**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\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Е. М. Бирюкова

Владимир 2023

CОДЕРЖАНИЕ

[**1 АНАЛИЗ ПРЕДМЕТНОЙ ОБЛАСТИ (ВКЛЮЧАЯ ОПИСАНИЕ ПРЕДПРИЯТИЯ)** 3](#_Toc154327569)

[**2 РАЗРАБОТКА ПРОЕКТА ФИЗИЧЕСКОГО УРОВНЯ КОРПОРАТИВНОЙ ЛВС** 10](#_Toc154327570)

[**3 РАЗРАБОТКА ПРОЕКТА КАНАЛЬНОГО УРОВНЯ КОРПОРАТИВНОЙ ЛВС** 12](#_Toc154327571)

[**4 РАЗРАБОТКА ПРОЕКТА СЕТЕВОГО УРОВНЯ КОРПОРАТИВНОЙ ЛВС** 12](#_Toc154327572)

[**5 РАСЧЕТ СТОИМОСТИ ПРОЕКТА** 15](#_Toc154327573)

[**6 РАЗРАБОТКА МОДЕЛИ КОРПОРАТИВНОЙ ЛВС В CISCO PACKET TRACER** 16](#_Toc154327574)

[**7 ЭКСПЕРИМЕНТАЛЬНОЕ ИССЛЕДОВАНИЯ МОДЕЛИ** 20](#_Toc154327575)

[**ЗАКЛЮЧЕНИЕ** 25](#_Toc154327576)

[**СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ** 26](#_Toc154327577)

# **1 АНАЛИЗ ПРЕДМЕТНОЙ ОБЛАСТИ (ВКЛЮЧАЯ ОПИСАНИЕ ПРЕДПРИЯТИЯ)**

Локальная вычислительная сеть (ЛВС, локальная сеть; англ. Local Area Network,LAN)  представляет  собой  систему распределённой обработки данных, охватывающую небольшую территорию (диаметром до 10 км) внутри учреждений, НИИ, вузов, банков и т.п., это система взаимосвязанных и распределённых на фиксированной территории средств передачи и обработки информации, ориентированных на коллективное использование общесетевых ресурсов - аппаратных, информационных, программных.

В обобщённой структуре ЛВС выделяют совокупность абонентских узлов, или систем, серверов и коммуникационной подсети (КП). Основными компонентами сети являются кабели (передающие среды), рабочие станции (АРМ пользователей сети), платы интерфейса сети (сетевые адаптеры), серверы сети. Серверы сети - это аппаратно-программные системы, выполняющие функции управления распределением сетевых ресурсов общего доступа, которые могут работать и как обычная абонентская система. В ЛВС может быть несколько различных серверов для управления сетевыми ресурсами, однако всегда имеется один (или более) файл-сервер (сервер БД) для управления внешними ЗУ общего доступа и организации распределённых БД (РБД).

Основные характеристики ЛВС:

1. территориальная протяжённость сети;

2. максимальная скорость передачи данных;

3. максимально возможное расстояние между рабочими станциями в сети;

4. топология сети;

5. вид физической передачи данных;

6. максимальное число каналов передачи данных;

7. тип передачи сигналов (синхронный или асинхронный);

8. метод доступа абонентов в сети;

9. структура ПО сети;

10. возможность передачи речи и видеосигналов;

11. условия надёжной работы сети.

К наиболее типичным областям применения ЛВС относятся следующие:

• обработка текстов;

• организация собственных информационных систем;

• обмен информацией между АС сети;

• обеспечение распределённой обработки данных;

• поддержка принятия управленческих решений;

• организация электронной почты;

• коллективное использование дорогостоящих ресурсов.

Типы ЛВС.

Для деления на группы используются определённые классификационные признаки.

По назначению ЛВС делятся на информационные (информационно-поисковые), управляющие (технологическими, административными, организационными и другими процессами), расчётные, информационно-расчётные и др.

По типам используемых в сети ЭВМ можно разделить на неоднородные, где применяются различные классы (микро-, мини-, большие) и модели (внутри классов), ЭВМ, а также различное абонентское оборудование, и однородные, содержащие одинаковые модели ЭВМ и однотипный состав абонентских средств.

По организации управления однородные ЛВС различаются на сети с централизованным и децентрализованным управлением.

По топологии, т.е. конфигурации элементов в сети ЛВС делятся: на общую шину, кольцо, звезду и др.

Типичными методами доступа к передающей среде в современных ЛВС являются:

1.множественный доступ с контролем несущей и обнаружением конфликтов (CSMA/CD), иначе называемый методом доступа Ethernet. Используется в ЛВС с шинной топологией, обеспечивает высокую скорость передачи данных и надёжность.

2.маркерное кольцо (метод доступа  Token  Ring). Рассчитан на кольцевую топологию сети. Это селективный метод доступа в кольцевой моноканал, именуемый «маркерное кольцо». В качестве маркера используется уникальная последовательность битов. Маркер не имеет адреса и может находиться в одном из двух состояний: свободен или занят.

3.маркерная шина (метод доступа  Arcnet). Используется в ЛВС с топологий «звезда» и «общая шина». Это селективный метод доступа в моноканал, называемый «маркерная шина». Маркер создается одной из станций сети и имеет адресное поле, где указывается номер (адрес) станции, владеющий маркером. Передачу производит только та станция, которая в данный момент владеет маркером (эстафетной палочкой).

В отличие от протоколов нижнего уровня, обеспечивающих доступ к передающей среде, протоколы верхнего уровня (называемые также протоколами среднего уровня, так как они реализуются на 4-м и 5- уровнях модели ВОС) служат для обмена данными. Они предоставляют программам интерфейс для передачи данных методом дейтаграмм, когда пакеты адресуются и передаются без подтверждения получения, и методом сеансов связи, когда устанавливается логическая связь между взаимодействующими станциями (источником и адресатом) и доставка сообщений подтверждается.

Программное обеспечение ЛВС.

ПО ЛВС имеет иерархическую структуру, соответствующую семиуровневой модели ВОС. Это существенно облегчает задачу стандартизации ПО в соответствии с общепринятыми протоколами. Известно, что основная задача ЛВС - обеспечение функционирования прикладных процессов, реализуемых АС сети. Выполнение прикладных процессов обеспечивается средствами прикладных программ сети (ППС), которые реализуют протоколы верхнего (прикладного) уровня модели ВОС и соответственно образуют верхний уровень программной структуры ЛВС. Выполнение процессов взаимодействия, с помощью которых осуществляется передача данных между прикладными процессами различных АС, производится средствами сетевых операционных систем (СОС), а также аппаратными средствами сети. Обычно программы СОС локальных сетей реализуют протоколы трёх верхних уровней модели ВОС: прикладного уровня (вместе с ППС), представительного и сеансового. Протоколы нижних 4-х уровней (транспортного, сетевого, канального и физического), как правило, реализуются аппаратными средствами (сетевым адаптером), но в принципе процедуры этих уровней (кроме физического) могут быть реализованы программными средствами СОС.

Функционирование ЛВС.

