Некоммерческое акционерное общество

АЛМАТИНСКИЙ УНИВЕРСИТЕТ ЭНЕРГЕТИКИ И СВЯЗИ ИМЕНИ ГУМАРБЕКА ДАУКЕЕВА

Кафедра телекоммуникаций и инновационных технологий

Современные методы измерений в телекоммуникациях

Методические указания к выполнению лабораторных работ
для магистрантов по образовательной программе
7М06201 – «Радиотехника, электроника и телекоммуникации»
Направление «Телекоммуникации»

Алматы 2022

СОСТАВИТЕЛИ: К.С. Чежимбаева. Современные методы измерений в телекоммуникациях. Методические указания к выполнению лабораторных работ для магистрантов по образовательной программе 7М06201 – «Радиотехника, электроника и телекоммуникации». Направление «Телекоммуникации. – Алматы: АУЭС, 2022. – 95 с.

Методические указания содержат материалы по подготовке и выполнению лабораторных работ с применением пакета моделирования по программе Cisco Packet Tracer. В методических указаниях дано описание экспериментов и приведены методика проведения и обработки опытных данных, перечень рекомендуемой литературы и контрольные вопросы.

Методические указания предназначены для магистрантов в онлайн режиме специальностей по образовательной программе 7М06201 – «Радиотехника, электроника и телекоммуникации». Направление «Телекоммуникации.

Ил. 22 , табл.7 , библиогр. – 7 назв.

Рецензент: к.т.н., профессор Сатимова Е.Г.

Печатается по дополнительному плану издания некоммерческого акционерного общества «Алматинский университет энергетики и связи имени Гумарбека Даукеева» на 2022 год.

© НАО «Алматинский университет энергетики и связи имени Гумарбека Даукеева», 2022 г.

Содержание

Введение 4

1 Исследование получения IP адреса в ЛВС по средствам DHCP..... 5

2 Исследование динамической маршрутизации на примере OSPF с использованием программы PacketTracer..... 8

3 Исследование организации списков доступа на примере Cisco с использованием программы PacketTracer …… 12

4 Перераспределение между EIGRP и OSPF на примере Cisco с использованием программы PacketTracer ……..... 18

5 Настройка туннелей точка-точка GRE..... 23

6 Настройка туннеля GRE «точка-точка» в сети VPN ……..... 27

7 Настройка избыточности с использованием HSRP ……... 32

8 Настройка протоколов HSRP и GLBP..... 40

9 Комплексная лабораторная работа на примере IT компании..... 50

10 Настройка списка доступа Access list..... 59

11 Обеспечение сетевой безопасности на платформе Cisco packet tracer..... 65

12 Демилитаризованная зона (DMZ)..... 74

13 Исследование протокола syslog с помощью NTP…….. 82

14 Лабораторная работа № 14. Исследование WI-FI – беспроводной передача данных …… 86

15 Траблшутинг корпоративной сети…….. 92

Список использованной литературы……..……. 95

Введение

ЛВС (или Локальная Вычислительная Сеть, LAN – Local Area Network) – это объединение вычислительных устройств в единую информационную сеть с использованием средств проводной или беспроводной связи.

В состав ЛВС входят следующие примеры:

- компьютеры;
- серверы;
- кабели соединительные;
- маршрутизаторы;
- модемы;
- коммутаторы;
- дополнительное оборудование (принтеры, системы резервного копирования и так далее);
- программное обеспечение для настройки и сетевые протоколы.

После включения маршрутизаторов протокол ищет непосредственно подключенных соседей и устанавливает с ними «дружеские» отношения. Затем они обмениваются друг с другом информацией о подключенных и доступных им сетях. То есть они строят карту сети (топологию сети). Данная карта одинакова на всех маршрутизаторах. На основе полученной информации запускается алгоритм SPF (Shortest Path First – «выбор наилучшего пути»), который рассчитывает оптимальный маршрут к каждой сети. Данный процесс похож на построение дерева, корнем которого является сам маршрутизатор, а ветвями — пути к доступным сетям. Данный процесс, то есть конвергенция, происходит очень быстро.

Протокол HSRP предназначен для того, чтобы добиться практически 100% доступности и отказоустойчивости первого хопа от отправителя («маршрут по умолчанию», *default gateway*, также иногда называемый «шлюз последней надежды»). Это достигается путём использования у двух или более маршрутизаторов или маршрутизирующих коммутаторов третьего уровня одного IP-адреса и MAC-адреса так называемого виртуального маршрутизатора. Такая группа называется HSRP-группой.

Active маршрутизатор – маршрутизатор, который отвечает за отправку пакетов, отправленных на IP-адрес, который ассоциирован с виртуальным маршрутизатором.

Например, для работы некоторых игровых серверов требуется обеспечить отображение большого количества портов или адреса портов назначаются таким сервером динамически в широком диапазоне.

Лабораторная работа № 1. Исследование получения IP адреса в ЛВС по средствам DHCP.

1.1 Цель работы: исследование принципов получения IP-адреса

1.2 Подготовка к работе:

Повторить разделы: создание стандартных технологий локальных сетей; коммутация сообщений, назначение IP-протокола, модель OSI, различие между сообщением и сигналом, определение пакета, кадра, фрейма.

Теоретическое описание

DHCP (англ. Dynamic Host Configuration Protocol — протокол динамической настройки узла) — прикладной протокол, позволяющий сетевым устройствам автоматически получать IP-адрес и другие параметры, необходимые для работы в сети TCP/IP. Данный протокол работает по модели «клиент-сервер». IP-адрес можно назначать вручную каждому клиенту, то есть компьютеру в локальной сети. Но в больших сетях это очень трудозатратно, к тому же, чем больше локальная сеть, тем выше возрастает вероятность ошибки при настройке. Поэтому для автоматизации назначения IP был создан протокол DHCP.

ЛВС (или Локальная Вычислительная Сеть, LAN – Local Area Network) – это объединение вычислительных устройств в единую информационную сеть с использованием средств проводной или беспроводной связи.

В состав ЛВС входят следующие примеры:

- компьютеры,
- серверы,
- кабели соединительные,
- маршрутизаторы,
- модемы,
- коммутаторы,
- дополнительное оборудование (принтеры, системы резервного копирования и так далее),
- программное обеспечение для настройки и сетевые протоколы.

1.3 Описание лабораторной работы

В данной лабораторной работе используются маршрутизаторы, коммутаторы, ПК через програмное обеспечение Cisco. В данной лабораторной работе должны построить сеть доступа, научиться настраивать DHCP в интерфейсе маршрутизатора. После всех выполненных команд нужно проверить работоспособность сети.

1.4 Рабочее задание:

Осуществить получение IP-адреса для PC1 и PC0.

1.4.1 Схема подключения

Соберем 2 сети, каждая из которых содержит по одному ПК и 1 свитчу.

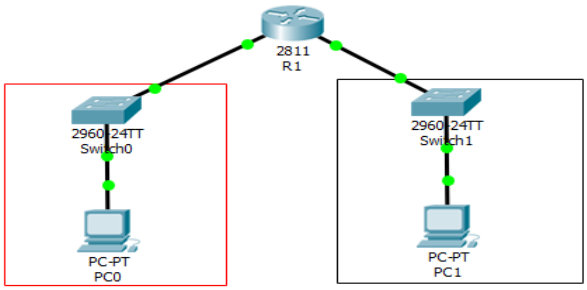


Рисунок 1.1 – Схема соединения

Удостовериться, что на клиентской стороне активирован DHCP, во вкладке IP configuration.

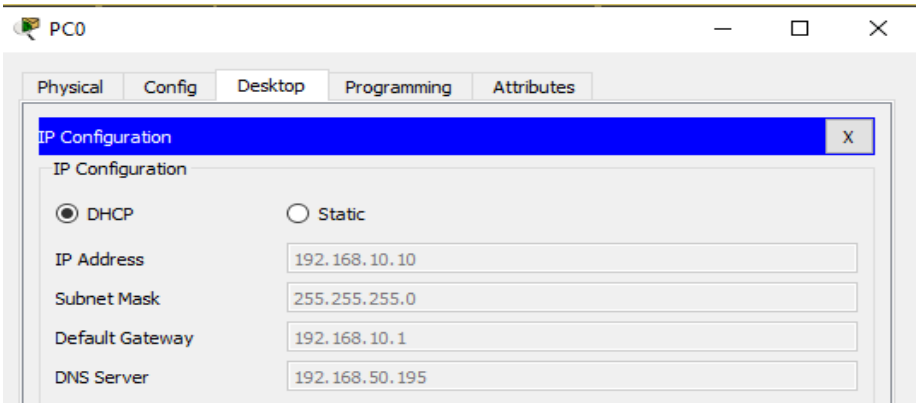


Рисунок 1.2 – конфигурация IP-адресов

Заходим в CLI интерфейс маршрутизатора.

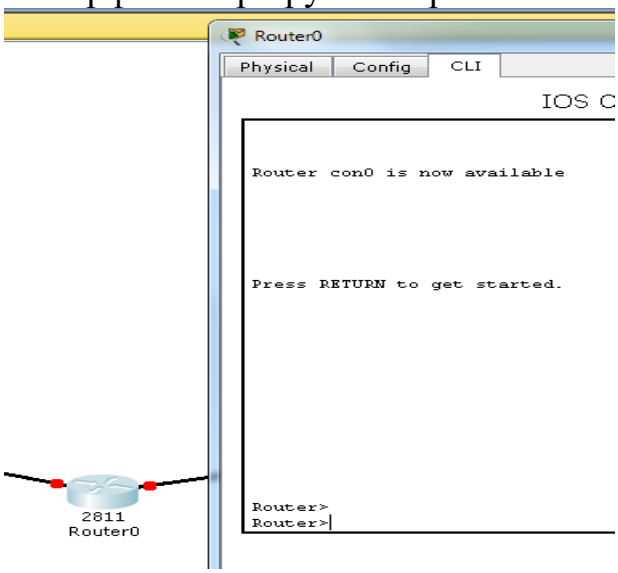


Рисунок 1.3 – CLI интерфейс маршрутизатора

Зайдя в режим глобального конфигурирования, изменяем имя маршрутизатора и исключаем из пула адресов зарезервированные IP- адреса.

1.4.2 Набираем команды.

Адрес и маска DHCP ПК1 192.168.10.0 - 255.255.255.0
Адрес и маска DHCP ПК2 192.168.11.0 - 255.255.255.0

enable
configure terminal
hostname R1
ip dhcp excluded-address 192.168.10.1 192.168.10.9
ip dhcp excluded-address 192.168.10.254
ip dhcp excluded-address 192.168.11.1 192.168.11.9
ipdhcpexcluded-address 192.168.11.254
Создаем 2 DHCP пула, для 2-х интерфейсов в разных подсетях.
ip dhcp pool S1
network 192.168.10.0 255.255.255.0
default-router 192.168.10.1
dns-server 192.168.50.195
exit
ip dhcp pool S2
network 192.168.11.0 255.255.255.0
default-router 192.168.11.1
dns-server 192.168.50.195
exit
Поднимаем интерфейсы для подключения клиентской стороны.
interface fastEthernet 0/0
no shutdown
ip address 192.168.10.1 255.255.255.0
exit
interface fastEthernet 0/1
no shutdown
ip address 192.168.11.1 255.255.255.0
exit
exit
1.4.3 Порядок проверки получения IP по DHCP:

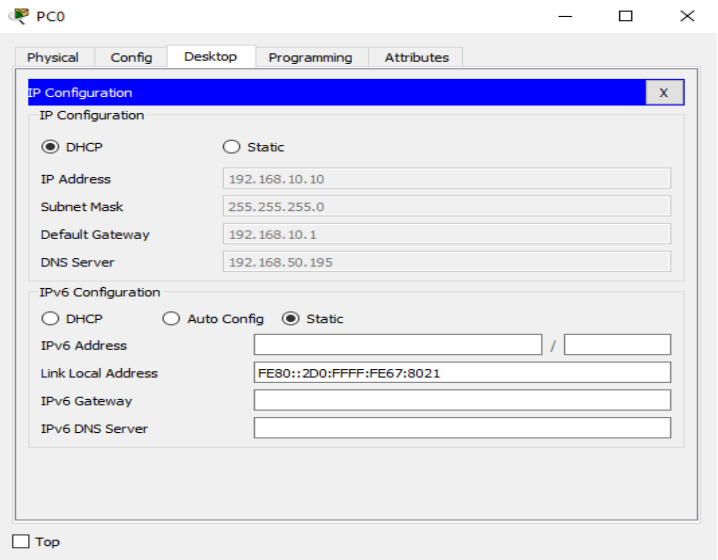


Рисунок 1.4 – Проверка на получения IP по DHCP

1.5 Задания для самостоятельной работы

1.5.1 Построить сеть с топологию «звезда». Добавить еще 2 ПК.

1.5.2 Нужно указать адрес DHCP для ПК.

Адрес и маска DHCP ПК1 176.98.1.1 - 255.255.255.0

Адрес и маска DHCP ПК2 176.98.2.1 - 255.255.255.0

Адрес и маска DHCP ПК3 176.98.3.1 - 255.255.255.0

Адрес и маска DHCP ПК4 176.98.3.1 - 255.255.255.0

1.5.3 Через ПК1 отправлять ping к соседнему ПК2.

1.5.4 Сделать анализ задержек пакетов.

1.5.5 Приготовить отчет со скриншотами и анализами задержек пакетов (в виде таблицы) и ответить на контрольные вопросы.

1.6 Контрольные вопросы:

1. В каких сетевых технологиях реализованы достаточно просто алгоритмы доступа к среде адресации и передаче данных?
2. Задачи адресации компьютеров (или узлов).?
3. Что такое передача сообщений, пакетов?
4. Определение локальных вычислительных сетей (ЛВС).
5. Назначение IP и DHCP протокола.

