Министерство науки и высшего образования российской федерации

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых»

(ВлГУ)

**КУРСОВАЯ РАБОТА**

Дисциплина: Сети и системы передачи информации

Тема: Разработка корпоративной локально-вычислительной сети предприятия

Руководитель:

Доцент кафедры ИЗИ \_\_\_\_\_\_\_\_\_\_\_\_\_\_ М.М. Агафонова

Исполнитель:

Студент гр. ИБ-120\_\_\_\_\_\_\_\_\_\_\_\_\_\_ И.И. Гусев

Владимир 2023

**СОДЕРЖАНИЕ**

[**ВВЕДЕНИЕ** 3](#_Toc154228835)

[**1 АНАЛИЗ ПРЕДМЕТНОЙ ОБЛАСТИ** 4](#_Toc154228836)

[**2 СХЕМА ФИЗИЧЕСКОГО/КАНАЛЬНОГО УРОВНЯ КОРПОРАТИВНОЙ ЛВС** 10](#_Toc154228837)

[**3 СХЕМА СЕТЕВОГО УРОВНЯ КОРПОРАТИВНОЙ ЛВС** 12](#_Toc154228838)

[**4 РАСПРЕДЕЛЕНИЕ АДРЕСНОГО ПРОСТРАНСТВА** 14](#_Toc154228839)

[**5 ЭКОНОМИЧЕСКИЙ РАСЧЕТ** 16](#_Toc154228840)

[**6 ТЕСТИРОВАНИЕ** 17](#_Toc154228841)

[**ЗАКЛЮЧЕНИЕ** 21](#_Toc154228842)

[**СПИСОК ИСПОЛЬЗУЕМЫХ ИСТОЧНИКОВ** 22](#_Toc154228843)

[**ССЫЛКА НА ПРОЕКТ** 23](#_Toc154228844)

**ВВЕДЕНИЕ**

Цель работы: на базе нескольких информационных технологий разработать проект корпоративной ЛВС. Используя эмулятор сетей Cisco Packet Tracer, разработать модель проектируемой сети.

Задачи:

1) Анализ предметной области (включая описание предприятия).

2) Разработать проект физического уровня корпоративной ЛВС.

3) Разработать проект канального уровня корпоративной ЛВС.

4) Разработать проект сетевого уровня корпоративной ЛВС.

5) Расчёт стоимости проекта.

6) Разработка модели в Cisco Packet Tracer.

7) Экспериментальное исследование модели.

8) Подготовка документации проекта.

Актуальность выполнения проекта:

Приобретение навыков. Проектирование и моделирование ЛВС является актуальным в виду возросшей популярности внедрения и дальнейшей модернизации сетевых технологий на предприятии.

Планируемые научные/научно-технические результаты работ по проекту:

Разработать проект физического уровня корпоративной ЛВС, разработать проект канального уровня корпоративной ЛВС, разработать проект сетевого уровня корпоративной ЛВС, разработка модели в Cisco Packet Tracer.

**1 АНАЛИЗ ПРЕДМЕТНОЙ ОБЛАСТИ**

Лока́льная вычисли́тельная сеть (ЛВС, локальная сеть; англ. Local Area Network, LAN) — компьютерная сеть, покрывающая обычно относительно небольшую территорию или небольшую группу зданий (дом, офис, фирму, институт).

Существуют способы классифицировать сеть. Основным критерием классификации принято считать способ администрирования. То есть в зависимости от того, как организована сеть и как она управляется, её можно отнести к локальной, распределённой, городской или глобальной сети. Управляет сетью или её сегментом сетевой администратор. В случае сложных сетей их права и обязанности строго распределены, ведётся документация и журналирование действий команды администраторов.

Компьютеры могут соединяться между собой, используя различные среды доступа: медные проводники (витая пара), оптические проводники (оптические кабели) и через радиоканал (беспроводные технологии). Проводные, оптические связи устанавливаются через Ethernet и прочие средства. Отдельная локальная вычислительная сеть может иметь связь с другими локальными сетями через шлюзы, а также быть частью глобальной вычислительной сети (например, Интернет) или иметь подключение к ней.

Чаще всего локальные сети построены на технологиях Ethernet. Следует отметить, что ранее использовались протоколы Frame Relay, Token ring, которые на сегодняшний день встречаются всё реже, их можно увидеть лишь в специализированных лабораториях, учебных заведениях и службах. Для построения простой локальной сети используются маршрутизаторы, коммутаторы, точки беспроводного доступа, беспроводные маршрутизаторы, модемы и сетевые адаптеры. Реже используются преобразователи (конвертеры) среды, усилители сигнала (повторители разного рода) и специальные антенны.