На эффективность функционирования ЛВС оказывают влияние следующие основные факторы:

• уровень квалификации пользователей сети;

• качество и возможности СОС, особенно такие, как разнообразие и удобство административных средств для управления сетью и работы пользователей, использование общесетевых ресурсов;

• топология сети и используемые в ней протоколы передачи данных;

• количество и возможности аппаратного обеспечения сети;

• количество АС в сети, степень их активности, технология работы пользователей, время на удовлетворение запросов пользователей;

• объём и технология использования информационного обеспечения (БД и БЗ);

• перечень предоставляемых услуг и их интеллектуальный уровень;

• средства и методы защиты информации в сети;

• средства и методы обеспечения отказоустойчивости ЛВС;

• используемые режимы функционирования сети.

Важным фактором в обеспечении высокой эффективности функционирования ЛВС является организация распределённой базы данных (РБД), предоставляющей собой логически единую базу данных, отдельные физические части которой размещены на несколько ЭВМ сети.

Характеристики основных ЛВС.

Наибольший интерес представляют те ЛВС, которые получили широкое распространение, в том числе и в России. К их числу относят: Ethernet, Arcnet, Token Ring, PC Network, Cluster/One, PLAN 4000 и др. Основные характеристики первых трёх сетей указаны в таблице (рисунок 1).

Рисунок 1-Характеристики ЛВС

Обозначения: ВП — витая пара;

КК - коаксиальный кабель;

ВОЛС - волоконно-оптическая линия связи;

ПК - персональный компьютер.

**Адресация.**

IP-адресация – это система присвоения уникальных идентификаторов устройствам в сети Интернет. IP-адрес (Internet Protocol Address) – это числовой адрес, который используется для идентификации и маршрутизации пакетов данных в сети.

IP-адрес состоит из 4 чисел, разделенных точками, например, 192.168.0.1. Каждое число может принимать значения от 0 до 255. Такая форма записи IP-адреса называется IPv4 (Internet Protocol version 4).

IP-адресация позволяет устройствам в сети обмениваться данными, определять источник и назначение пакетов, а также находить оптимальные пути для доставки данных.

IP-адресация может быть статической или динамической. В статической адресации IP-адрес назначается вручную администратором сети и остается неизменным. В динамической адресации IP-адрес назначается автоматически с помощью протокола DHCP (Dynamic Host Configuration Protocol).

IP-адресация является основой для работы сети Интернет и позволяет устройствам в сети обмениваться данными, обеспечивая их доставку и маршрутизацию.

Статическая и динамическая адресация – это два различных подхода к присвоению IP-адресов устройствам в сети.

Статическая адресация

Статическая адресация означает, что IP-адрес устройства назначается вручную и остается постоянным. При статической адресации администратор сети вручную назначает каждому устройству уникальный IP-адрес. Этот адрес не меняется, пока его не изменит администратор.

Преимуществом статической адресации является стабильность и предсказуемость адресов. Это позволяет легко управлять сетью и настраивать доступ к устройствам. Однако, недостатком статической адресации является необходимость вручную настраивать каждое устройство, что может быть трудоемким и затратным процессом, особенно в больших сетях.

Динамическая адресация

Динамическая адресация означает, что IP-адрес устройства назначается автоматически с использованием протокола DHCP (Dynamic Host Configuration Protocol). При динамической адресации существует DHCP-сервер, который автоматически назначает IP-адрес устройствам в сети.

Преимуществом динамической адресации является автоматическое назначение и управление IP-адресами. Это упрощает процесс настройки и управления сетью, особенно в больших сетях. Кроме того, динамическая адресация позволяет эффективно использовать доступные IP-адреса, так как адреса могут быть переиспользованы, когда устройство покидает сеть или выключается.

Недостатком динамической адресации является то, что IP-адрес устройства может изменяться со временем. Это может создавать проблемы, если устройство требует постоянного доступа по определенному IP-адресу. Однако, эту проблему можно решить с помощью использования статического IP-адреса для таких устройств.

**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:

* С помощью использования интернет-провайдера;
* 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.**

Рассмотрим корпоративную сеть на примере юридической коммерческой организации ООО “*ЮрКомВ*”. Организация осуществляет прием посетителей, в помещениях всегда многолюдно. В здании подвал, первые два этажа и смежные помещения занимают (арендуют) прочие «не охраняемые» собственники. Перекрытия полов и потолков «капитальные» из железобетонных панелей. Имеется деревянный люк на плоскую крышу, чердака нет.

Все внутренние двери являются деревянными, филенчатыми полнотелыми. Двери в служебные кабинеты и бухгалтерию, кассу, архив, канцелярию, серверную, пост охраны и др. имеют по одному врезному замку. Двери в холлах, коридорах, тамбурах 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». Во всех служебных кабинетах имеются персональные компьютеры, на складах дорогостоящие материальные ценности.

В помещениях кассы и 2 установлены сейфы весом по 150-200 кг без крепления к полу и стенам.

Кабинет 2 – защищаемое режимное помещение, с хранением информации, составляющей служебную тайну.

**Двери:**

Д1 – Дверь пластиковая полнотелая с одним врезным замком;

Решетчатые раздвижные двери в помещениях отсутствуют.

**Окна:**

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

О2 - Окно с деревянными рамами с двойным остеклением без защитных пленок, решетки отсутствуют.

Экспликация помещений объекта:

1-Приемная; 1а-кабинет начальника; 2- Канцелярия; 3-5 – Служебные кабинеты; 6-Служебный кабинет; 6а-Склад; 6б-Архив; 7 – Служебные кабинеты; 7а-Отдел кадров; 8 – Бухгалтерия; 9-10 – Служебный кабинет; 11 – Пост охраны; 12 – Коридор; 13 –Лестничная клетка; 14 – Санузлы; 15 - Служебный кабинет; 16-Серверная.

# **2 РАЗРАБОТКА ПРОЕКТА 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.

Таблица 1-Условные обозначения

|  |  |
| --- | --- |
| Условное обозначение | Наименование |
|  | Рабочее место (ПК) |
|  | Сервер |
|  | Коммутатор Cisco 2960 |
|  | Маршрутизатор Cisco 2621XM |
|  | Кабель Голд Мастер UTP 5е RJ45 интернет кабель LAN сетевой Ethernet патчкорд |
|  | Hyperline,U/UTP, cat 5e 4х2х24AWG |
|  | Wi-Fi Роутер |