Лабораторная работа № 2. Исследование динамической маршрутизации на примере OSPF с использованием программы PacketTracer

2.2 Цель работы: исследование принципов функционирования OSPF.

2.2 Подготовка к работе: повторить разделы: создание стандартных технологий локальных сетей; коммутация сообщений, назначение IP-протокола, модель OSI, функционирование OSPF.

Теоретическое описание

OSPF (англ. Open Shortest Path First) — протокол динамической маршрутизации, основанный на технологии отслеживания состояния канала (link-state technology) и использующий для нахождения кратчайшего пути алгоритма Дейкстры.

После включения маршрутизаторов протокол ищет непосредственно подключенных соседей и устанавливает с ними «дружеские» отношения. Затем они обмениваются друг с другом информацией о подключенных и доступных им сетях. То есть они строят карту сети (топологию сети). Данная карта одинакова на всех маршрутизаторах. На основе полученной информации запускается алгоритм SPF (Shortest Path First – «выбор наилучшего пути»), который рассчитывает оптимальный маршрут к каждой сети. Данный процесс похож на построение дерева, корнем которого является сам маршрутизатор, а ветвями — пути к доступным сетям. Данный процесс, то есть конвергенция, происходит очень быстро.

2.3 Описание лабораторной работы

В данной лабораторной работе нужно построить сеть с помощью маршрутизатора, коммутатора с добавлением технологии OSPF, что поможет улучшить работоспособность работы сети.

2.4 Рабочее задание: осуществить получение маршрутной информации между R1 и R2.

2.4.1 Соберем 2 сети, каждая из которых содержит по одному ПК, свитчу и маршрутизатору.

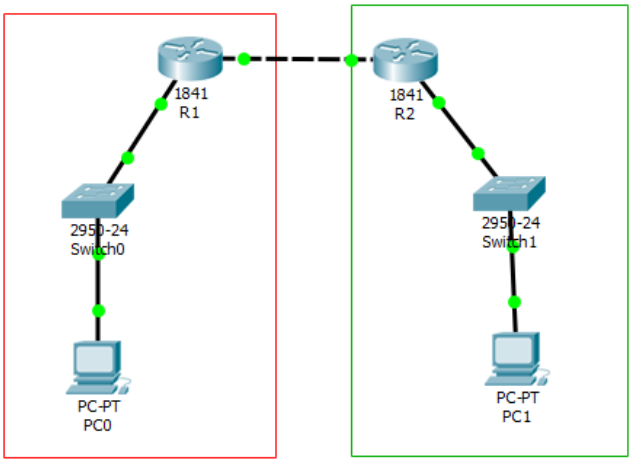


Рисунок 2.1 – Схема соединения

2.4.2 Удостовериться, что на клиентской стороне не активирован DHCP во вкладке IP configuration и прописываем статические IP адреса: 192.168.1.10/24 для PC0 и 192.168.2.10/24 для PC1.

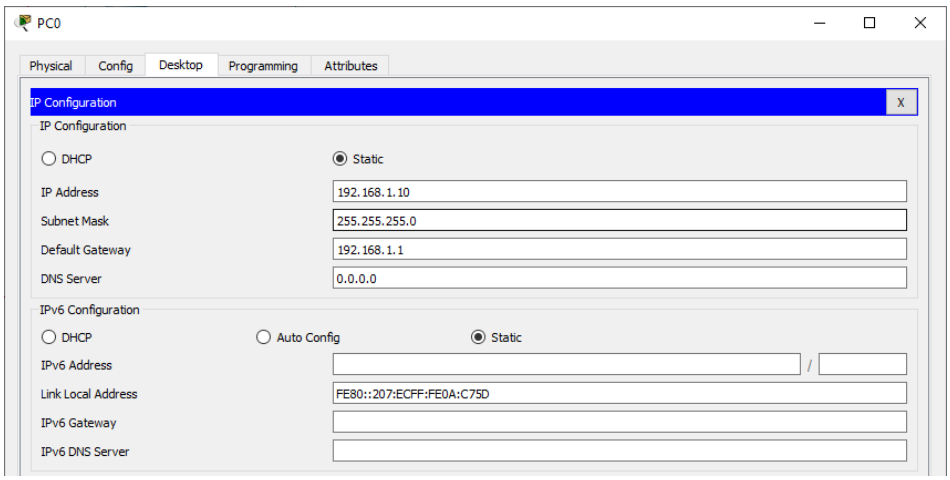


Рисунок 2.2 – конфигурация IP-адресов

2.4.3 Заходим в CLI интерфейс маршрутизатора, один раз кликнув на него левой кнопкой мыши.

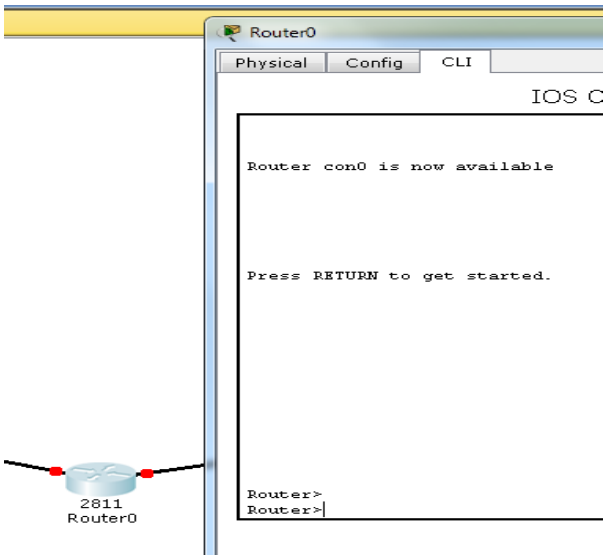


Рисунок 2.3 – CLI интерфейс маршрутизатора

2.4.4 Зайдя в режим глобального конфигурирования, изменяем имя маршрутизатора.

Набор команды

enable

configure terminal

hostname R1

2.4.5 Подготавливаем интерфейсы на R1 в сторону R2 и в сторону сети доступа.

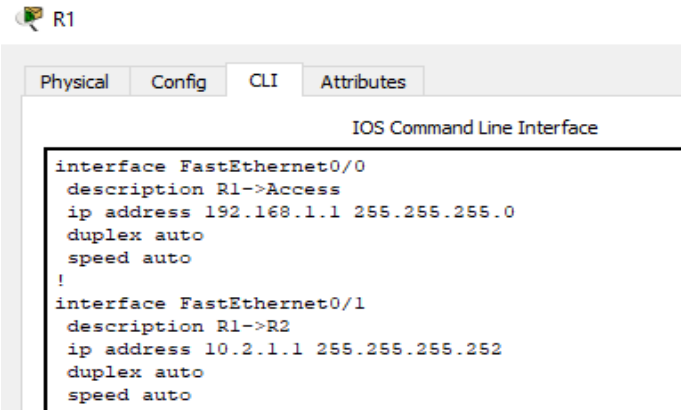


Рисунок 2.4 – Присваивание IP-адреса интерфейсам на маршрутизаторе R1

2.4.6 Активируем протокол OSPF на R1.

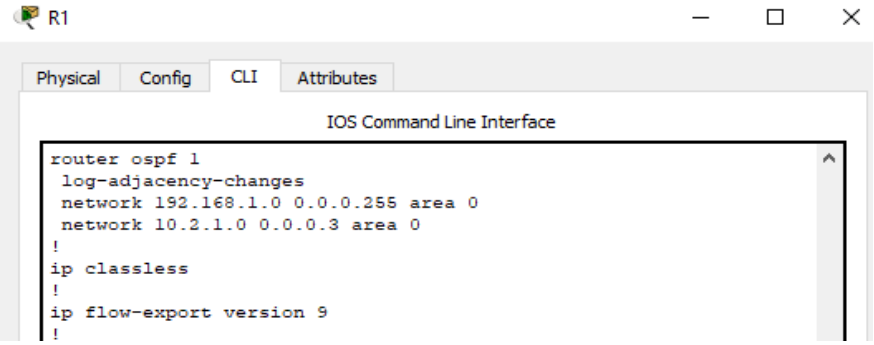


Рисунок 2.5 – Активация OSPF на маршрутизаторе R1

2.4.7 Производим симметричную настройку для маршрутизатора R2.
10.2.1.2/30 – интерфейс, смотрящий в сторону R1.
192.168.2.1 – интерфейс, смотрящий в сторону сети доступа.

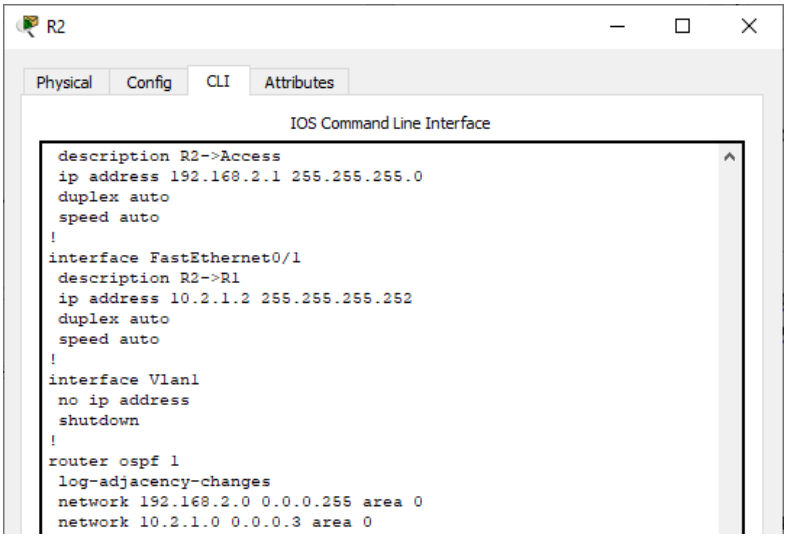


Рисунок 2.6 – Команды для маршрутизатора R2

2.5 Порядок проверки получения маршрутной информации

Проверяем состояние таблицы маршрутизации.

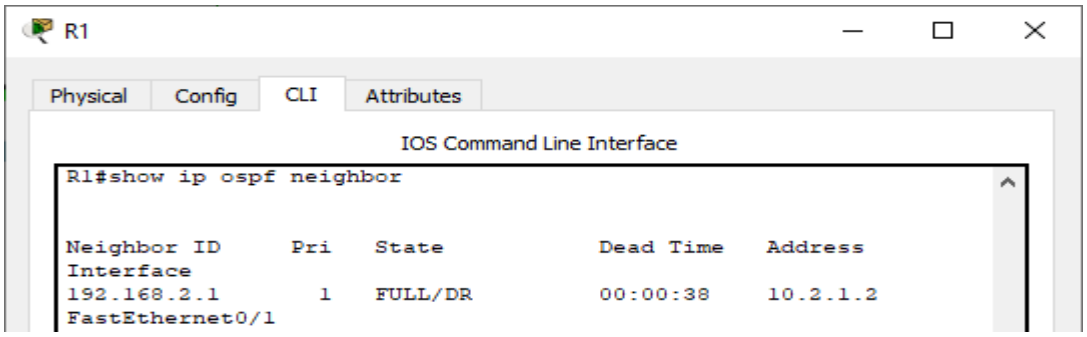


Рисунок 2.7 – Таблица маршрутизации на R1

2.6 Задания для самостоятельной работы

2.6.1 Построить сеть с топологию «звезда».

2.6.2 Настроить ПК статистическом режиме и выбрать область 0 (area 0). Выбрать один адрес для шлюза. Добавить маршрутизатором технологию OSPF.

2.6.3 Проверить работу OSPF через команду *show ip ospf neighbor*.

2.6.4 Проверить работу доставки пакетов *(через команды ping адрес ПК).*

2.6.5 Подготовить отчет и ответить на контрольные вопросы.

2.6 Контрольные вопросы

1. Рассказать об OSPF алгоритме.
2. Типы сообщений, используемых в OSPF.
3. Какое конечное состояние протокола OSPF?

Лабораторная работа № 3. Исследование организации списков доступа на примере Cisco с использованием программы PacketTracer

3.1 Цель работы: Организация списков доступа в ЛВС**.**

3.2 Подготовка к работе: повторить разделы: создание стандартных технологий локальных сетей; коммутация сообщений, организация ACL.

Теоретическое описание

VLAN (Virtual Local Area Network, виртуальная локальная сеть) — это функция в роутерах и коммутаторах, позволяющая на одном физическом сетевом интерфейсе (Ethernet, Wi-Fi интерфейсе) создать несколько виртуальных локальных сетей. VLAN используют для создания логической топологии сети, которая никак не зависит от физической топологии.

Достоинства использования VLAN:

- Гибкое разделение устройств на группы

Как правило, одному VLAN соответствует одна подсеть. Компьютеры, находящиеся в разных VLAN, будут изолированы друг от друга. Также можно

объединить в одну виртуальную сеть компьютеры, подключенные к разным коммутаторам.

- Уменьшение широковещательного трафика в сети

Каждый VLAN представляет отдельный широковещательный домен. Широковещательный трафик не будет транслироваться между разными VLAN. Если на разных коммутаторах настроить один и тот же VLAN, то порты разных коммутаторов будут образовывать один широковещательный домен.

- Увеличение безопасности и управляемости сети

В сети, разбитой на виртуальные подсети, удобно применять политики и правила безопасности для каждого VLAN. Политика будет применена к целой подсети, а не к отдельному устройству.

- Уменьшение количества оборудования и сетевого кабеля

Для создания новой виртуальной локальной сети не требуется покупка коммутатора и прокладка сетевого кабеля. Однако вы должны использовать более дорогие управляемые коммутаторы с поддержкой VLAN.