Маршрутизация в локальных сетях используется примитивная, если она вообще необходима. Чаще всего это статическая либо динамическая маршрутизация (основанная на протоколе RIP).

Иногда в локальной сети организуются рабочие группы — формальное объединение нескольких компьютеров в группу с единым названием.

Сетевой администратор — человек, ответственный за работу локальной сети или её части. В его обязанности входит обеспечение и контроль физической связи, настройка активного оборудования, настройка общего доступа и предопределённого круга программ, обеспечивающих стабильную работу сети.

Технологии локальных сетей реализуют, как правило, функции только двух нижних уровней модели OSI — физического и канального. Функциональности этих уровней достаточно для доставки кадров в пределах стандартных топологий, которые поддерживают LAN: звезда, общая шина, кольцо и дерево. Однако из этого не следует, что компьютеры, связанные в локальную сеть, не поддерживают протоколы уровней, расположенных выше канального. Эти протоколы также устанавливаются и работают на узлах локальной сети, но выполняемые ими функции не относятся к технологии LAN.

**Адресация.**

В локальных сетях, основанных на протоколе IPv4, могут использоваться специальные адреса, назначенные IANA (стандарты RFC 1918 и RFC 1597):

10.0.0.0—10.255.255.255;

172.16.0.0—172.31.255.255;

192.168.0.0—192.168.255.255.

Такие адреса называют частными, внутренними, локальными или «серыми»; эти адреса недоступны из сети Интернет. Необходимость использовать такие адреса возникла из-за того, что при разработке протокола IP не предусматривалось столь широкое его распространение, и постепенно адресов стало не хватать. Для решения этой проблемы был разработан протокол IPv6, однако он пока малопопулярен. В различных непересекающихся локальных сетях адреса могут повторяться, и это не является проблемой, так как доступ в другие сети происходит с применением технологий, подменяющих или скрывающих адрес внутреннего узла сети за её пределами — NAT или прокси дают возможность подключить ЛВС к глобальной сети (WAN). Для обеспечения связи локальных сетей с глобальными применяются маршрутизаторы (в роли шлюзов и файрволов).

Конфликт IP адресов — распространённая ситуация в сети, при которой в одной IP-подсети оказываются два или более компьютеров с одинаковыми IP-адресами. Для предотвращения таких ситуаций и облегчения работы сетевых администраторов применяется протокол DHCP, позволяющий компьютерам автоматически получать IP-адрес и другие параметры, необходимые для работы в сети TCP/IP.

Корпоративная сеть – это структурная сеть какой-либо организации, главной целью которой является создание эффективной внутренней и внешней работы этой организации. По сути, это взаимосвязанная совокупность локальных сетей под влиянием глобальной сети. Пользователями данной сети являются исключительно сотрудники данной организации. Часто корпоративная сеть включает в себя также офисы, отделения, подразделения и иные структуры организации в различных городах и странах.

**Организация объединенной корпоративной сети.**

Локальные корпоративные сети каждого отделения связаны друг с другом опорной (транспортной) сетью. При масштабной организации, когда отделения и офисы компании находятся в разных городах и странах, в качестве опорных сетей могут использоваться уже существующие глобальные сети передачи данных, а именно сети Интернет. Основной обмен данных осуществляется в локальных сетях, а опорная сеть предназначена для согласования проектных результатов, получаемых в разных офисах организации. Этому способствует иерархическая структура сети, тем самым снижая трафик в каналах передачи данных.

Канал передачи данных включает в себя опорную транспортную сеть в роли линии связи для обмена данными между отделениями, оконечную аппаратуру приема-передачи данных, коммутационное оборудование на маршруте передачи данных.

Первая задача для организации объединенной корпоративной сети –каналы связи. Есть несколько вариантов организации каналов связи между отделениями:

* Собственный физический канал связи
* VPN

В первом варианте каналы строятся между отделениями. Это может быть медный кабель, коаксиал, оптический кабель, радиосвязь и прочее.