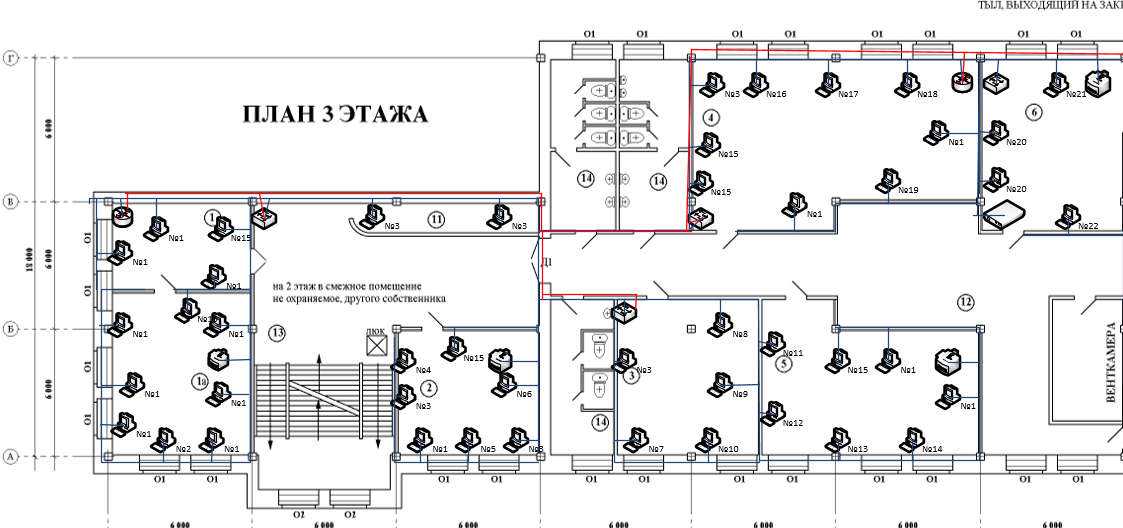
****

Рисунок 2-Схема предприятия физического/канального уровня (часть 1)

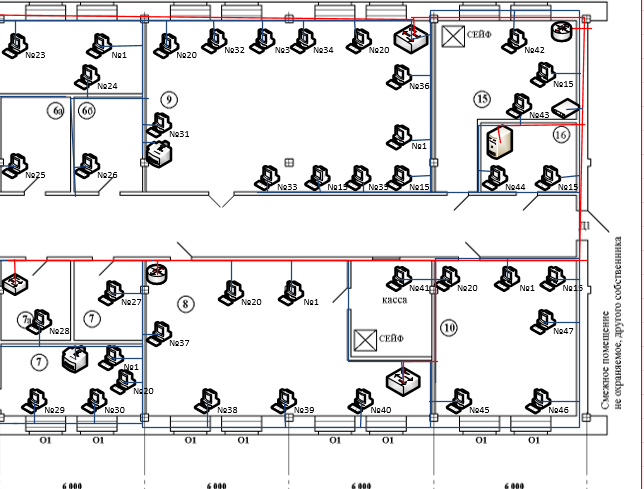
****

Рисунок 3-Схема предприятия физического/канального уровня (часть 2)

# **3 РАЗРАБОТКА ПРОЕКТА КАНАЛЬНОГО УРОВНЯ КОРПОРАТИВНОЙ ЛВС**

Для построения схемы канального уровня корпоративной ЛВС использовалось 7 сетевых коммутаторов Cisco WS-C2960S-24TS-L. Использовалось 2 вида проводки: Кабель Ethernet (Кабель Голд Мастер UTP 5е RJ45 интернет кабель LAN сетевой Ethernet патчкорд), Витая пара (Hyperline,U/UTP, cat 5e 4х2х24AWG).

На схеме данного уровня представлена сеть спроектированная в Visio (рисунок 1,2), в которой имеется разделение на Vlan. VLAN – это технология, которая дает возможность выстроить такую виртуальную сеть, которая будет независима от физических устройств. С ее помощью сотрудники, работающие в разных зданиях, могут подключаться к порту одного коммутатора или сразу к нескольким. По сути, это виртуальная локальная сеть, которая выглядит как группа хостов, взаимодействующих так, словно они подключены к широковещательному домену. VLAN обладает теми же свойствами, что и классическая физическая локальная сеть, но при этом дает возможность объединять устройства, не имея прямого физического доступа.

Таблица 2 –Количество оборудования

|  |  |  |
| --- | --- | --- |
|  | | |
| Условное обозначение | Кол-во | Описание |
|  | 71 | Рабочее место (ПК) |
|  | 7 | Коммутатор |
|  | 6 | Маршрутизатор |
|  | 2 | Wifi |
|  | 1 | Сервер |

# **4 РАЗРАБОТКА ПРОЕКТА СЕТЕВОГО УРОВНЯ КОРПОРАТИВНОЙ ЛВС**

На схеме данного уровня представлена сеть, которая так же спроектированная в Cisco Packet Tracer. Для разработки схемы было использовано 4 маршрутизатора Cisco 2621MX. Так же были установлены 2 Wi-Fi роутера TP-Link TL-WR841N 10/100BASE-TX, СЕРВЕР DELL R550 16SFF для аутентификации через сервис ААА.

Таблица 3 -Распределение адресного пространства

|  |  |  |
| --- | --- | --- |
| **Сегмент сети** | **Структурное подразделение** | **Шлюз** |
| **192.168.1.0/24** | Приемная, кабинет начальника, канцелярия, пост охраны | 192.168.1.20 |
| **192.168.2.0/24** | Служебные кабинеты | 192.168.2.30 |
| **192.168.3.0/24** | Служебный кабинет, архив, склад | 192.168.3.50 |
| **192.168.4.0/24** | Служебный кабинет, отдел кадров | 192.168.4.60 |
| **192.168.5.0/24** | Служебные кабинеты, северная | 192.168.5.70 |
| **192.168.6.0/24** | Бухгалтерия, служебный кабинет | 192.168.6.80 |

Таблица 4 -Условные обозначения

|  |  |  |
| --- | --- | --- |
|  | | |
| Условное обозначение | Кол-во | Описание |
|  | 71 | Рабочее место (ПК) |
|  | 1 | Сервер |
|  | 2 | Wi-Fi Роутер |
|  | 7 | Коммутатор |
|  | 6 | Маршрутизатор |
|  | 6 | Ноутбук |