Access port, или порт доступа, — порт, находящийся в определенном VLAN и передающий не тегированные кадры. Как правило, это порт, смотрящий на пользовательское устройство.

Trunk port, или магистральный порт, — порт, передающий тегированный трафик. Как правило, этот порт поднимается между сетевыми устройствами.

3.3 Описание лабораторной работы

В данной лабораторной работе нужно построить небольшую сеть, состоящую из двух VLAN с несколькими станциями, пары серверов, маршрутизатора и коммутатора. Настроить DHCP в интерфейсе маршрутизатора и создать список доступа. На коммутаторе нужно создать два VLAN и подготовить порты доступа. После всех выполненных команд проверить работоспособность сети.

3.4 Рабочее задание: осуществить ограничение доступа из VLAN 10 на WEB сервер и из VLAN 30 на FTP посредством списков доступа.

3.4.1 Собрать сеть, приведенную ниже.

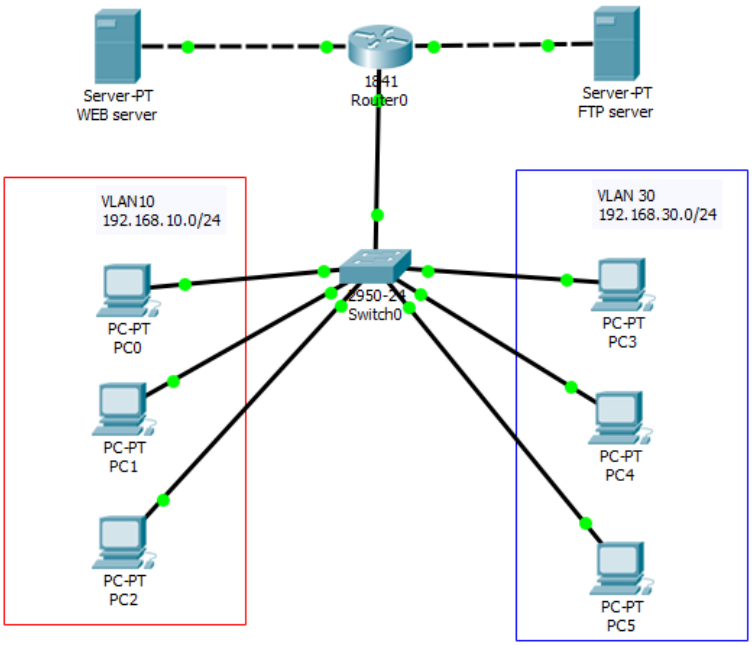


Рисунок 3.1 – Дизайн сети

3.4.2 Удостовериться, что на клиентской стороне активирован DHCP.

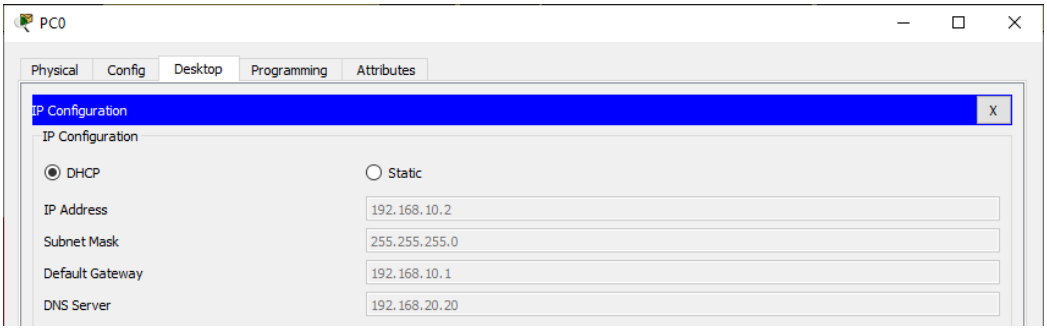


Рисунок 3.2 – Конфигурация IP-адресов рабочих станций

3.4.3 Заходим в CLI интерфейс маршрутизатора, один раз кликнув на него левой кнопкой мыши.

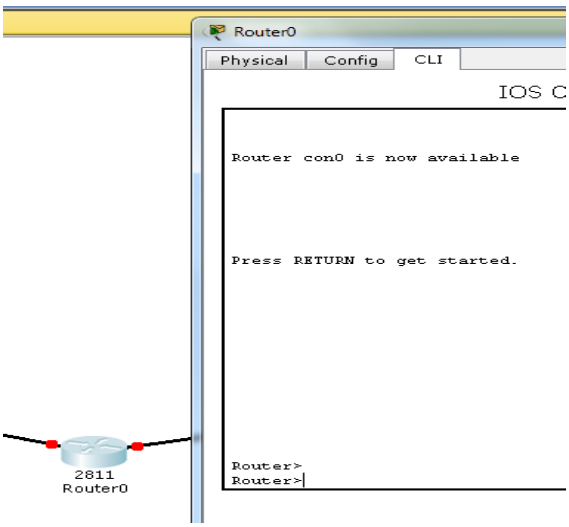


Рисунок 3.3 – CLI интерфейс маршрутизатора

3.4.4 Зайдя в режим глобального конфигурирования, изменяем имя маршрутизатора.

enable
configure terminal
no ip domain-lookup
hostname R1

3.4.5 Создать DHCP pool с резервированием IP.

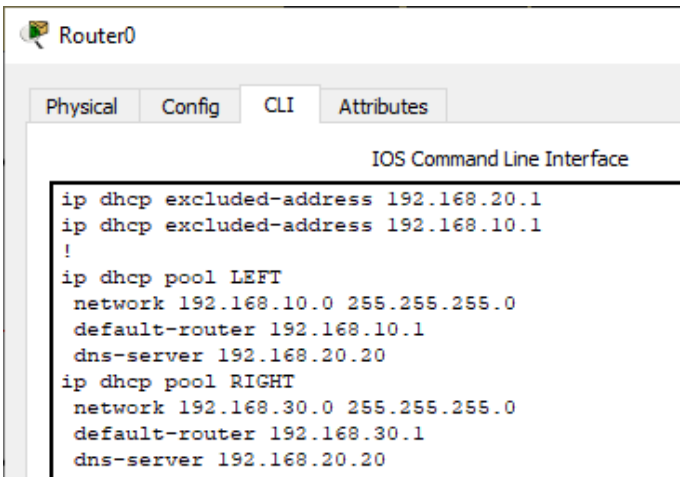


Рисунок 3.4 – Создание DHCP pool на маршрутизаторе R1

3.4.6 Подготовить интерфейсы на R1, идущие в сторону WEB, FTP и S1.

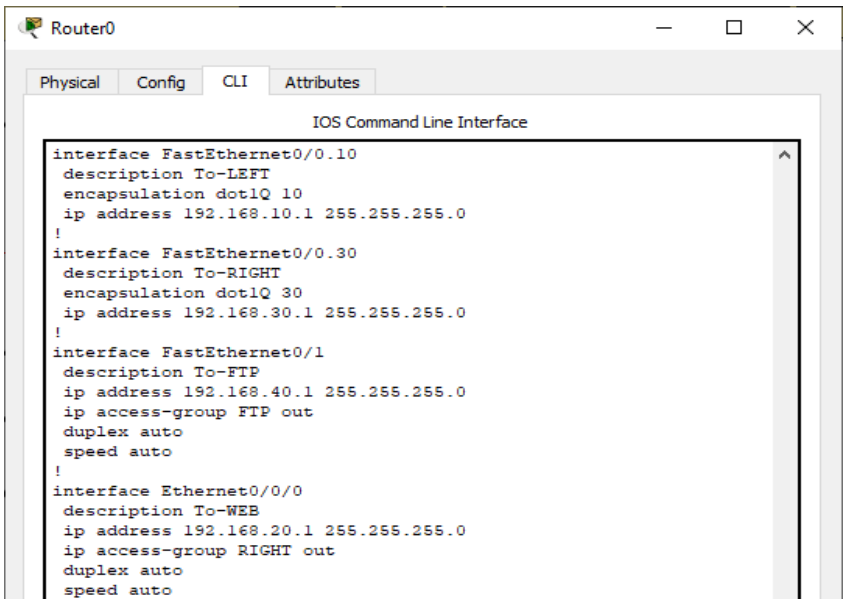


Рисунок 3.5 – Конфигурация интерфейсов на маршрутизаторе R1

3.4.7 Настроить коммутатор S1, подготовив access и trunk порты для VLAN.

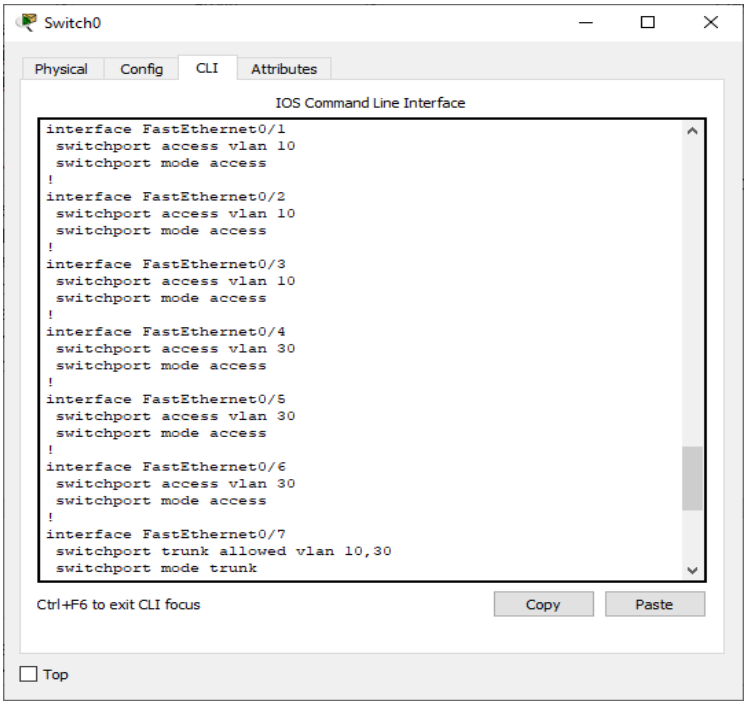


Рисунок 3.6 – Команды для коммутатора R2

3.4.8 Производим настройку списков доступа на R1 с целью выполнения требований ограничения доступа.

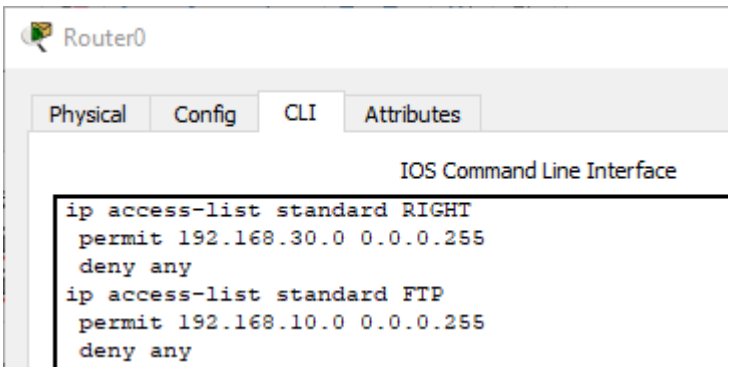


Рисунок 3.7 – Списки доступа на R1

3.5 Порядок проверки выполнения задания:

В VLAN 10 провести тестирование:

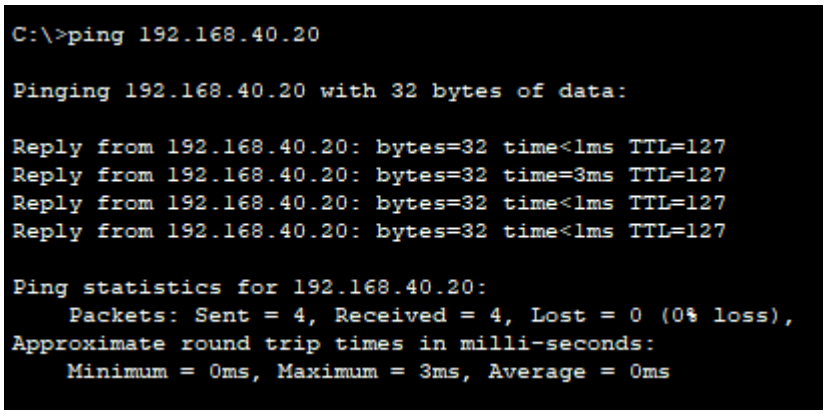


Рисунок 3.8 – Ping FTP server на VLAN 10

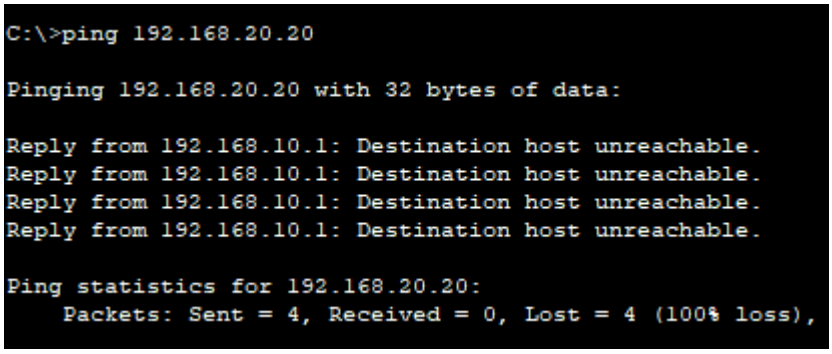


Рисунок 3.9 – Ping WEB server на VLAN 10

В VLAN 30 провести тестирование:

```
C:\>ping 192.168.20.20

Pinging 192.168.20.20 with 32 bytes of data:

Reply from 192.168.20.20: bytes=32 time=1ms TTL=127
Reply from 192.168.20.20: bytes=32 time<1ms TTL=127
Reply from 192.168.20.20: bytes=32 time=1ms TTL=127
Reply from 192.168.20.20: bytes=32 time=1ms TTL=127

Ping statistics for 192.168.20.20:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Рисунок 3.10 – Ping WEB server на VLAN 30

```
C:\>ping 192.168.40.20

Pinging 192.168.40.20 with 32 bytes of data:

Reply from 192.168.30.1: Destination host unreachable.
Reply from 192.168.30.1: Destination host unreachable.
Reply from 192.168.30.1: Destination host unreachable.
Reply from 192.168.30.1: Destination host unreachable.