К достоинствам данного метода можно отнести:

* Гибкость (при предъявляемых требованиях канал возможно развернуть)
* Контроль и безопасность

Из недостатков:

* Развертывание
* Обслуживание
* Приемлемо для небольших расстояний – для организации связи между отделениями в других городах и странах лучше воспользоваться уже существующими сетями, а прокладка кабелей будет актуальна лишь в пределах небольшой территории, ограниченной несколькими километрами, или, например, между соседними зданиями.

Во втором варианте организации используются уже существующая глобальная сеть обмена данными между отделениями - поверх существующей сети организуется VPN.

Существуют 2 метода организации единой объединенной корпоративной сети организации через VPN:

1. С помощью использования интернет-провайдера;
2. С помощью использования собственного оборудования.

В первом случае, если главный офис и отделения организации подключены к сети Интернет через 1-ого интернет-провайдера, то, при наличии у него услуги VPN, можно рассчитывать на аренду выделенных линий (в том числе высокоскоростных) у интернет-провайдера.

Достоинства данного метода:

* Простота в использовании, так как обслуживание полностью возлагается на провайдера
* Универсальный размер канала – скорость передачи не может быть ниже заявленной

Недостатки данного метода:

* Бесконтрольность - организация не несет ответственность за оборудование, которое находится на стороне провайдера
* Дороговизна - при большой удаленности отделений друг от друга стоимость аренды каналов может значительно возрасти

Во втором случае, если отделения организации располагаются в разных странах и не могут пользоваться услугами одного провайдера, возможно, придется организовывать объединение отделений на основе собственного оборудования.

Достоинства данного метода:

* Низкая стоимость – деньги организации расходуются только на оплату Интернета
* Способность справиться с ростом масштабов деятельности

Недостатки данного метода:

* Скорость–передача данных может варьироваться

**Описание предприятия.**

Объект – государственная организация кредитно-финансовой системы «*Креатив Код*», занимающая один этаж двухэтажного кирпичного здания с суточным постом физической охраны. Организация кредитно-финансовой системы 'Креатив Код' занимается разработкой инновационных финансовых инструментов, предоставлением кредитной поддержки для развития предприятий, а также осуществляет образовательные программы и исследования в области финансов и инвестиций.

Перекрытия полов и потолков «капитальные» из железобетонных панелей. Имеется деревянный люк на плоскую крышу. Все внутренние двери являются деревянными, филенчатыми полнотелыми. Двери в служебные кабинеты имеют по одному врезному замку. Двери в холлах, коридорах, тамбурах и на лестничных клетках остекленные в верхней половине двери и запорных устройств не имеют.

Все внутренние перегородки и стены (кроме наружных по периметру здания) являются гипсокартонными каркасными или в «кирпич (0,5 кирпича)» «не капитальными».

Двери:

Д1 – Дверь деревянная, полнотелая, филенчатая с одним врезным замком;

Д2 - Дверь деревянная, полнотелая, филенчатая с одним врезным замком;

Окна:

О1 - Окно пластиковое с двойным остеклением без защитных пленок, решетка со стороны помещения размер ячейки 120х150, из прутка D=16мм ;

О2 - Окно пластиковое с двойным остеклением без защитных пленок, решетка со стороны улицы размер ячейки 200х200, из прутка D=12мм;

Экспликация помещений объекта:

1-10 - Служебные кабинеты (Администраторы, техники); 5-Серверная; 9 – Приемная; 12 - Актовый зал; 21 – 29 - Служебные кабинеты; 11,17 –Коридор; 13 – 16,18,19 - Аудитории; 22 – Архив; 20,23 – Санузлы;

**2 СХЕМА ФИЗИЧЕСКОГО УРОВНЯ КОРПОРАТИВНОЙ ЛВС**

Разработка схемы физического уровня осуществлялась в приложении Visio. Использовались различные встроенные инструменты. На данной схеме представлен план помещения с кабинетами, оборудованием и проводкой.

Для построения схемы канального уровня корпоративной ЛВС использовалось 4 сетевых коммутатора Cisco WS-C2960S-24TS-L.

Использовался 1 вид проводки: многожильный медный кабель (Folan U/UTP Cat5e ZH нг(А)-HF 25х2х0,52.