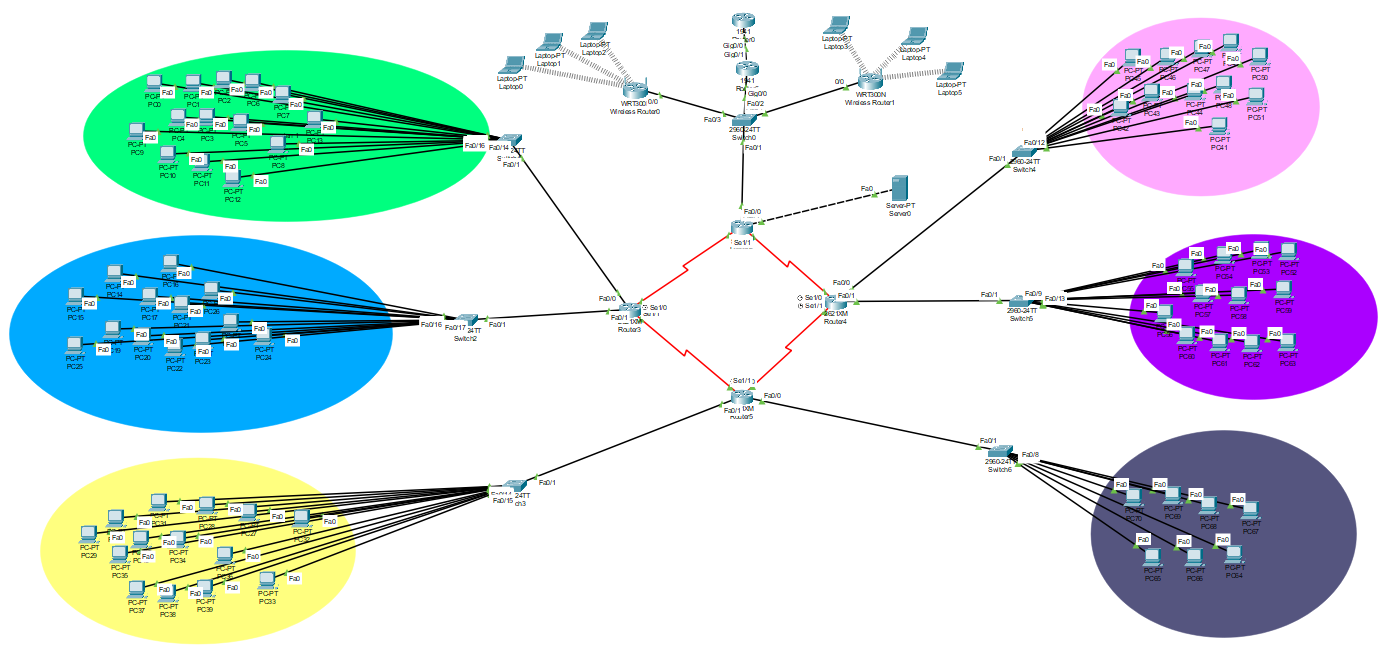
****

Рисунок 4-Схема предприятия сетевого уровня

# **5 РАСЧЕТ СТОИМОСТИ ПРОЕКТА**

Таблица 5 -Расчет стоимости

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| № | Наименование | Модель,конфигурация | Кол-во | Цена за 1 единицу |
| 1 | ПК | DELL Optiplex 5000 | 71 шт. | 85000  рублей |
| 2 | Сервер | DELL R550 16SFF | 1 шт. | 524 958 рублей |
| 3 | Маршрутизатор | MikroTik RB5009UG+S+IN | 6 шт. | 28000  рублей |
| 4 | Wi-Fi Роутер | TP-Link TL-WR841N 10/100BASE-TX | 2 шт. | 2000  рублей |
| 5 | Коммутатор | D-Link DGS-1250-52X | 7 шт. | 32000  рублей |
| 7 | Розетка 1 | DiXiS 2 Gang Socket с портами 2 USB / 2 Type-C | 71 шт. | 2000  рублей |
| 8 | Розетка 2 | Legrand Etika | 71 шт. | 220  рублей |
| 9 | Проводка 1 | Кабель Голд Мастер UTP 5е RJ45 интернет кабель LAN сетевой Ethernet патчкорд | 120 м. | 900  рублей |
| 10 | Проводка 2 | Hyperline,U/UTP, cat 5e 4х2х24AWG | 200 м. | 2000  рублей |

**ИТОГ:**

ПК: 71\*85 000 = 6 035 000 рублей

Сервер: 1\*524 958 = 524 958 рублей

Маршрутизатор: 6\*28 000 = 168 000 рублей

Wi-Fi Роутер: 2\*2000 = 4000 рублей

Коммутатор: 7\*32 000 = 224 000 рублей

Розетка 1: 71\*2000 = 142 000 рублей

Розетка 2: 71\*220 = 15 620 рублей

Проводка 1: 24\*900 = 21 600 рублей

Проводка 2: 4\*2000 = 8 000 рублей

**ВСЕГО: 7 143 178 рублей.**

Все цены были взяты с сайтов: <https://market.yandex.ru/> и <https://www.citilink.ru>.

# **6 РАЗРАБОТКА МОДЕЛИ КОРПОРАТИВНОЙ ЛВС В CISCO PACKET TRACER**

При разработке модели корпоративной ЛВС использовалось приложение Cisco Packet Tracer.