Ping statistics for 192.168.40.20:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Рисунок 3.11 – Ping FTP server на VLAN 30

3.5 Задания для самостоятельной работы

3.5.1 Построить сеть.

3.5.2 Прописать настройки DHCP pool Right и Left (192.168.11.0/ 192.168.12.0).

3.5.3 Настроить доступ access list standart 192.168.1.1.

3.5.4 Пропинговать Vlan 10 и 30.

3.5.5 Подготовить отчет и сделать анализ по задержке пакетов.

3.6 Контрольные вопросы

1. Рассказать о типах списков доступа.
2. В чем различия в именованных и нумерованных списках доступа?
3. В чем различия между стандартными и расширенными списками доступа?

Лабораторная работа № 4. Перераспределение между EIGRP и OSPF на примере Cisco с использованием программы PacketTracer

4.1 Цель работы: получение таблицы маршрутизации**.**

4.2 Подготовка к работе: повторить разделы: принцип работы протоколов EIGRP, OSPF и их взаимодействие, маршрутизация в сети.

Теоретическое описание

Протокол EIGRP (Enhanced Interior Gateway Routing Protocol) — это усовершенствованный протокол маршрутизации на базе векторов расстояния,

разработанный компанией Cisco Systems. Как следует из названия этого протокола, EIGRP представляет собой усовершенствование другого протокола маршрутизации Cisco — протокола внутренней маршрутизации (IGRP).

Функции EIGRP:

- Алгоритм диффузного обновления.
- Установление отношений смежности с соседними устройствами.
- Надежный транспортный протокол (RTP).
- Частичные и ограниченные обновления.
- Распределение нагрузки с равной и неравной стоимостью.

OSPF (англ. Open Shortest Path First) — протокол динамической маршрутизации, основанный на технологии отслеживания состояния канала (link-state technology) и использующий для нахождения кратчайшего пути алгоритм Дейкстры.

Принцип работы OSPF:

- Маршрутизаторы обмениваются маленькими HELLO-пакетами.
- Обменявшись пакетами, они устанавливают соседские отношения, добавляя каждый друг друга в свою локальную таблицу соседей.
- Маршрутизаторы собирают состояния всех своих линков (связей с соседями), включающие в себя id Маршрутизатора, id соседа, сеть и префикс между ними, тип сети, стоимость линка (метрику) и формируют пакет, называемый LSA (Link State Advertisement).
- Маршрутизатор рассылает LSA своим соседям, те распространяют LSA дальше.
- Каждый маршрутизатор, получивший LSA, добавляет в свою локальную табличку LSDB (Link State Database) информацию из LSA.
- В LSDB скапливается информация обо всех парах, соединённых в сети маршрутизаторов, то есть каждая строчка таблицы — это информация вида: «Маршрутизатор A имеет соединение со своим соседом – маршрутизатором B, между ними сеть такая-то с такими-то свойствами».
- После обмена LSA каждый маршрутизатор знает про все линки, на основании пар строится полная карта сети, включающая все маршрутизаторы и все связи между ними.
- На основании этой карты каждый маршрутизатор индивидуально ищет кратчайшие с точки зрения метрики маршруты во все сети и добавляет их в таблицу маршрутизации.

4.3 Описание лабораторной работы

В данной лабораторной работе нужно построить 2 подсети, разделенные перераспределяющим маршрутизатором. Настроить IP на интерфейсах маршрутизатора и рабочих станциях. На 3 маршрутизаторах настроить EIGRP, OSPF и переход между ними. После всех выполненных команд нужно проверить таблицу маршрутизации.

4.4 Рабочее задание: осуществить переход от EIGRP в OSPF в Router3 и получить таблицу маршрутизации.

4.4.1 Собрать сеть, приведенную ниже.

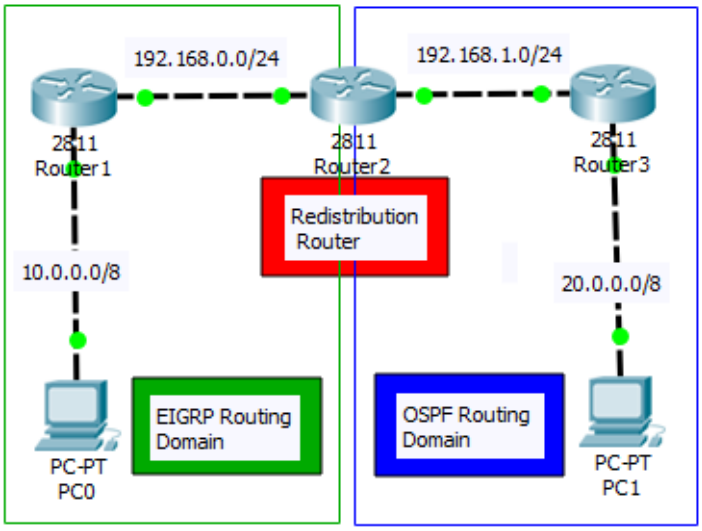


Рисунок 4.1 – Дизайн сети

4.4.2 В интерфейсах роутеров и компьютеров прописываем IP адреса.

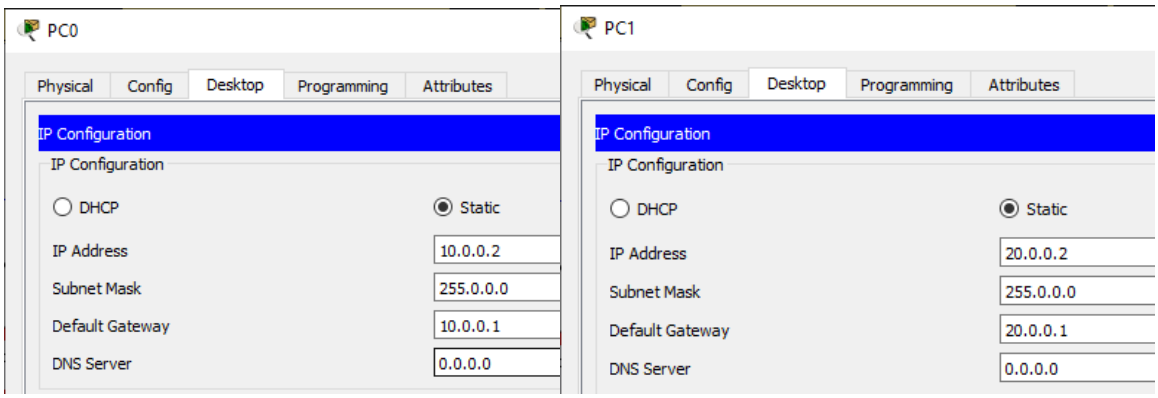


Рисунок 4.2 – Конфигурация IP-адресов рабочих станций

4.4.3 После настройки IP-адресов вводим следующие команды для настройки маршрутизации EIGRP на Router1.

```
Router1(config)# router eigrp 100
Router1(config-router)# network 10.0.0.0
Router1(config-router)# network 192.168.0.0
Router1(config-router)# exit
```

4.4.4 Затем переходим к Router2 и вводим следующие команды для настройки маршрутизации RIP:

```
Router2(config)# router eigrp 100
Router2(config-router)# network 192.168.0.0
```

Router2(config-router)# exit

4.4.5 Затем на Router2 выполнить следующие команды для настройки маршрутизации OSPF. Предполагаем, что наши маршрутизаторы OSPF (Router1 и Router2) принадлежат области 0.

Router2(config)# router ospf 100
Router2(config-router)# network 192.168.1.0 0.0.0.255 area0
Router2(config-router)# exit

4.4.6 Затем переходим к Router3 и вводим следующие команды для настройки маршрутизации OSPF:

Router3(config)#router ospf 100
Router3(config-router)#network 192.168.1.0 0.0.0.255 area0
Router3(config-router)#network 20.0.0.0 0.255.255.255 area0
Router3(config-router)#exit

4.4.7 Затем переходим к Router1 и выполняем следующую команду, чтобы отобразить таблицу маршрутизации.

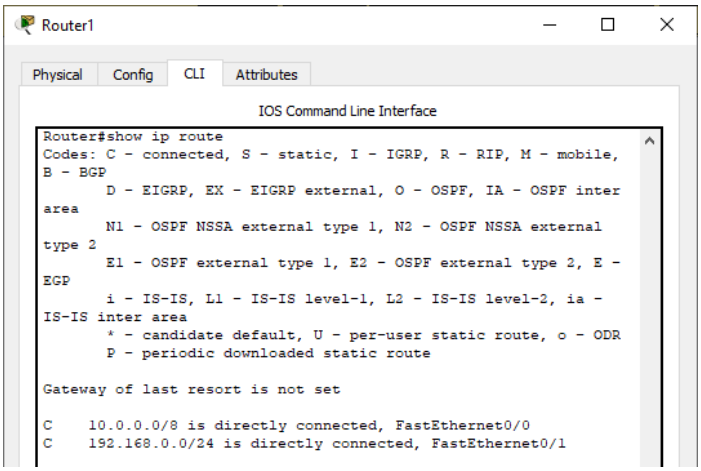


Рисунок 4.3 – Таблица маршрутизации на Router1

4.4.8 Чтобы перераспределить EIGRP в OSPF и наоборот, нам необходимо выполнить следующие команды на Router2.

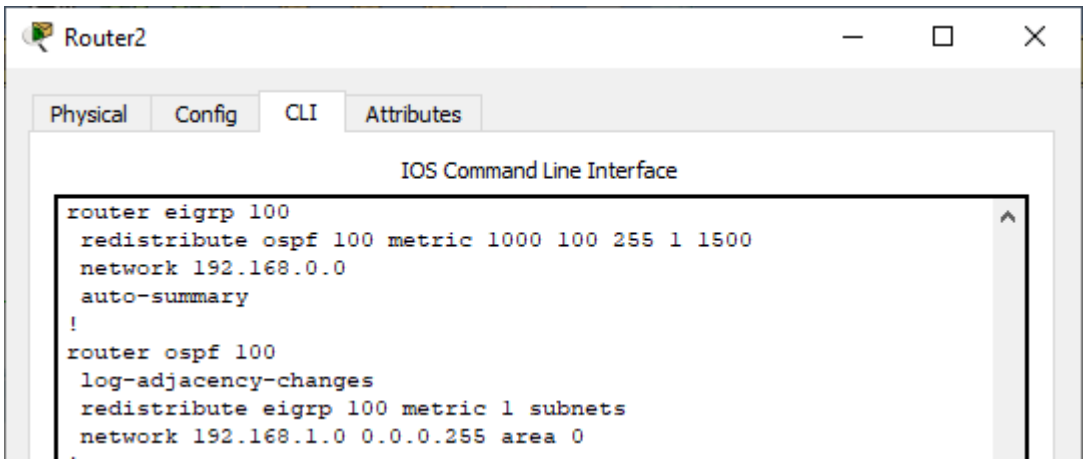


Рисунок 4.4 – Команды для перераспределения на Router2

4.4.9 После того, как мы перераспределили EIGRP в OSPF и наоборот, переходим к Router1 и выполним следующую команду, чтобы просмотреть таблицу маршрутизации. Можно увидеть, что сети 20.0.0.0/8 и 192.168.1.0/24 добавляются через внешний EIGRP.

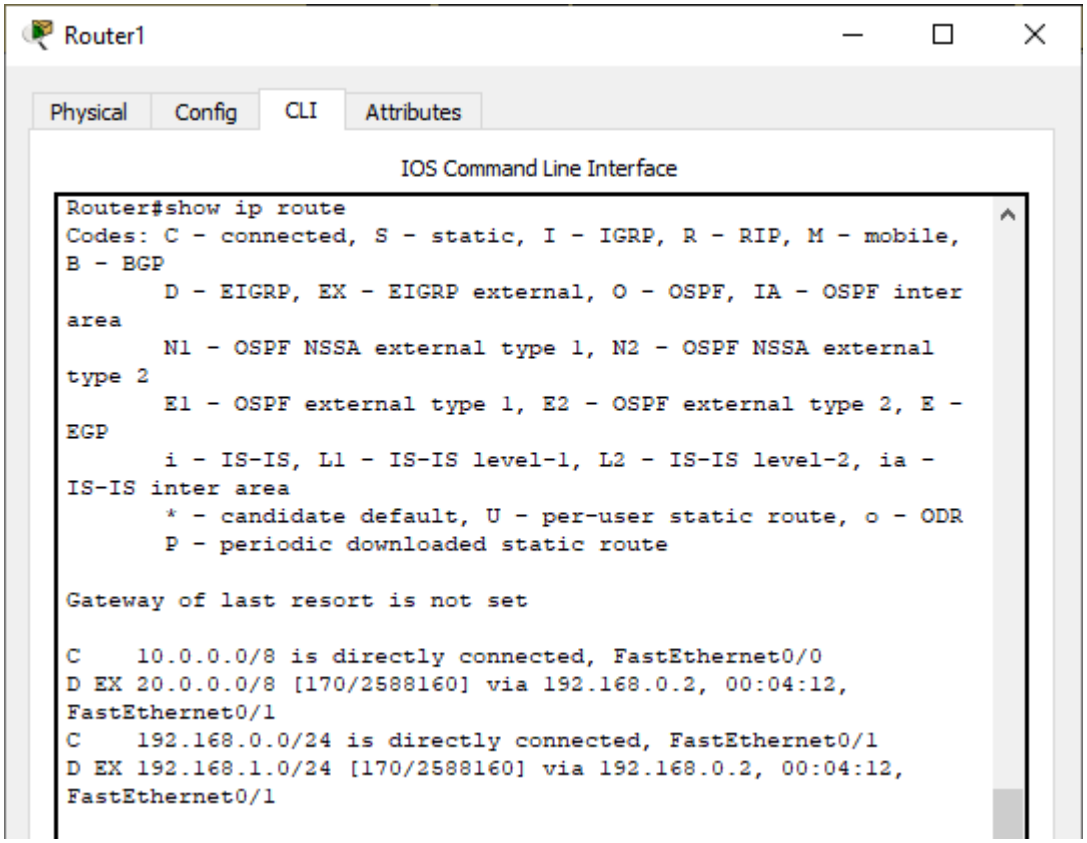


Рисунок 4.5 – Таблица маршрутизации на Router1

4.4.10 Затем переходим к Router3 и выполняем следующую команду, чтобы просмотреть таблицу маршрутизации. Можно увидеть, что сети 10.0.0.0/8 и 192.168.0.0/24 добавляются через внешний протокол OSPF.