Таблица 1 – Условное обозначение

|  |  |
| --- | --- |
| Условное обозначение | Наименование |
|  | Рабочее место (ПК) |
|  | Сервер |
|  | Коммутатор Cisco 2960 |
|  | Маршрутизатор Cisco 2811 |
|  | Кабель UTP Cat 5e 1x2x0,51 |
|  | Wi-Fi Роутер |



Рисунок 1 – Схема предприятия

**3 СХЕМА КАНАЛЬНОГО УРОВНЯ КОРПОРАТИВНОЙ ЛВС**

На данной схеме представлена сеть канального уровня корпоративной ЛВС, в которой использовалось 5 маршрутизаторов TP-LINK Archer AX53. Так же были установлены 2 Wi-Fi роутера MERCUSYS MR30G AC1200, 1 сервер HPE Proliant DL360 Gen9 для аутентификации через сервис ААА.

Кабель: многожильный медный (Folan U/UTP Cat5e ZH нг(А)-HF)

Таблица 2 – Условное обозначение

|  |  |  |
| --- | --- | --- |
| Условное обозначение | Кол-во | Описание |
|  | 59 | Рабочее место (ПК) |
|  | 1 | Сервер |
|  | 2 | Wi-Fi Роутер |
|  | 4 | Коммутатор |
|  | 5 | Маршрутизатор |
|  | 6 | Ноутбук |

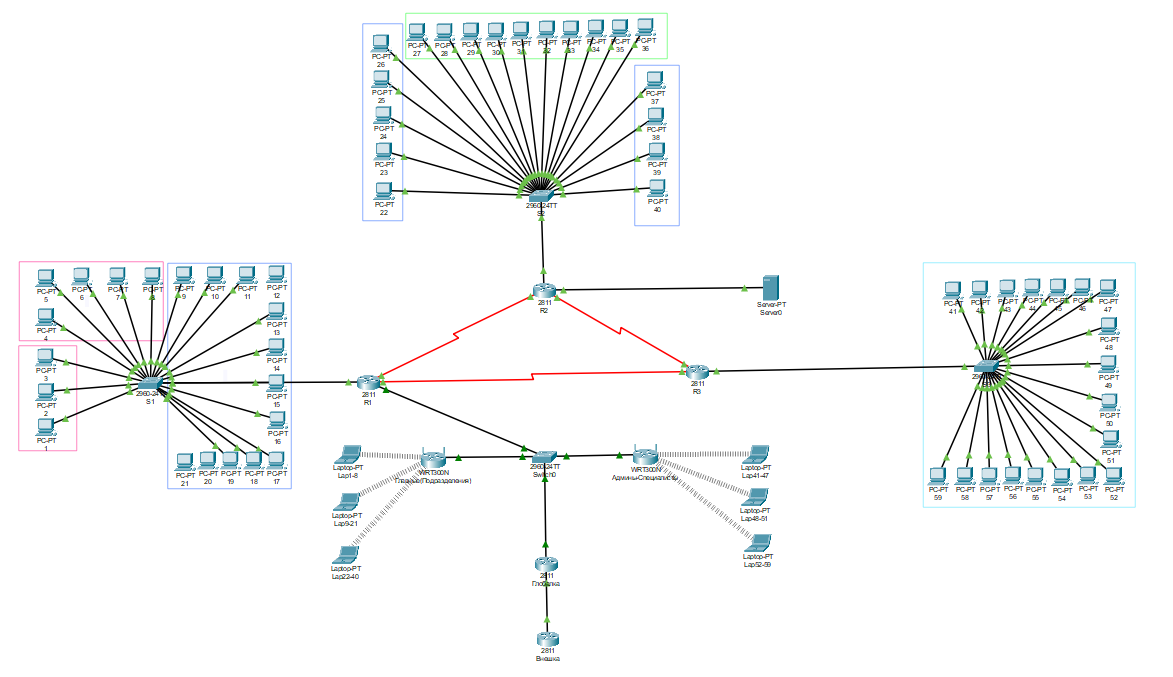


Рисунок 2 – Схема сетевого уровня

**4 РАСПРЕДЕЛЕНИЕ АДРЕСНОГО ПРОСТРАНСТВА**

Таблица 3 – распределения адресного пространства

|  |  |  |
| --- | --- | --- |
| **Адрес сети** | **Наименование** | **Шлюз** |
| 192.168.10.0/24 | Аудитория (1) | 192.168.10.1 |
| 192.168.20.0/24 | Аудитория (2) | 192.168.20.1 |
| 192.168.30.0/24 | Аудитория (3) | 192.168.30.1 |
| 10.1.1.0/30 | R1-R2 | - |
| 10.2.2.0/30 | R2-R3 | - |
| 10.3.3.0/30 | R3-R1 | - |
| 192.168.11.3 | Кабинет №1 (wi-fi) | 192.168.11.2 |
| 192.168.11.4 | Кабинет №2 (wi-fi) | 192.168.11.2 |
| 192.168.80.1 | Server | 192.168.80.2 |

Access list (ACL) в Cisco Packet Tracer используется для фильтрации IP-трафика на маршрутизаторах и коммутаторах. Он позволяет управлять обменом IP-пакетами на основе набора заданных правил.