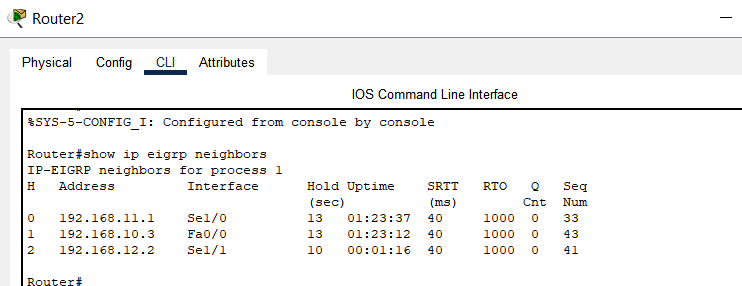
**Соседство между маршрутизаторами:**

Рисунок 5- IP адреса маршрутизатора №1 (R2), составляющих соседство

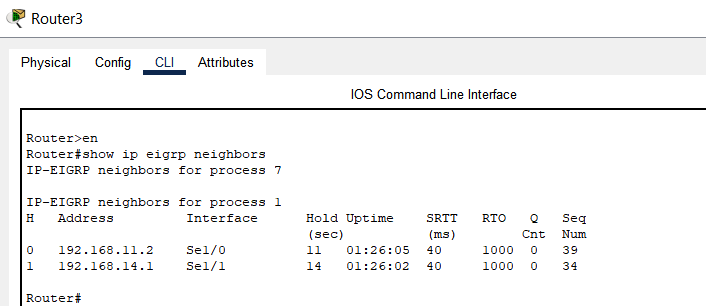


Рисунок 6- IP адреса маршрутизатора №2 (R3), составляющих соседство

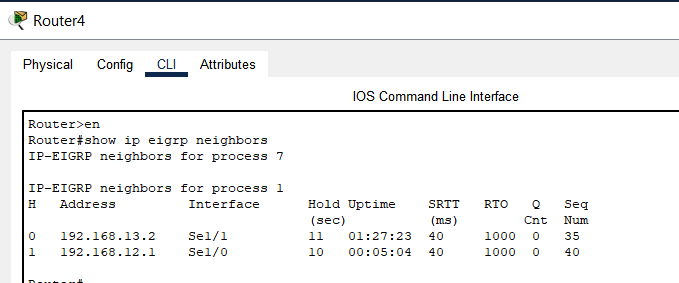


Рисунок 7-IP адреса маршрутизатора №3 (R4), составляющих соседство

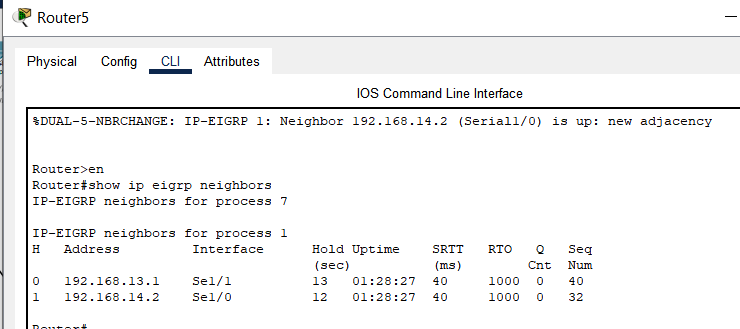


Рисунок 8-IP адреса маршрутизатора №4 (R5), составляющих соседство

**Созданные Vlan-ы и их принадлежность к интерфейсам на коммутаторах:**

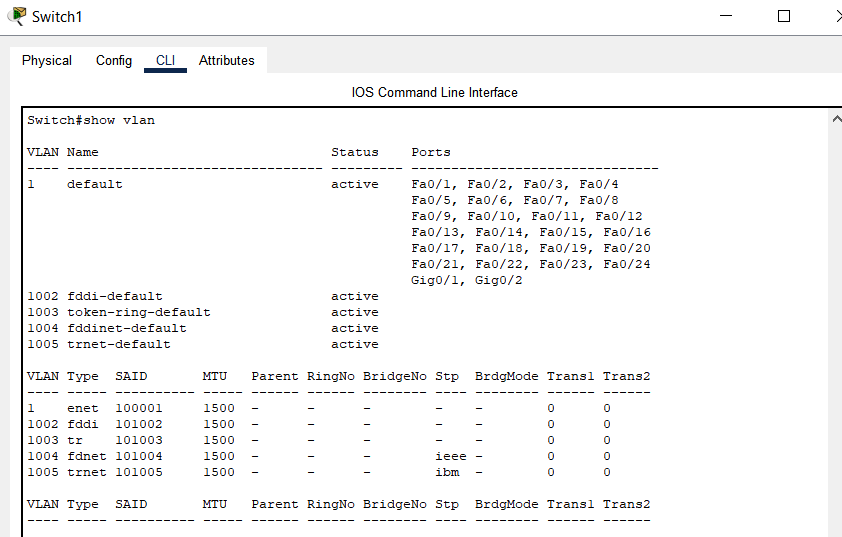


Рисунок 9-Vlan 1 и принадлежащие им интерфейсы на коммутаторе №1 (S1)

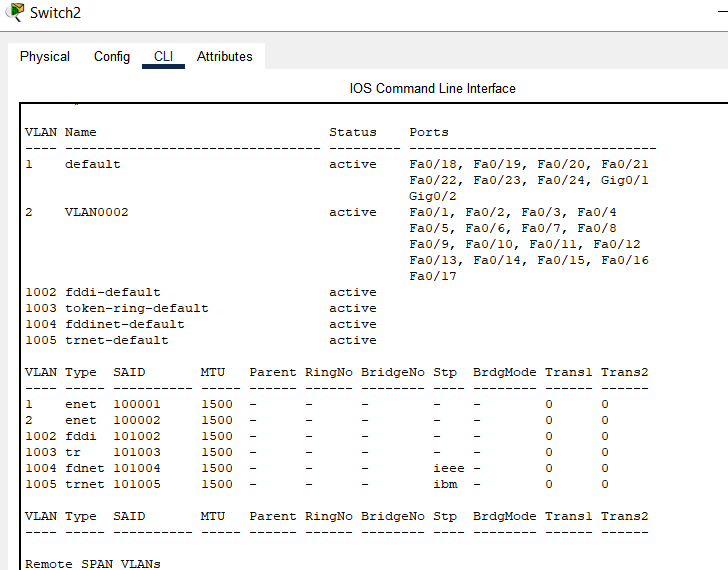


Рисунок 10-Vlan 2 и принадлежащие им интерфейсы на коммутаторе №2 (S2)

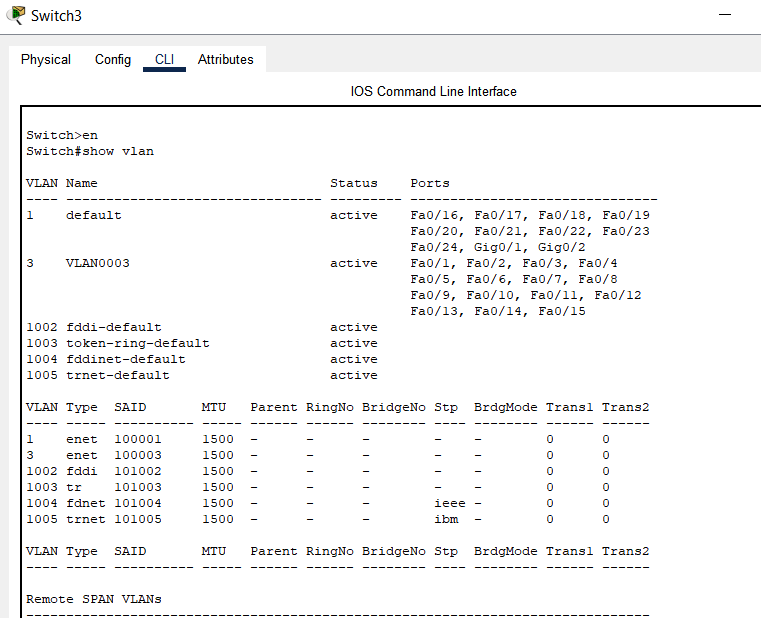


Рисунок 11-Vlan 3 и принадлежащие им интерфейсы на коммутаторе №3 (S3)

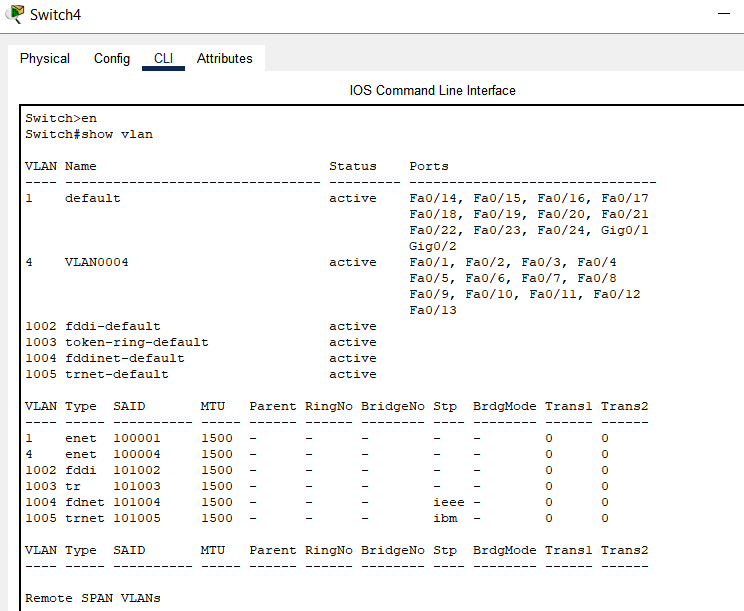


Рисунок 12-Vlan 4 и принадлежащие им интерфейсы на коммутаторе №4 (S4)

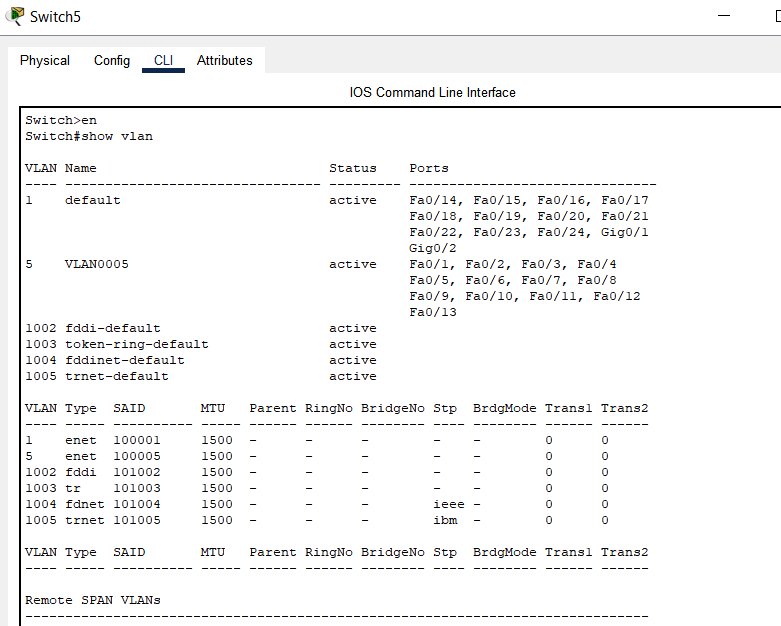


Рисунок 13-Vlan 5 и принадлежащие им интерфейсы на коммутаторе №5 (S5)