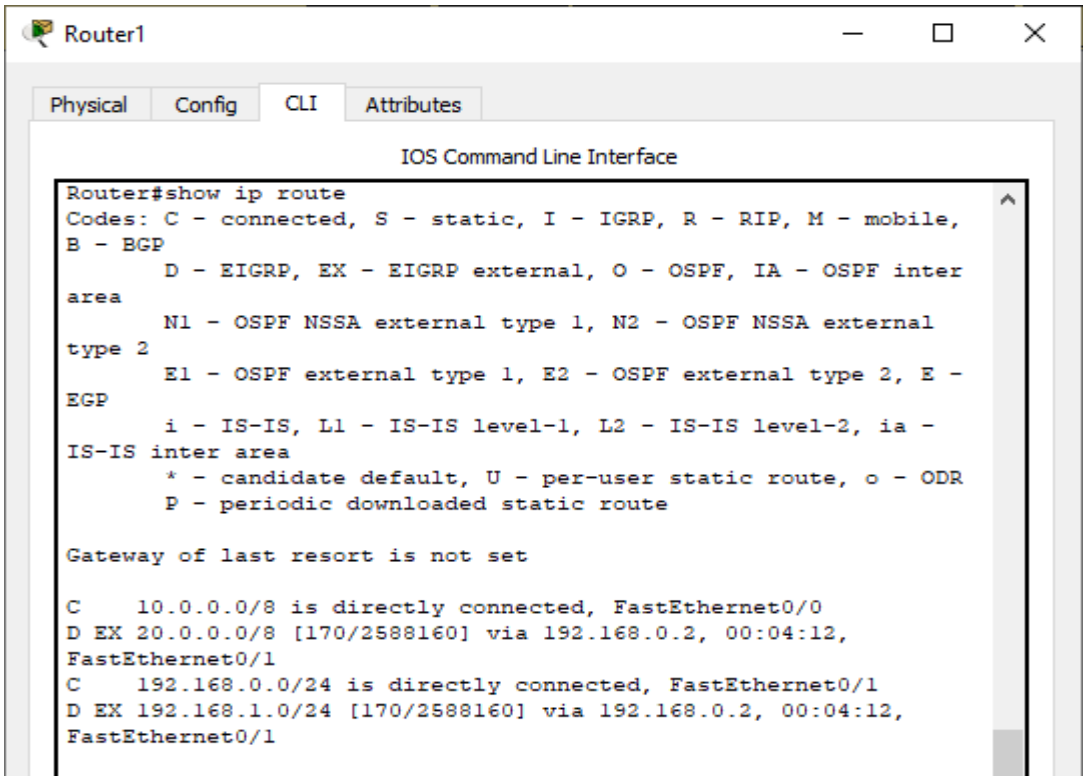


Рисунок 4.6 – Таблица маршрутизации на Router3

4.5 Задания для самостоятельной работы

4.5.1 Построить сеть.

4.5.2 Выбрать статистический режим, прописать EIGRP 192.168.3.1 и OSPF 192.168.4.1.

4.5.3 Проверить работу каждого маршрутизатора через команду show ip route.

4.5.4 Попинговать ПК1 и ПК2.

4.5.5 Сделать отчет и ответить на контрольные вопросы.

4.6 Контрольные вопросы

1 Дать понятие на протокол OSPF.

2 Дать понятие на протокол EIGRP.

3 Какие виды сообщений OSPF существуют?

4 В чем заключается разница между протоколами EIGRP и OSPF?

Лабораторная работа № 5. Настройка туннелей точка–точка GRE 5.1

Цель лабораторный работы: научиться настраивать двухточечные туннели GRE.

5.2 Подготовка к работе: Повторить принцип работы туннеля GRE.

Теоретические описание

GRE (англ. Generic Routing Encapsulation — общая инкапсуляция маршрутов) — протокол туннелирования сетевых пакетов, разработанный

компанией Cisco Systems. Его основное назначение — инкапсуляция пакетов сетевого уровня сетевой модели OSI в IP-пакетов.

GRE туннель представляет собой соединение точка–точка, его можно считать одной из разновидностей VPN туннеля, без шифрования. Основное достоинство GRE – это возможность передавать широковещательный трафик, что позволяет пропускать через такой туннель протоколы маршрутизации, использующие его, IPSec — протокол защиты сетевого трафика на IP-уровне, туннели в чистом виде этого не могут. Причин для организации GRE туннеля может быть множество: от банальной необходимости пробросить свою сеть через чужое IP-пространство до использования протоколов OSPF, RIPv2, EGRP совместно с IPSec. Также GRE, в отличие от IPIP, может помочь пробросить немаршрутизируюмые протоколы, такие как NetBios, IPX, AppleTalk.

Различия между туннелями GRE или IPIP:

- IPIP — инкапсулирует только unicast IPv4-трафик
- GRE — IPv4/IPv6 unicast/multicast трафик

5.3 Описание лабораторной работы

В данной лабораторной работе нужно настроить туннели точка–точка с помощью протокола GRE. Настроить имена хостов, настроить каждый маршрутизатор с соответствующими адресами IPv4 на обоих интерфейсах FastEthernet, туннель GRE на каждом маршрутизаторе, статический маршрут на маршрутизаторах. После всех выполненных команд проверить состояние интерфейсного туннеля и убедиться, что трафик проходит через туннель.

5.4 Выполнение работы

5.4.1 Для выполнения этой лабораторной работы собрать сеть, приведенную ниже.

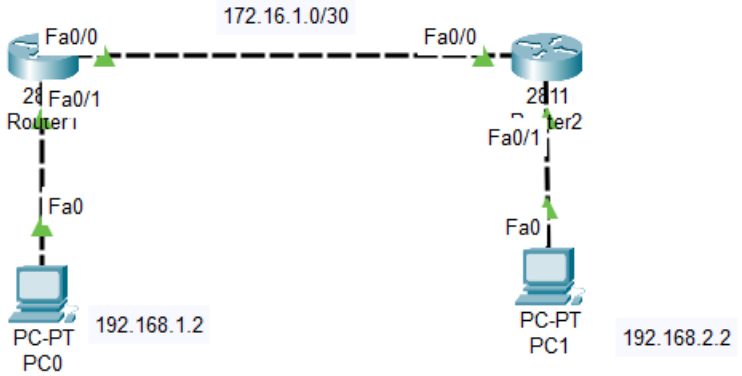


Рисунок 5.1 – Топология сети

5.4.2 Настроить имена хостов на R1 и R2.

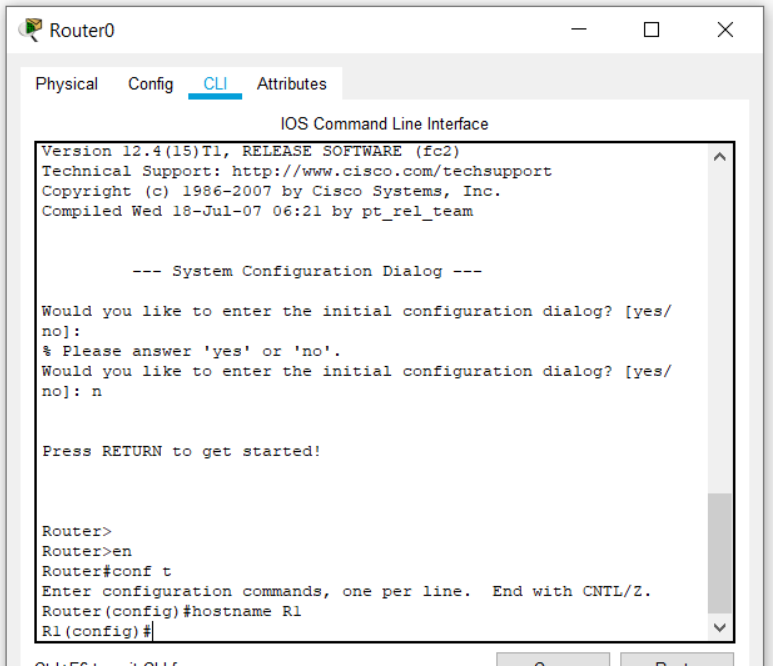


Рисунок 5.2 – CLI интерфейс маршрутизатора R1

5.4.3 Настроить каждый маршрутизатор с соответствующими адресами IPv4 на обоих интерфейсах FastEthernet.

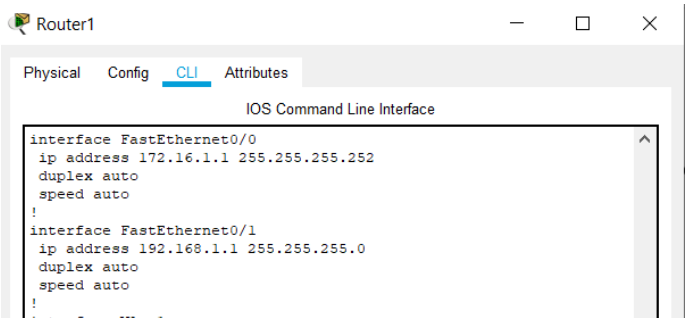


Рисунок 5.3 – Настройка маршрутизатора R1

5.4.4 Настроить туннель GRE (пронумерованный 1) на каждом маршрутизаторе с соответствующим адресом IPv4 (10.10.10.0/30)

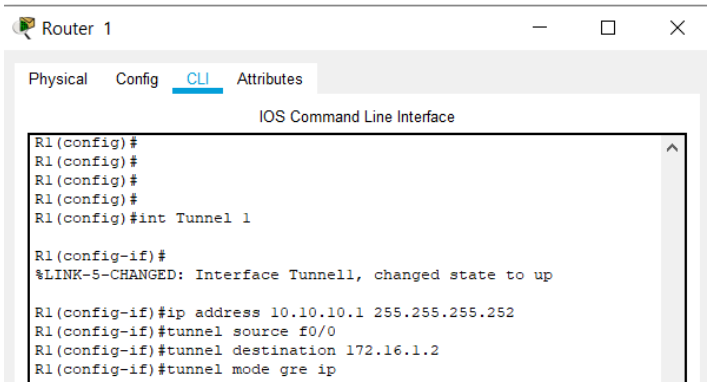


Рисунок 5.4 – Настройка туннеля GRE на маршрутизаторе R1

5.4.5 Настроить статический маршрут на маршрутизаторе R1 к 192.168.2.0/24 через интерфейс туннеля 1 и настроить аналогично маршрутизатор R2.

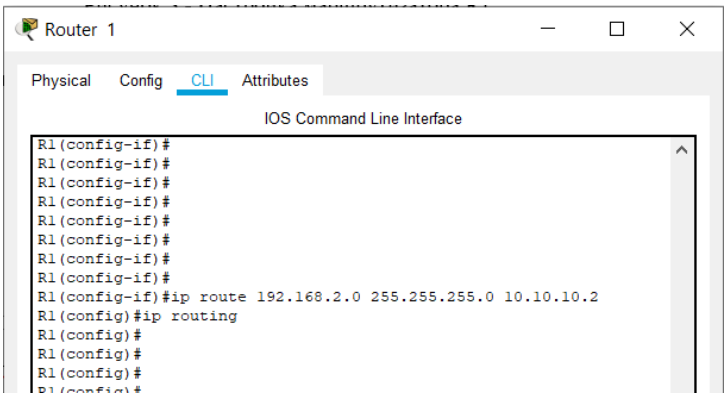


Рисунок 5.5 – Настройка статического маршрута на маршрутизаторе R1

5.4.6 Проверить состояние интерфейсного туннеля и убедиться, что трафик проходит через туннель, как ожидалось.