ACL используется для различных целей, включая:

* Фильтрация трафика: ACL позволяет разрешать или блокировать определенные типы трафика на основе IP-адреса отправителя, IP-адреса получателя, порта и других параметров. Например, вы можете настроить ACL для блокировки доступа к определенным веб-сайтам или для разрешения доступа только определенным устройствам в сети.
* Обеспечение безопасности: ACL используется для защиты сети от нежелательного или вредоносного трафика. Вы можете настроить ACL для блокировки нежелательных IP-адресов, отслеживания попыток несанкционированного доступа или применения других мер безопасности.
* Оптимизация сетевых ресурсов: ACL позволяет оптимизировать использование сетевых ресурсов, например, ограничивая пропускную способность для определенного типа трафика или предоставляя приоритет определенным службам или приложениям.
* Отделение сегментов сети: ACL может использоваться для разделения сегментов сети и предотвращения нежелательного доступа между ними. Например, вы можете настроить ACL, чтобы предотвратить доступ от гостевой сети к ресурсам корпоративной сети.

В своем access-list я использовал метод «разрешено все, что не запрещено». Такой способ обеспечивает безопасность от внешних атак, а также дает корректную работу внутри самого предприятия и обеспечивает стабильную и качественную работу одной подсети с другой. Access-list прописан на роутере, который выходит в глобальную сеть. Это было сделано с той целью, чтобы обезопасить работу предприятия от различных атак, например от DOS или DDOS атак.

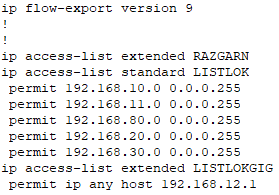


Рисунок 3 – access list

**5 ЭКОНОМИЧЕСКИЙ РАСЧЕТ**

Таблица 4 – Расчет стоимости

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| № | Наименование | Модель, конфигурация | Кол-во | Цена за 1 единицу |
| 1 | ПК | Ryzen 5 5600G, ssd 240, 16gb DDR4, БП 350W, win 10 pro, office 19 business [AMD Radeon Vega 7](https://market.yandex.ru/catalog--nastolnye-kompiutery/26910110/list?hid=91011&glfilter=36036031%3A36427318) | 59 шт. | 32 978  рублей |
| 2 | Ноутбук | Acer Aspire A315-34-C34A Intel Celeron N4020/4Gb/500Gb/Intel UHD/15.6"FHD/DOS (NX. HE3ER.01R) | 6 шт | 27 351  рублей |
| 3 | Сервер | Сервер HPE Proliant DL360 Gen9 8SFF, 2x Intel Xeon E5-2650v4, 384Gb 2400MHz, p440ar, 2x 500W | 1 шт. | 127000  рублей |
| 4 | Маршрутизатор | Маршрутизатор TP-LINK Archer AX53 AX3000 | 4 шт. | 5000  рублей |
| 5 | Wi-Fi Роутер | MERCUSYS MR30G AC1200 | 2 шт. | 4000  рублей |
| 6 | Розетка сетевая | Розетка NA214 RJ-45 кат.5e внешняя 2 порта, 110&Krone, белый | 118 шт. | 300  рублей |
| 7 | Кабель ethernet | Патч корд 10 м Голд Мастер UTP 5е RJ45 интернет кабель 10 метров LAN сетевой Ethernet патчкорд серый (NA102--10M), контакты blade с позолотой 03FU | 118 шт | 300  рублей |
| 8 | Кабель канал | Миниканал Экопласт 25x16 мм 2 м цвет черный | 59 шт | 800 рублей |

**ИТОГ:**

Таблица 5 – сумма вложенных средств

|  |  |  |  |
| --- | --- | --- | --- |
|  | Кол-во | Цена | Сумма |
| ПК | 59 шт. | 32 978 рублей | 1945702 |
| Ноутбук | 6 шт | 27 351 рублей | 164106 |
| Сервер | 1 шт. | 127000 рублей | 127 000 |
| Маршрутизатор | 4 шт. | 5000 рублей | 12 000 |
| Wi-Fi Роутер | 2 шт. | 4000 рублей | 8 000 |
| Розетка сетевая | 118 шт. | 300 рублей | 35400 |
| Кабель ethernet | 118 шт | 300 рублей | 35400 |
| Кабель канал | 59 шт | 32 978 рублей | 47200 |

**ВСЕГО: 2,196,008 рублей.**

Все цены были взяты с сайта: <https://market.yandex.ru/>

**6 ТЕСТИРОВАНИЕ**

Данная модель прошла тестирование и работает корректно. Примеры тестирования приведены ниже.