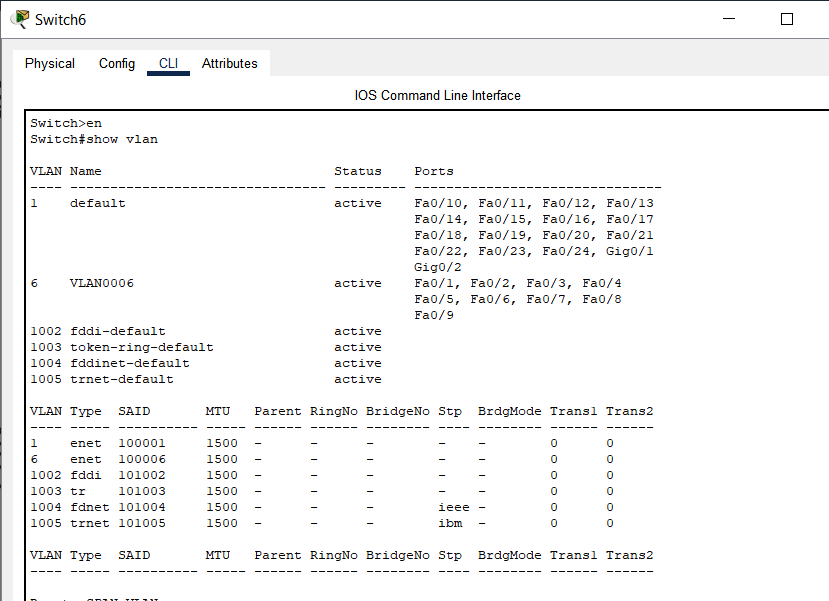


Рисунок 14-Vlan 6 и принадлежащие им интерфейсы на коммутаторе №6 (S6)

**Сервис AAA для внутренней безопасности предприятия:**

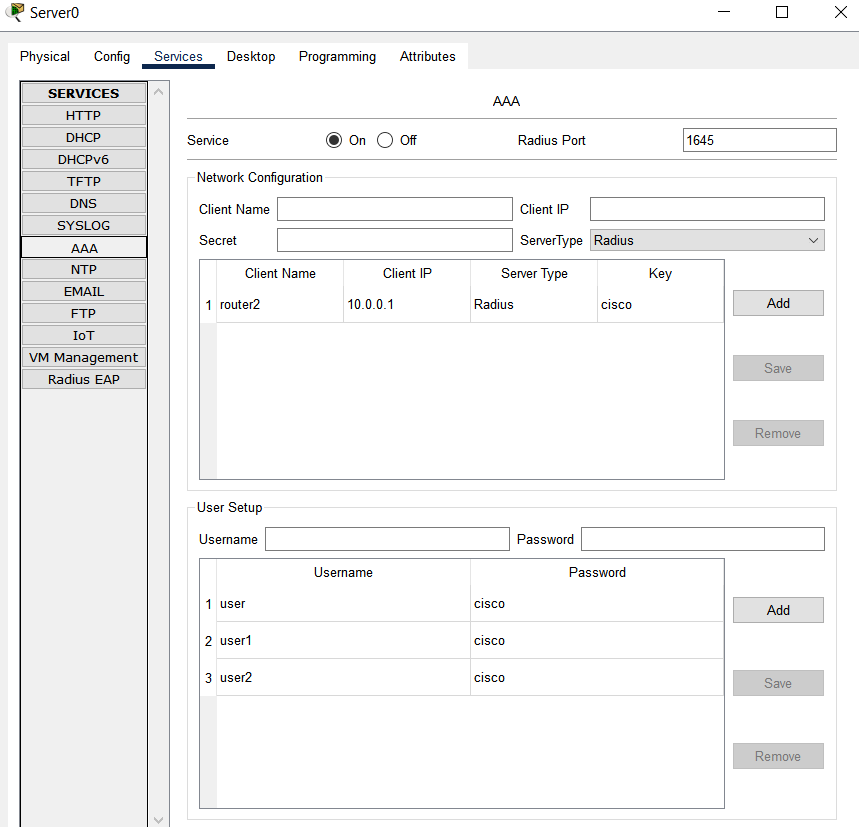


Рисунок 15-Логины и пароли, которые хранятся на сервере №1 (Server0)

# **7 ЭКСПЕРИМЕНТАЛЬНОЕ ИССЛЕДОВАНИЯ МОДЕЛИ**

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

Роутер 2 не должен пропускать любой не известный трафик на этапе его поступления. Но запросы из локальной сети в глобальную должны проходить. Проверим, возьмем компьютер руководителя (ПК 1) и отправим запрос на маршрутизатор провайдера:

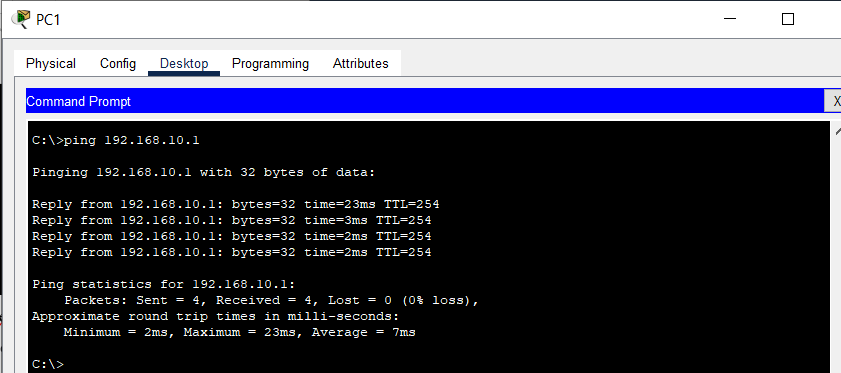


Рисунок 16-Эхо запрос от руководителя к интернет-провайдеру

Как можно заметить все успешно. Теперь проверим, что будет если запрос будет поступать от интернет-провайдера на компьютер руководителя (IP адрес руководителя 192.168.1.1):

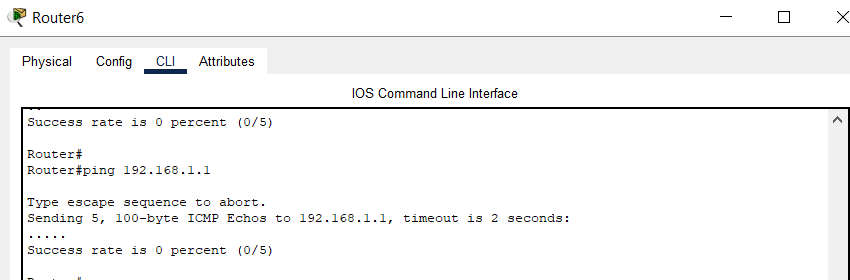


Рисунок 17-Эхо запрос от интернет-провайдера на компьютер руководителя

Эхо запрос не прошел – это значит, что все работает корректно.

