *NS* – количество коммутаторов второго уровня; *S* – количество портов коммутатора второго уровня; *NMS* – количество коммутаторов третьего уровня; *MS* – количество портов коммутатора третьего уровня; *NR* – количество маршрутизаторов; *R* – количество портов маршрутизатора.

**6 МЕРОПРИЯТИЯ ПО ОБЕСПЕЧЕНИЮ УПРАВЛЕНИЯ, ОТКАЗОУСТВОЙЧИВОСТИ, И БЕЗОПАСНОСТИ СЕТИ И ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ**

Одним из важнейших пунктов при обеспечении отказоустойчивости сети является резервирование коммутаторов высокого уровня и маршрутизаторов. В таком случае, если один из компонентов выйдет из строя, благодаря резервному сеть продолжит работать. Реализация такого приёма изображена на рисунке 6.1:

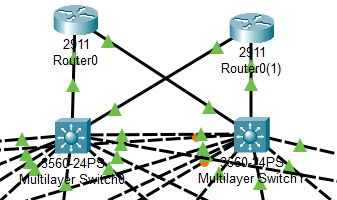


Рисунок 6.1 – Резервирование сети

Для фильтрации трафика и разграничения доступа отделов необходимо использовать *ACL*-списки. В качестве примера: благодаря ним рядовой сотрудник не сможет удалённо проникнуть к конфиденциальной информации. Также они помогают контролировать входящий и исходящий трафик.

*ACL*-списки всегда размещаются на интерфейсе, и начинают работать со входящим или исходящим трафиком, смотря куда назначены. Если трафик входит в маршрутизатор, то он является входящим, а если выходит из него – исходящим.

*ACL* бывает трёх типов:

1 Стандартный. Может проверять только адрес источника.

2 Расширенный. Может проверять адрес источника и адрес получателя, а также заглядывать внутрь пакета и определять тип трафика.

3 Именованный. Может быть как стандартным, так и расширенным, используется для удобства. Ему присваивается определенное имя, а не порядковый номер.

При настройке *ACL*-списков важно знать, что обработка ведётся строго в том порядке, в каком записаны команды, так что для корректной работы нужно составить заранее план создания *ACL*-списков и записывать туда все введенные команды. Это может быть простой блокнот, но он очень упрощает процесс. Есть ещё несколько правил, которые следует знать:

1 Если одно условие из списка совпало, пакет дальше не обрабатывается.

2 В конце каждого списка стоит условие «*deny any*».

3 На один интерфейс можно разместить только один список.

4 Стандартные списки размещаются ближе к получателю, а расширенные – к отправителю.

В проектируемой сети использован антивирус *K7 Endpoint Security*, который разработан специально для защиты корпоративных данных. Для выбранной компании был подключен пакет «*K7 for Business*». Он включает защиту от вирусов и интернет-угроз, контроль приложений и устройств, двусторонний межсетевой экран для регулирования входящего и исходящего трафика, а также систему обнаружения и предотвращения вторжений. Доступны средства защиты как локальной, так и облачной инфраструктуры предприятия.

Современный офис так же должен иметь корпоративный *VPN* для дополнительной безопасности и отказоустойчивости в случаях временно введённых интернет-провайдером ограничений. Кроме этого, *VPN* является замечательным способом организации доступа отдельного компьютера в локальную сеть компании. Сотрудники, которые находятся в командировке, смогут легко подключиться к сети компании, без необходимости покупки дорогостоящего ПО. Для подключения *VPN* необходимо вызвать команду специалистов, которые установят ПО на компьютеры компании.

В качестве дополнительной меры безопасности были приобретены источники бесперебойного питания *APC Smart-UPS XL Modular 3000VA.* В случае отключения электроэнергии у работников будет время сохранить важные файлы и избежать утери данных.

Для устранения проблемы доставки возвратных пакетов в моделируемой сети была использована технология *PAT*. Она транслирует частные адреса локальных хостов в один имеющийся зарегистрированный. Процесс настройки *PAT* описан в следующей главе.

**7 МОДЕЛИРОВАНИЕ ПРОЕКТИРУЕМОЙ КОМПЬЮТЕРНОЙ СЕТИ**