Как уже упоминалось выше access-list должен блокировать и не пропускать любой не известный трафик на этапе его поступления. Но запросы из локальной сети в глобальную должны проходить. Проверим, возьмем компьютер (ПК №22) и отправим запрос на маршрутизатор провайдера (IP адрес провайдера 192.168.12.1):

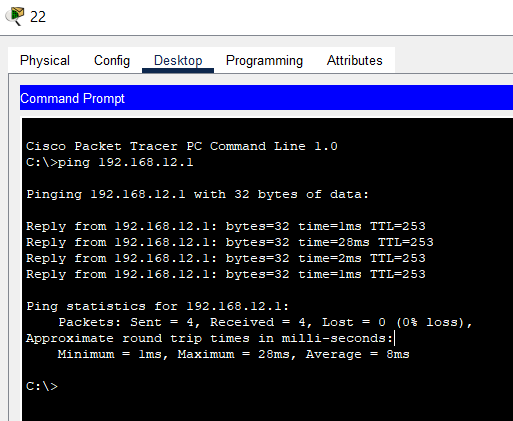


Рисунок 4 – Эхо запрос от руководителя к интернет-провайдеру

Как можно заметить все успешно. Теперь проверим, что будет если запрос будет поступать от интернет-провайдера (Внешка) на компьютер №1 (IP адрес ПК 192.168.10.2):

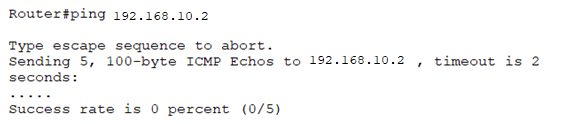


Рисунок 5 – Эхо запрос от интернет-провайдера на компьютер

Эхо запрос не прошел – это значит, что access-list работает корректно.

Проверка протокола AAA для предоставления пользователям безопасного удаленного доступа к сетевому оборудованию. Проверим подключение с помощью telnet с ПК 1 к маршрутизаторам R1, R2, R3.

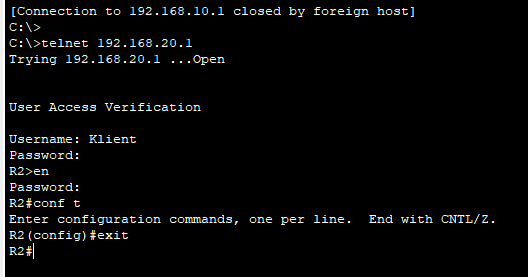


Рисунок 6 – подключение с помощью telnet с ПК 1 к маршрутизаторe R2

Также тест был успешно проведен на маршрутизаторах R1, R3, с IP адресами R1 - 192.168.10.1, R2 - 192.168.20.1, R3 - 192.168.30.1.

Далее посмотрим, как настроены и работают Wi-Fi сети. В данном проекте имеется 2 Wi-fi роутера, Роутер №1 является приватным и предназначен для руководства, администрации и иных сотрудников, Роутер №2 является общедоступным (гостевым) для служебных помещений.

И так, рассмотрим ситуацию, что руководитель или работник хотят подключиться к Wi-fi роутеру, предназначенному для (Админ) с помощью ноутбука (Lap 9-21, IP адрес: 192.168.11.3).

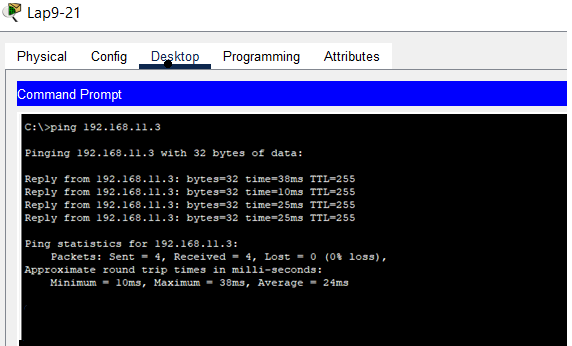


Рисунок 7 – Удачная попытка удаленного подключения сотрудника

Видим, что связи есть.