Далее проверим удаленное подключение. Представим, что кто-то из соседнего отдела хочет удаленно подключится к шлюзу компьютера руководителя (IP адрес шлюза 10.0.0.1) и получить доступ к маршрутизатору №2 (R2).

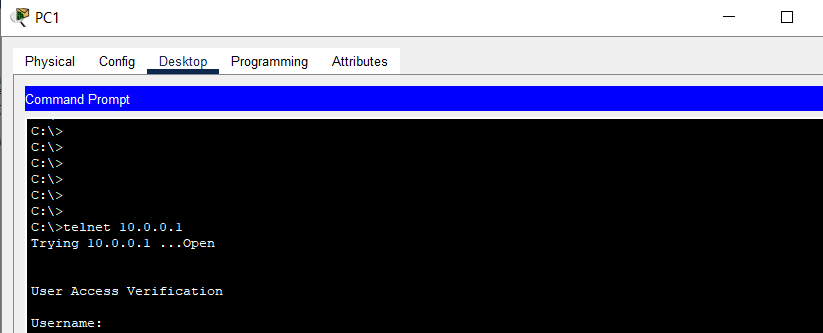


Рисунок 18-Удаленное подключение к шлюзу компьютера руководителя

Видим, что подключение произошло, но у нас запрашивается логин и пароль. У противника есть 5 секунд чтобы ввести логин и пароль иначе оборвется соединение. (Рисунок 17)

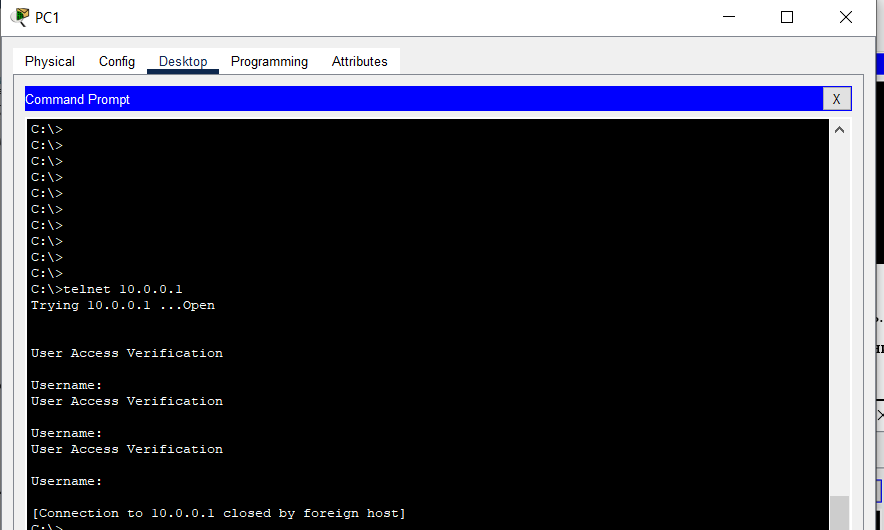


Рисунок 19-Обрыв удаленного подключения через telnet

Теперь введем корректно логин и пароль и посмотрим, что получится.

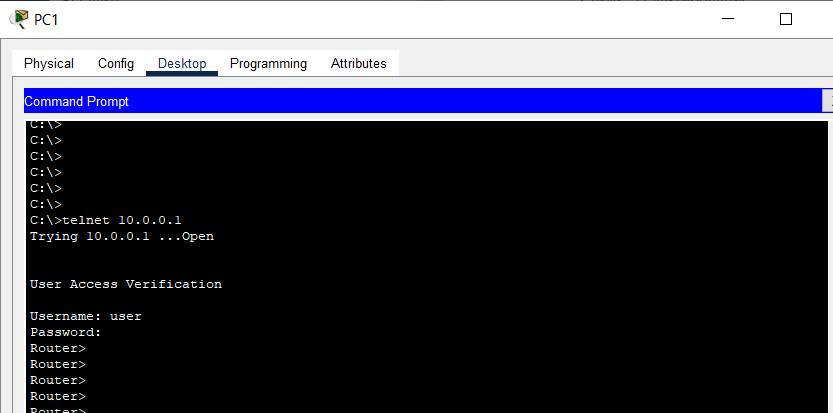


Рисунок 20-Успешное удаленное соединение

Как можно заметить, все прошло успешно, и противник может получить доступ к маршрутизатору, только зная логин и пароль, которые хранятся на сервере.

Далее посмотрим, как настроены и работают Wi-Fi сети. В данном проекте имеется 2 Wi-fi роутера, Роутер №1 являются приватными и предназначены для сотрудников, роутер №0 является общедоступным (гостевым). При этом доступ к LAN для гостей ограничен, то есть устройство, подключенное к гостевому Wi-fi не имеет доступа к локальной сети предприятия.

Посмотрим, что будет если противник подключится к гостевой сети с помощью ноутбука и захочет зайти в локальную сеть предприятия подключившись удаленно к шлюзу компьютера руководителя.

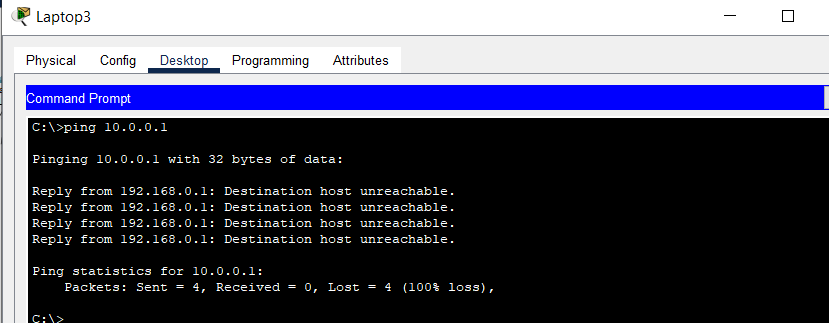


Рисунок 21-Неудачная попытка удаленного подключения противника в локальную сеть

Видим, что связи нет. А это значит, что настройки выполнены корректно.

Теперь проверим имеется ли связь между Vlan-ами. Отправим эхо запросы с компьютера руководителя (ПК №1), сотрудникам находящимся в других Vlan.

Как можно увидеть на скринах ниже, связь со всеми Vlan-ами имеется, эхо запросы проходят успешно, потери минимальные.