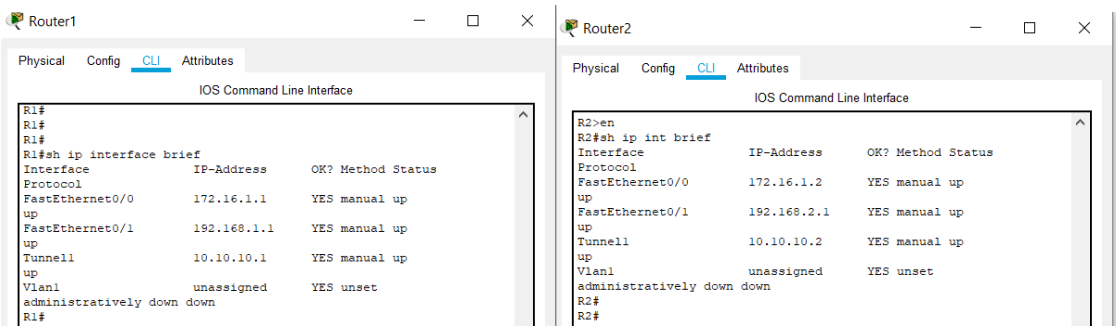


Рисунок 5.6 – Состояние интерфейсного туннеля на маршрутизаторах

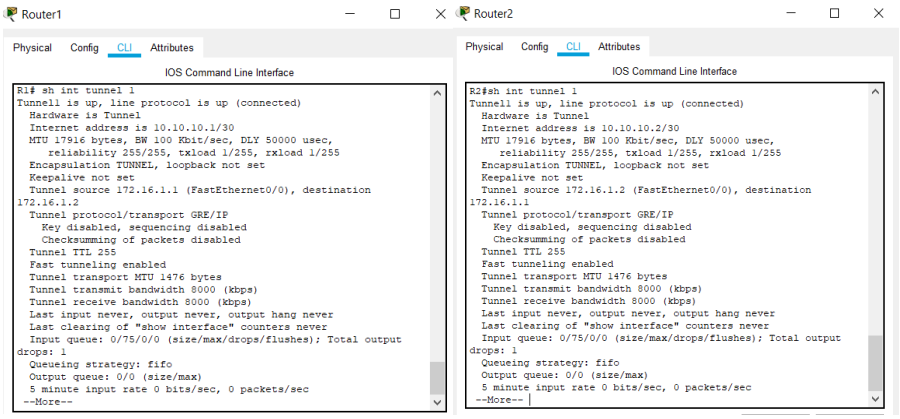


Рисунок 5.7 – Состояние интерфейсного туннеля на маршрутизаторах

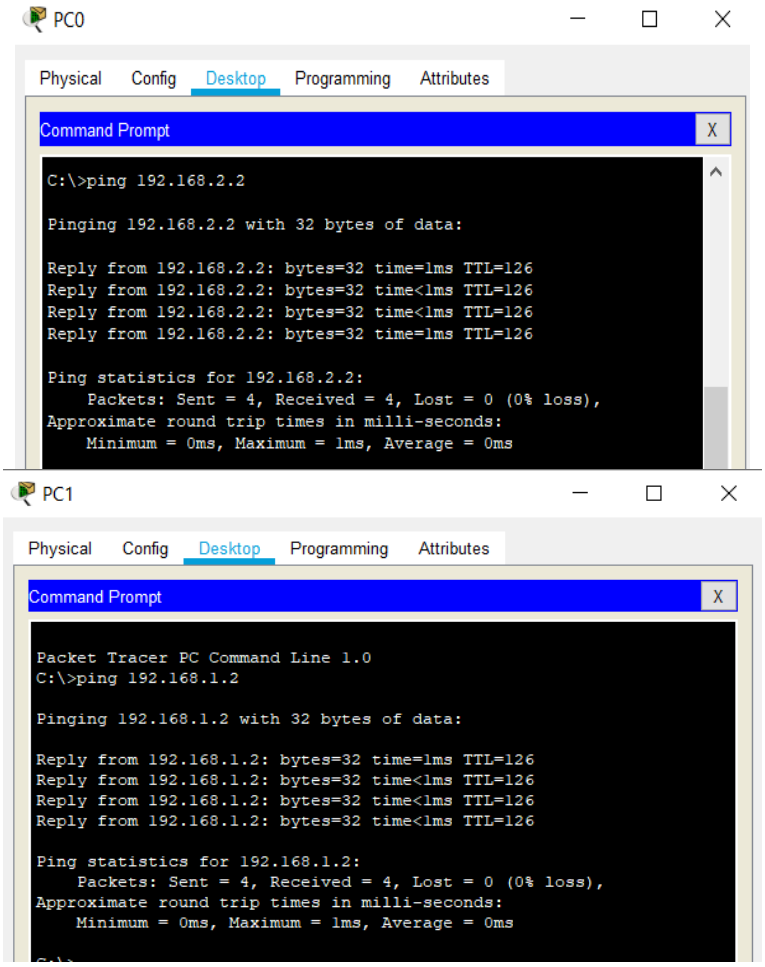


Рисунок 5.8 – Ping адреса 192.168.1.2 и 192.168.2.2 на компьютерах P0, P1

5.5 Задания для самостоятельной работы

5.5.1 Составить сеть с топологией «звезда».

5.5.2 Настроить маршрутизаторы (176.96.1.1).

5.5.3 Настроить туннелирование на адрес 172.16.3.1.

5.5.4 Попинговать ПК0 ПК1.

5.5.5 Сделать отчет и ответить на контрольные вопросы.

5.6 Контрольные вопросы

1 Дать понятие технологии GRE.

2 Какие протоколы подразумевает туннелирование?

3 Как происходит инкапсуляция заголовка GRE в IP-пакете?

Лабораторная работа № 6. Настройка туннеля GRE «точка–точка» в сети VPN

6.1 Цель лабораторный работы: научиться настраивать двухточечные туннели GRE с сетях VPN.

6.2 Подготовка к работе: повторить принцип работы туннели GRE, OSPF и VPN.

Теоретические описание

Универсальная инкапсуляция при маршрутизации (GRE) — это протокол туннелирования, способный инкапсулировать различные протоколы сетевого уровня между двумя объектами по общедоступной сети, например, в Интернете.

GRE можно использовать с:

- подключением сети IPv6 по сетям IPv4;
- пакетами групповой рассылки, например, OSPF, EIGRP и приложениями потоковой передачи данных.

VPN (англ. Virtual Private Network — виртуальная частная сеть) — это безопасное зашифрованное подключение пользователя к сети, с которым он может обходить локальные ограничения и сохранять конфиденциальность.

6.3 Описание лабораторной работы

В этой лабораторной работе необходимо настроить незашифрованный туннель GRE VPN «точка–точка» и убедиться, что сетевой трафик использует туннель. Также будет нужно настроить протокол маршрутизации OSPF внутри туннеля GRE VPN. Туннель GRE существует между маршрутизаторами WEST и EAST в области 0 OSPF. Интернет-провайдер не знает о туннеле GRE. Для связи между маршрутизаторами WEST и EAST и интернет-провайдером применяются статические маршруты по умолчанию.

6.4 Выполнение работы:

Часть 1. Настройка основных параметров устройства.

Часть 2. Настройка туннеля GRE.

Часть 3. Организация маршрутизации по туннелю GRE.

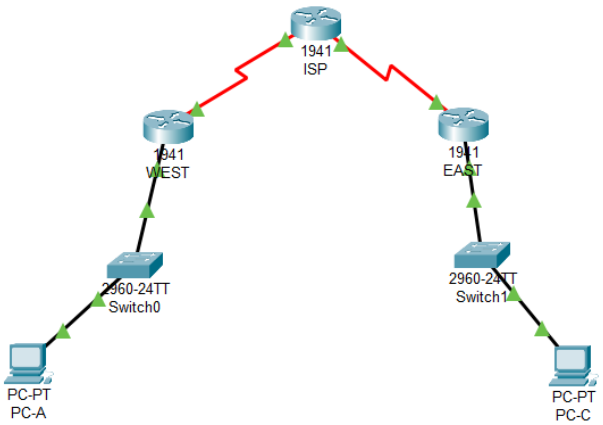


Рисунок 6.1 – Топология сети

Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
WEST	G0/1	172.16.1.1	255.255.255.0	Н/Д (недоступно)
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	Н/Д (недоступно)
	Tunnel0	172.16.12.1	255.255.255.252	Н/Д (недоступно)
ISP	S0/0/0	10.1.1.2	255.255.255.252	Н/Д (недоступно)
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	Н/Д (недоступно)
EAST	G0/1	172.16.2.1	255.255.255.0	Н/Д (недоступно)
	S0/0/1	10.2.2.1	255.255.255.252	Н/Д (недоступно)
	Tunnel0	172.16.12.2	255.255.255.252	Н/Д (недоступно)
PC-A	NIC	172.16.1.3	255.255.255.0	172.16.1.1
PC-C	NIC	172.16.2.3	255.255.255.0	172.16.2.1

Рисунок 6.2 – Таблица адресации

Часть 1: Настройка основных параметров устройств

В части 1 настроили топологию сети и базовые параметры маршрутизатора, например, IP-адреса интерфейсов, маршрутизацию, доступ к устройствам и пароли.

Шаг 1: Подключите кабели сети согласно приведенной топологии.

Шаг 2: Выполните инициализацию и перезагрузку маршрутизаторов и коммутаторов.

Шаг 3: Произведите базовую настройку маршрутизаторов.

Шаг 4: Настройте маршруты по умолчанию к маршрутизатору интернет-провайдера.

WEST(config)# ip route 0.0.0.0 0.0.0.0 10.1.1.2

```
WEST(config)#ip route 0.0.0.0 0.0.0.0 10.1.1.2
WEST(config)#
```

EAST(config)# ip route 0.0.0.0 0.0.0.0 10.2.2.2

```
EAST(config)#ip route 0.0.0.0 0.0.0.0 10.2.2.2
EAST(config)#
```

Часть 2: Настройка туннеля GRE В части 2 необходимо настроить туннель GRE между маршрутизаторами WEST и EAST

Шаг 1: Настройка интерфейса туннеля GRE.

а. Настройте интерфейс туннеля на маршрутизаторе WEST. В качестве интерфейса источника туннеля используйте S0/0/0 на маршрутизаторе WEST, а в качестве адреса назначения туннеля используйте 10.2.2.1 на маршрутизаторе EAST.

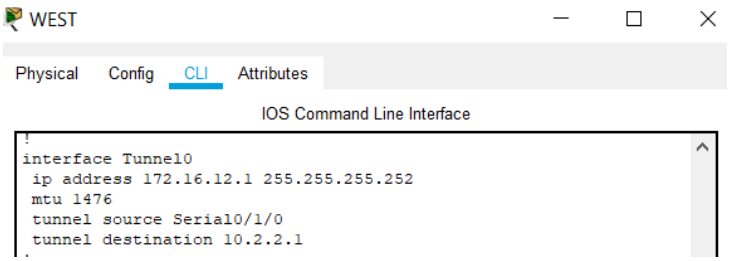


Рисунок 6.3 – Адресация для WEST

b. Настройте интерфейс туннеля на маршрутизаторе EAST. В качестве интерфейса источника туннеля используйте S0/0/1 на маршрутизаторе EAST, а в качестве адреса назначения туннеля используйте 10.1.1.1 на маршрутизаторе WEST.

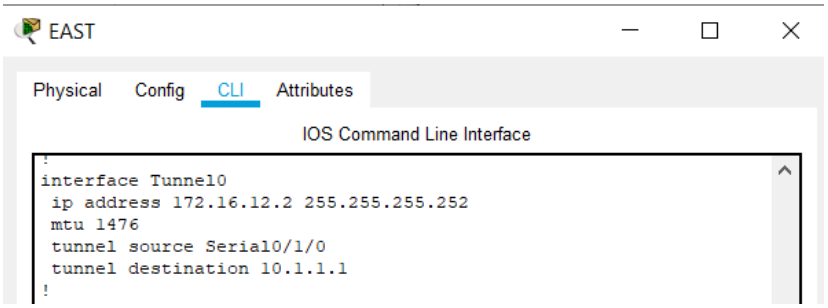


Рисунок 6.4 – Адресация для EAST

Шаг 2: Убедитесь, что туннель GRE работает:

а. Проверьте состояние интерфейса туннеля на маршрутизаторах WEST и EAST.

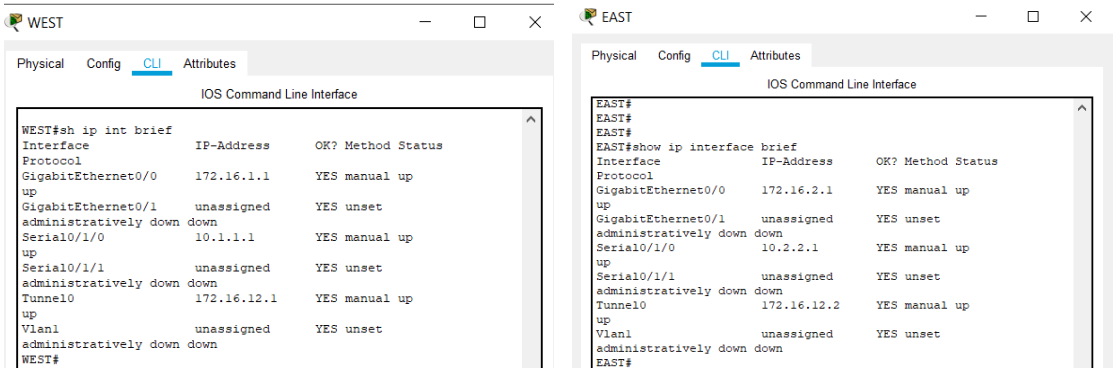


Рисунок 6.5 – Состояние интерфейса туннеля WEST

Отправьте ping-запрос по туннелю из маршрутизатора WEST на маршрутизатор EAST с использованием IP-адреса интерфейса туннеля.