Теперь представим ситуацию, что администрация или сотрудник подразделения решат подключиться к Wi-fi роутеру гостевому(служебный) (Lap 9-21), к другому роутеру (IP адрес: 192.168.11.4).

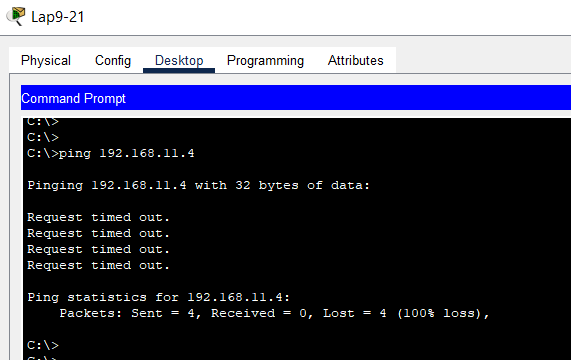


Рисунок 8 – Неудачная попытка удаленного подключения сотрудника

Результат отрицательный, сотрудник не смог подключился.

**ЗАКЛЮЧЕНИЕ**

В ходе выполненной работы мною были решены задачи:

1) Произведен анализ предметной области (включая описание предприятия).

2) Выполнена разработка проекта физического уровня корпоративной ЛВС.

3) Выполнена разработка проекта канального уровня корпоративной ЛВС.

4) Выполнена разработка проекта сетевого уровня корпоративной ЛВС.

5) Произведен экономический расчёт стоимости проекта.

6) Выполнена разработка модели в Cisco Packet Tracer.

7) Произведено экспериментальное исследование модели.

8) Сделана подготовка документации проекта.

В ходе выполнения, работал с такими приложениями, как Microsoft word – для написания отчета по курсовой работе, Microsoft Visio – для разработки физического уровня корпоративной ЛВС, Cisco Packet Tracer – для разработки канального и сетевого уровня корпоративной ЛВС. Для разработки физического уровня корпоративной ЛВС были использованы примеры работ по предмету «УИБ», который был в 6 семестре моего обучения.

В заключение, мною был разработан проект корпоративной ЛВС на базе нескольких информационных технологий. Используя эмулятор сетей Cisco Packet Tracer, разработал модель проектируемой сети.

**СПИСОК ИСПОЛЬЗУЕМЫХ ИСТОЧНИКОВ**

1. Книга В.Олифер “Компьютерные сети. Принципы, технологии, протоколы.” 5-ое издание, 2016 год.
2. Книга Э.Тененбаум, Д.Уэзеролл “Компьютерные сети”, 5-ое издание, 2012 год.
3. <https://www.cisco.com/c/en/us/support/docs/ip/enhanced-interior-gateway-routing-protocol-eigrp/16406-eigrp-toc.html>
4. <https://habr.com/ru/articles/138573/>
5. <https://wiki.merionet.ru/articles/nastrojka-router-on-a-stick-na-cisco/>
6. <https://komrunet.ru/blog/detail/vlan/>
7. <https://vasexperts.ru/blog/tehnologii/autentifikacziya-avtorizacziya-i-uchet-aaa-radius-ili-tacacs/>
8. <https://arny.ru/education/ccna-security/cisco-aaa/>
9. <https://www.vistlan.ru/info/blog/obzory-tovarov/mezhsetevoy-ekran-cisco-asa/>
10. <https://jakondo.ru/bazovaya-nastrojka-cisco-asa-adaptive-security-appliance-5505-sozdanie-vlan-nastrojka-dns-dhcp-route-nat/>
11. <https://wiki.merionet.ru/articles/struktura-korporativnoj-seti/>
12. Книга А.П.Пятибратов, Л.П. Гудыно, А.А. Кириченко “Вычислительные системы, сети и телекоммуникации”, 2-ое издание, 2004 год. Глава 16 – корпоративные вычислительные сети (КВС).
13. <https://habr.com/ru/articles/351564/>
14. <https://market.yandex.ru>
15. <http://wiki.pro-voip.ru/cisco/nastrojka-zonalnyh-mezhsetevyh-jekranov-cisco.html>

**ССЫЛКА НА ПРОЕКТ**