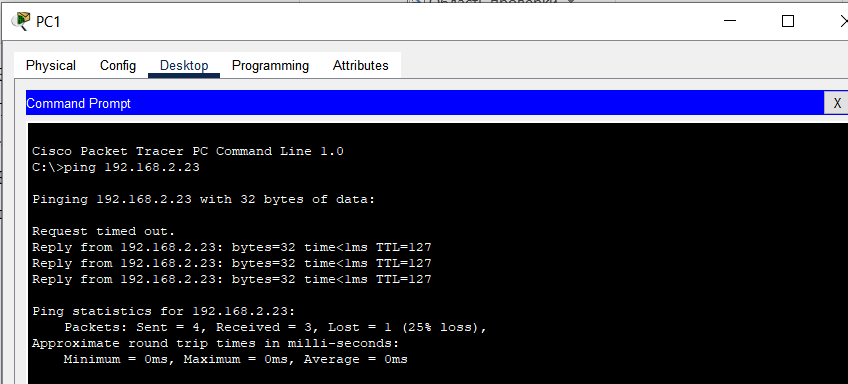


Рисунок 22-эхо запрос на компьютер №23 находящийся в Vlan2

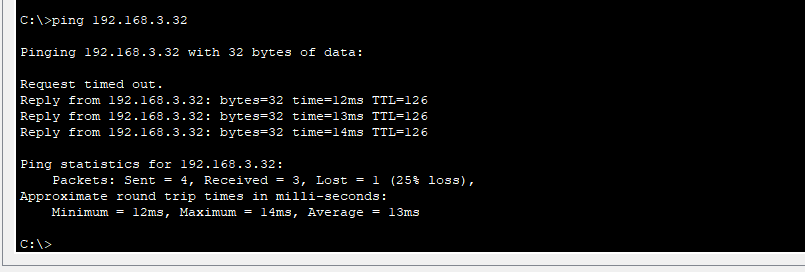


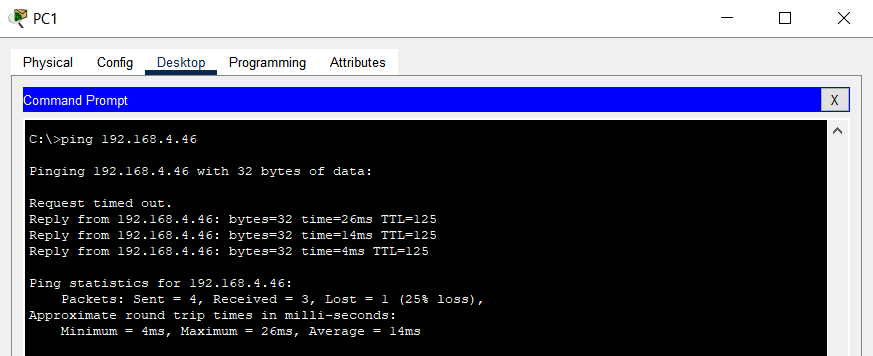
Рисунок 23-эхо запрос на компьютер №32 находящийся в Vlan3

Рисунок 24-эхо запрос на компьютер №46 находящийся в Vlan4

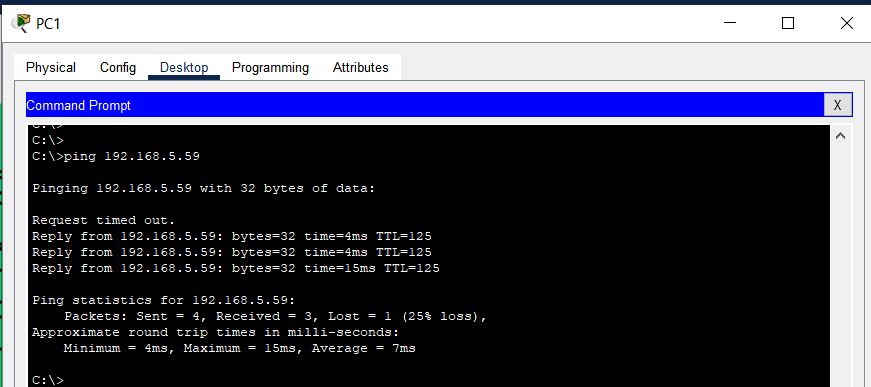


Рисунок 25-эхо запрос на компьютер №59 находящийся в Vlan5

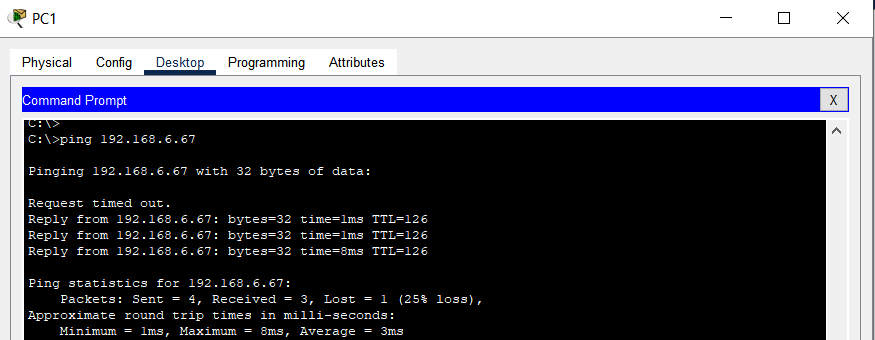


Рисунок 26-эхо запрос на компьютер №67 находящийся в Vlan6

# **ЗАКЛЮЧЕНИЕ**

В ходе курсовой работы мною был разработан проект корпоративной ЛВС. Используя эмулятор сетей Cisco Packet Tracer, была разработана модель проектируемой сети. Также были выполнены следующие задачи:

1) Анализ предметной области (включая описание предприятия).

2) Разработан проект физического уровня корпоративной ЛВС.

3) Разработан проект канального уровня корпоративной ЛВС.

4) Разработан проект сетевого уровня корпоративной ЛВС.

5) Произведен расчёт стоимости проекта.

6) Разработана модель в Cisco Packet Tracer.

7) Проведено экспериментальное исследование модели.

8) Подготовлена документация проекта.

# **СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ**

1. Книга В.Олифер “Компьютерные сети. Принципы, технологии,

протоколы.” 5-ое издание, 2016 год.

1. Книга Э.Тененбаум, Д.Уэзеролл “Компьютерные сети”, 5-ое издание,

2012 год.

1. <https://www.cisco.com/c/en/us/support/docs/ip/enhanced-interior-gateway-routing-protocol-eigrp/16406-eigrp-toc.html>
2. <https://habr.com/ru/articles/138573/>
3. <https://wiki.merionet.ru/articles/nastrojka-router-on-a-stick-na-cisco/>
4. <https://komrunet.ru/blog/detail/vlan/>
5. <https://vasexperts.ru/blog/tehnologii/autentifikacziya-avtorizacziya-i-uchet-aaa-radius-ili-tacacs/>
6. <https://arny.ru/education/ccna-security/cisco-aaa/>
7. <https://www.vistlan.ru/info/blog/obzory-tovarov/mezhsetevoy-ekran-cisco-asa/>
8. <https://jakondo.ru/bazovaya-nastrojka-cisco-asa-adaptive-security-appliance-5505-sozdanie-vlan-nastrojka-dns-dhcp-route-nat/>
9. <https://wiki.merionet.ru/articles/struktura-korporativnoj-seti/>
10. 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).
11. <https://habr.com/ru/articles/351564/>
12. <https://market.yandex.ru>
13. <http://wiki.pro-voip.ru/cisco/nastrojka-zonalnyh-mezhsetevyh-jekranov-cisco.html>

# **ССЫЛКА НА ПРОЕКТ**