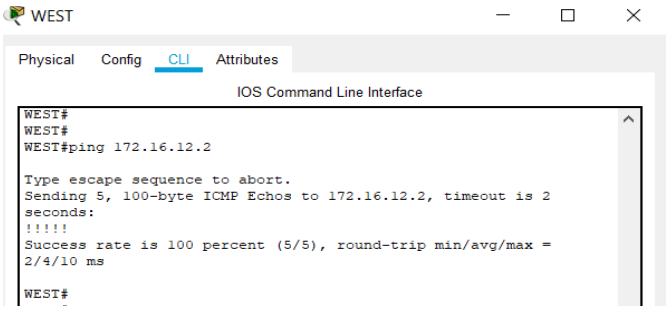


Рисунок 6.6 – Проверка IP-адреса

Часть 3: Включение маршрутизации через туннель GRE

В части 3 необходимо настроить протокол маршрутизации OSPF таким образом, чтобы локальные сети (LAN) на маршрутизаторах WEST и EAST могли обмениваться данными с помощью туннеля GRE. После установления туннеля GRE можно реализовать протокол маршрутизации. Для туннелирования GRE вместо сети, связанной с последовательным интерфейсом, сетевая инструкция будет включать IP-сеть туннеля, так же как в случае с другими интерфейсами, например Serial и Ethernet. Следует помнить, что маршрутизатор ISP в этом процессе маршрутизации не участвует.

a. Настройте процесс протокола OSPF с идентификатором 1 в области 0 на маршрутизаторе WEST для сетей 172.16.1.0/24 и 172.16.12.0/24.

```
WEST(config)# router ospf 1
WEST(config-router)# network 172.16.1.0 0.0.0.255 area 0
WEST(config-router)# network 172.16.12.0 0.0.0.3 area 0
```

b. Настройте процесс протокола OSPF с идентификатором 1 в области 0 на маршрутизаторе EAST для сетей 172.16.2.0/24 и 172.16.12.0/24.

```
EAST(config)# router ospf 1
EAST(config-router)# network 172.16.2.0 0.0.0.255 area 0
EAST(config-router)# network 172.16.12.0 0.0.0.3 area 0
```

Шаг 2. Проверка маршрутизации OSPF

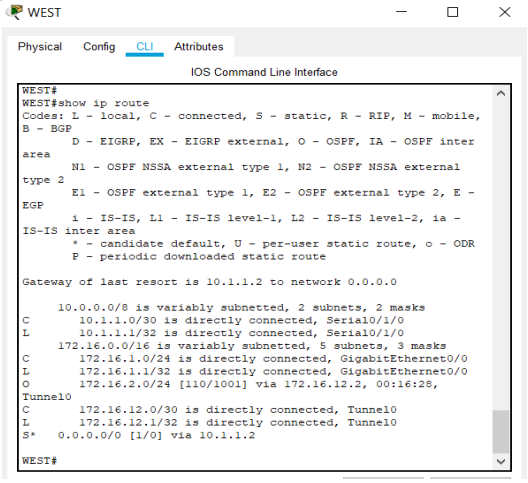
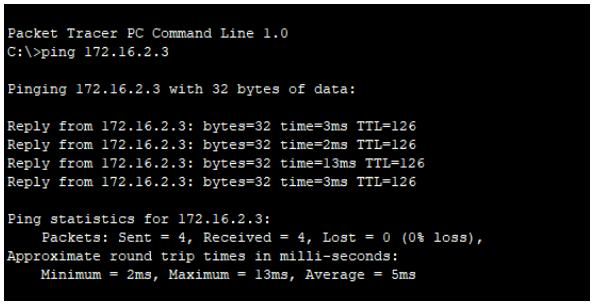


Рисунок 6.7 – Проверка работы маршрутизации OSPF

Шаг 3. Проверьте наличие сквозного соединения

а. Выполните ping-запрос от PC-A к PC-C. Ответы должны приходить успешно. Если это не так, найдите и устраните неполадки и убедитесь в наличии подключения между конечными узлами.



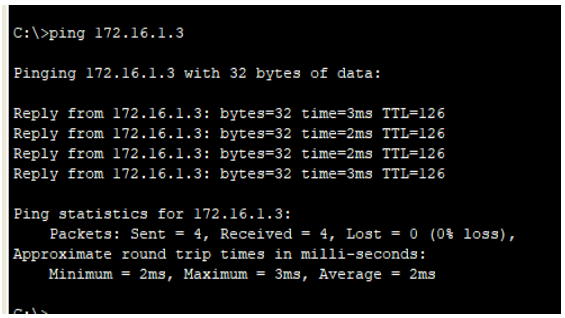


Рисунок 6.8 – Результаты пинга от ПК

6.5 Задания для самостоятельной работы

6.5.1 Поменять ip-адреса маршрутизаторов, ПК.

6.5.2 Поменять ip-адреса OSPF.

6.5.3 Убедиться, что идут пакеты, проверить по ping.

6.5.4 Сделать отчет и ответить на вопросы.

6.6 Контрольные вопросы

6.6.1 Как туннель GRE работает с VPN?

6.6.2 В чем преимущества сети VPN?

6.6.3 Достоинства и недостатки туннелирования.

6.6.4 В чем заключается работа loopback?

Лабораторная работа № 7. Настройка избыточности с использованием HSRP

7.1 Цель лабораторный работы: Понять структуру избыточности с HSRP.

7.2 Подготовка к работе: Повторить разделы HSRP, OSPF loopback, повторить настройки протокола RIP.

Теоретические описание

HSRP (Hot Standby Router Protocol) — проприетарный протокол Cisco, предназначенный для увеличения доступности маршрутизаторов, выполняющих роль шлюза по умолчанию. Это достигается путём объединения маршрутизаторов в *standby группу* и назначения им общего IP-адреса, который и будет использоваться как шлюз по умолчанию для компьютеров в сети.

Протокол HSRP предназначен для того, чтобы добиться практически 100% доступности и отказоустойчивости первого хопа от отправителя («маршрут по умолчанию», *default gateway*, также иногда называемый «шлюзом последней надежды»). Это достигается путём использования у двух

или более маршрутизаторов или маршрутизирующих коммутаторов третьего уровня одного IP-адреса и MAC-адреса, так называемого виртуального маршрутизатора. Такая группа называется HSRP-группой.

Active маршрутизатор – маршрутизатор, который отвечает за отправку пакетов, отправленных на IP-адрес, который ассоциирован с виртуальным маршрутизатором.

Маршрутизатор с наивысшим standby-приоритетом.

7.3 Описание лабораторной работы: В данной лабораторной работе нужно построить сеть с топологией «кольцо». Настроить все маршрутизации, включая резервную, добавляя протокол RIP и HSRP.

7.4 Выполнение работы:

Для настройки HSRP создали следующую топологию и подключили все устройства, как указано в топологии.

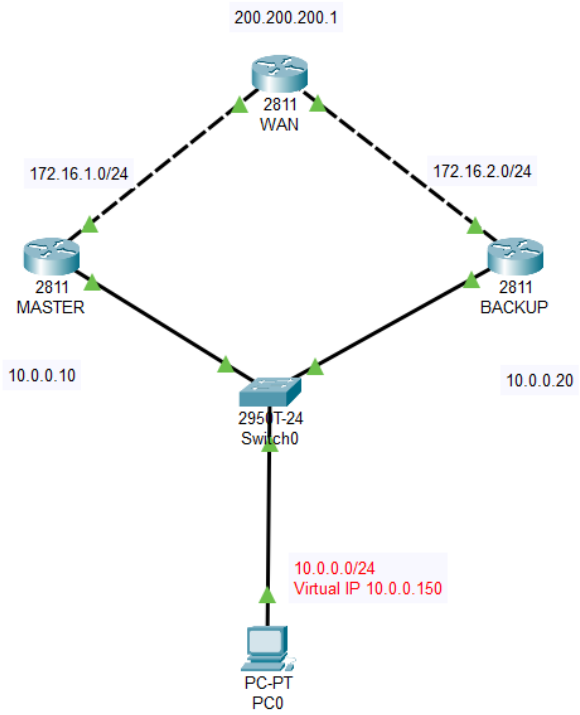


Рисунок 7.1 – Топология сети

Чтобы настроить и протестировать HSRP для предыдущей топологии, выполнили следующие шаги:

7.4.1 На маршрутизаторе WAN выполните следующие команды, чтобы настроить соответствующие IP-адреса на интерфейсах Loopback1, Fa0 / 0 и Fa0 / 1.

WAN(config)# interface Loopback1
WAN(config-if)# ip address 200.200.200.1 255.255.255.0
WAN(config-if)# no shutdown
WAN(config-if)# exit

WAN(config)# interface Fa0/ 0
WAN(config-if)# ip address 172.16.2.1 255.255.255.0
WAN(config-if)# no shutdown
WAN(config-if)# exit

WAN(config)# interface Fa0/ 1
WAN(config-if)# ip address 172.16.1.1 255.255.255.0
WAN(config-if)# no shutdown
WAN(config-if)# exit

7.4.2 На следующем рисунке показана IP-конфигурация маршрутизатора WAN.

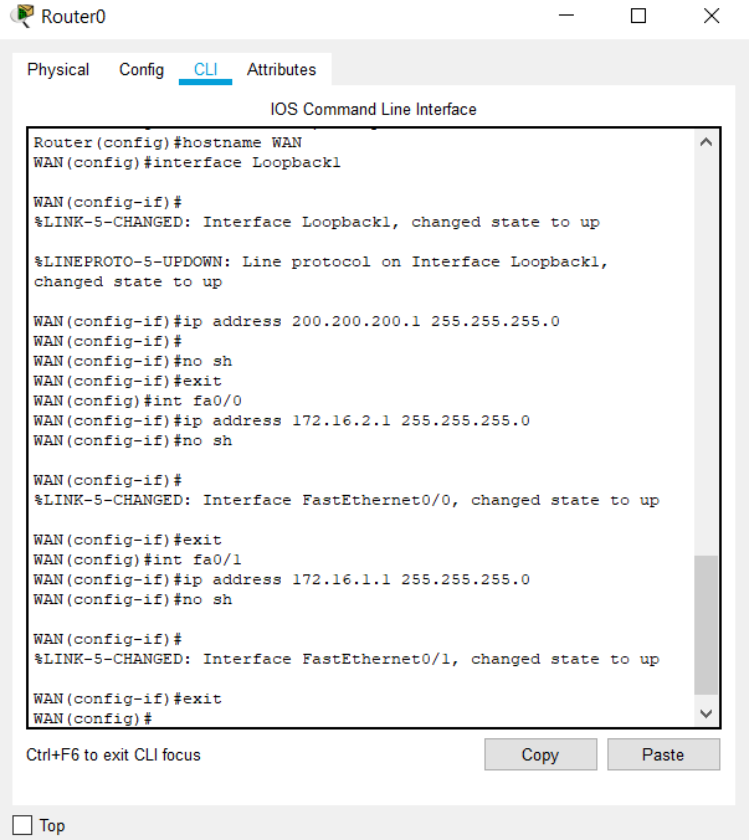


Рисунок 7.2 – Настройка маршрутизатора WAN

7.4.3 После настройки соответствующих IP-адресов выполнили следующие команды для настройки протокола маршрутизации RIP версии 2.

WAN(config)# router rip
WAN(config-router)# version 2
WAN(config-router)# network 172.16.1.0
WAN(config-router)# network 172.16.2.0
WAN(config-router)# network 200.200.200.0
WAN(config-router)# no auto-summary
WAN(config-router)# exit

7.4.4 На следующем рисунке показана маршрутизация RIP версии 2 на маршрутизаторе WAN.

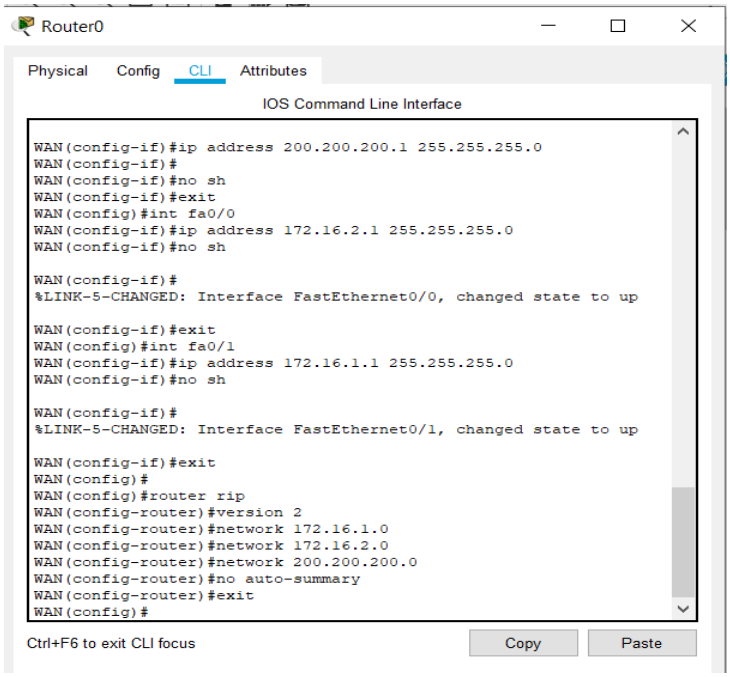


Рисунок 7.3 – Настройка маршрутизатора WAN

7.4.5 После того как настроили IP-адреса и маршрутизацию на маршрутизаторе WAN, пер–ешли к главному маршрутизатору и выполнили следующие команды. Этот маршрутизатор будет действовать как активный маршрутизатор.

7.4.6 Выполните следующие команды, чтобы настроить IP-адрес на интерфейсе Fa0 / 0.

Master(config)# interface Fa0/ 0
Master(config-if)# ip address 10.0.0.10 255.255.255.0
Master(config-if)# no shutdown
Master(config-if)# exit

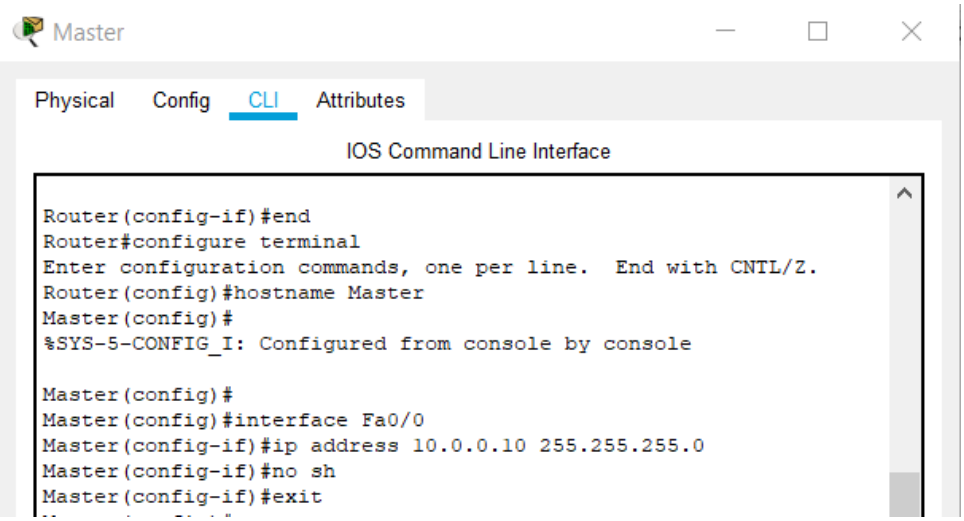


Рисунок 7.4 – Настройка маршрутизатора MASTER

7.4.7 Затем выполнили следующую команду, чтобы определить номер группы (1-4096) и установить 10.0.0.150 в качестве виртуального IP-адреса.

Master(config-if)# standby 1 ip 10.0.0.150

7.4.8 Затем выполнили следующую команду, чтобы установить значение приоритета, вытеснение и интерфейс отслеживания.

Master(config-if)# standby 1 priority 101
Master(config-if)# standby 1 preempt
Master(config-if)# standby 1 track fa0/ 1

7.4.9 Затем выполнили следующие команды, чтобы установить IP-адрес на интерфейсе Fa0 / 1.

Master(config)# interface Fa0/ 1
Master(config-if)# ip address 172.16.1.2 255.255.255.0
Master(config-if)# no shutdown
Master(config-if)# exit

7.4.10 Затем выполнили следующие команды, чтобы настроить маршрутизацию RIP версии 2.

Master(config)# router rip
Master(config-router)# version 2
Master(config-router)# network 172.16.1.0
Master(config-router)# network 10.0.0.0
Master(config-router)# no auto-summary
Master(config-router)# exit

7.4.11 На следующем рисунке показана конфигурация главного маршрутизатора.

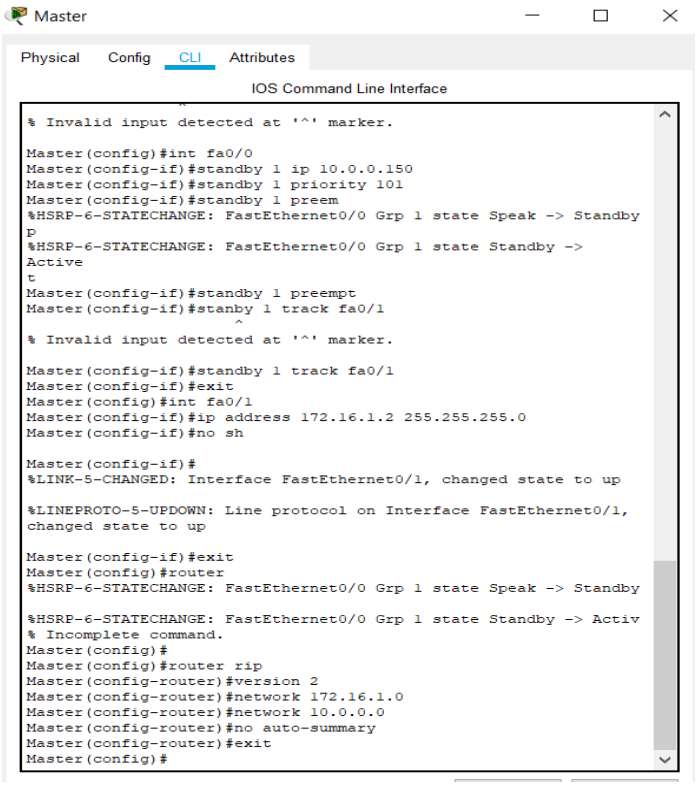


Рисунок 7.5 – Настройка маршрутизатора MASTER

7.4.12 Теперь перешли к Резервному маршрутизатору и выполнили следующие команды. На этом роутере мы установим значение приоритета 99 (ниже, чем у главного роутера).

Backup(config)# interface Fa0/ 0
Backup(config-if)# ip address 10.0.0.20 255.255.255.0
Backup(config-if)# no shutdown

Backup(config-if)# standby 1 ip 10.0.0.150
Backup(config-if)# standby 1 priority 99
Backup(config-if)# standby 1 preempt
Backup(config-if)# exit

Backup(config)# interface Fa0/ 1
Backup(config-if)# ip address 172.16.2.2 255.255.255.0
Backup(config-if)# no shutdown
Backup(config-if)# exit

Backup(config)# router rip
Backup(config-router)# version 2
Backup(config-router)# network 172.16.2.0
Backup(config-router)# network 10.0.0.0
Backup(config-router)# no auto-summary
Backup(config-router)# exit

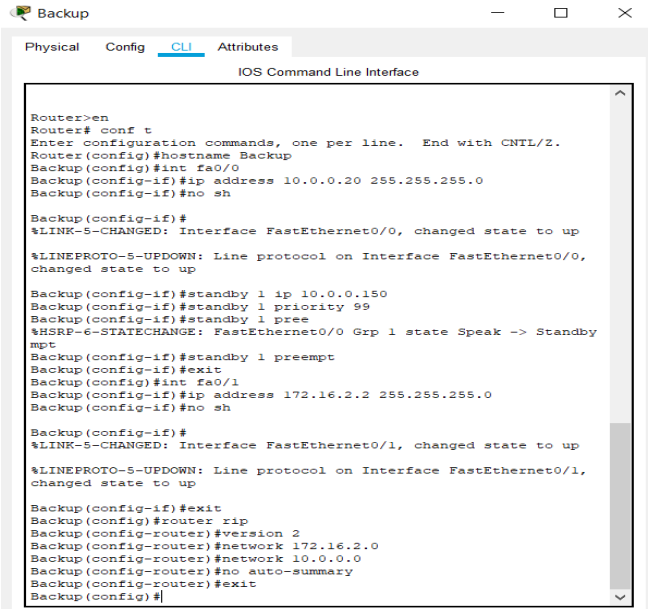


Рисунок 7.6 – Настройка резервного маршрутизатора

7.4.13 После того как настроили протокол маршрутизации HSRP на главном и резервном маршрутизаторах, проверили конфигурацию. Для этого на главном маршрутизаторе выполнили следующую команду.

Master# show standby

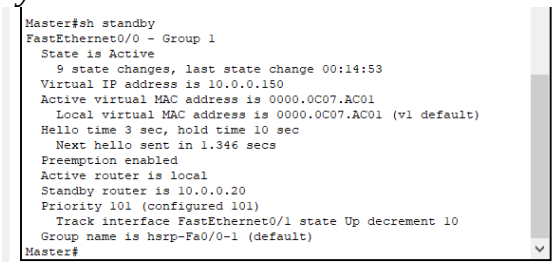


Рисунок 7.7 – Проверка конфигурации

7.4.14 На предыдущем рисунке вы можете видеть, что главный маршрутизатор в настоящее время работает как активный маршрутизатор, поскольку он имеет более высокий приоритет (101), чем резервный маршрутизатор (99).

7.4.15 Чтобы объяснить, что происходит при выходе из строя активного маршрутизатора, мы отключим интерфейс Fa0 / 0 на главном маршрутизаторе. Для этого выполните следующие команды.

Master(config)# int fa0/ 0

Master(config-if)# shutdown

7.4.16 Теперь перейдите к резервному маршрутизатору и выполните следующую команду.

Backup# show standby

```
Backup#
Backup#sh standby
FastEthernet0/0 - Group 1
  State is Active
    4 state changes, last state change 00:20:50
  Virtual IP address is 10.0.0.150
  Active virtual MAC address is 0000.0C07.AC01
    Local virtual MAC address is 0000.0C07.AC01 (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 0.592 secs
  Preemption enabled
  Active router is local
  Standby router is unknown
  Priority 99 (configured 99)
  Group name is hsrp-Fa0/0-1 (default)
Backup#
```

Рисунок 7.8 – Проверка конфигурации

7.4.17 На предыдущем рисунке вы можете видеть, что резервный маршрутизатор становится активным маршрутизатором и берет на себя обязанности по маршрутизации, как только интерфейс основного маршрутизатора выходит из строя. Это то, что делает протокол резервирования.

```
PC0
Physical  Config  Desktop  Programming  Attributes
Command Prompt
C:\>ping 200.200.200.1

Pinging 200.200.200.1 with 32 bytes of data:

Reply from 200.200.200.1: bytes=32 time=2ms TTL=254
Reply from 200.200.200.1: bytes=32 time<1ms TTL=254
Reply from 200.200.200.1: bytes=32 time<1ms TTL=254
Reply from 200.200.200.1: bytes=32 time<1ms TTL=254

Ping statistics for 200.200.200.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 2ms, Average = 0ms

C:\>ping 10.0.0.10

Pinging 10.0.0.10 with 32 bytes of data:

Reply from 10.0.0.10: bytes=32 time=1ms TTL=255
Reply from 10.0.0.10: bytes=32 time<1ms TTL=255
Reply from 10.0.0.10: bytes=32 time<1ms TTL=255
Reply from 10.0.0.10: bytes=32 time<1ms TTL=255

Ping statistics for 10.0.0.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 10.0.0.20

Pinging 10.0.0.20 with 32 bytes of data:

Reply from 10.0.0.20: bytes=32 time<1ms TTL=255
Reply from 10.0.0.20: bytes=32 time<1ms TTL=255
Reply from 10.0.0.20: bytes=32 time=2ms TTL=255
Reply from 10.0.0.20: bytes=32 time=1ms TTL=255

Ping statistics for 10.0.0.20:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 2ms, Average = 0ms
```

Рисунок 7.9 – Ping на маршрутизатор WAN, MASTER, BACKUP с P0

7.5 Задания для самостоятельной работы

7.5.1 Нужно поменять loopback0 и прописать на все настройки маршрутизаторов

7.5.2 На один маршрутизатор добавить протокол EIGRP и проверить работоспособность.

7.5.3 Попинговать все маршрутизаторы, сделать анализ по задержке пакетов.

7.5.4 Приготовить отчет и ответить на контрольные вопросы.

7.6 Контрольные вопросы

1. Опишите протокол HSRP.
2. Что такое Standby router?
3. Что такое Hello Time?
4. Что такое Hold time?

Лабораторная работа № 8. Настройка протоколов HSRP и GLBP

8.1 Цель лабораторный работы: Понять суть работы протоколов HSRP и GLBP.

8.2 Подготовка к работе: Повторить разделы HSRP, GLBP, виртуальный терминал настройки протокола OSPF.

Теоретические описание

GLBP (Gateway Load Balancing Protocol) — проприетарный протокол Cisco, предназначенный для увеличения доступности маршрутизаторов, выполняющих роль шлюза по умолчанию, и балансировки нагрузки между этими маршрутизаторами.

GLBP работает аналогично, но не идентично другим протоколам резервирования шлюза, таким как HSRP и VRRP. Эти протоколы позволяют нескольким маршрутизаторам участвовать в сконфигурированной виртуальной группе маршрутизаторов с общим виртуальным IP-адресом. Один член группы выбирается активным маршрутизатором, в то время как другие остаются неактивными до тех пор, пока не произойдет сбой с активным маршрутизатором. При этом эти резервные маршрутизаторы обладают ресурсами, которые почти не используются в течение всего времени эксплуатации этой системы. GLBP обеспечивает распределение нагрузки на несколько маршрутизаторов (шлюзов), используя один виртуальный IP-адрес и несколько виртуальных MAC-адресов. Каждый хост сконфигурирован с одинаковым виртуальным IP-адресом, и все маршрутизаторы в виртуальной группе участвуют в передаче пакетов.

8.3 Описание лабораторной работы

В этой лабораторной работе вам предстоит выполнить настройку двух протоколов FHRP. В части 2 необходимо настроить протокол Cisco Hot Standby Routing Protocol (HSRP).

В лабораторной работе используются маршрутизаторы с интеграцией сервисов серии Cisco 1941 под управлением ОС Cisco IOS 15.2(4) M3 (образ universalk9). В лабораторной работе используются коммутаторы серии Cisco Catalyst 2960s под управлением ОС Cisco IOS 15.0(2) (образ lanbasek9). Допускается использование коммутаторов и маршрутизаторов других моделей под управлением других версий ОС Cisco IOS. В зависимости от модели устройства и версии Cisco IOS доступные команды и их результаты могут отличаться от приведённых в описании лабораторных работ. Точные

идентификаторы интерфейсов приведены в сводной таблице интерфейсов маршрутизаторов в конце лабораторной работы.

Протокол spanning-tree обеспечивает беспетлевую избыточность между коммутаторами в пределах сети LAN. Однако оно не предоставляет избыточные шлюзы по умолчанию для устройств оконечных пользователей в пределах сети на случай сбоя одного из маршрутизаторов. Протоколы обеспечения избыточности на первом хопе (First Hop Redundancy Protocols, FHRP) предоставляют избыточные шлюзы по умолчанию для оконечных устройств. При этом конфигурация оконечного пользователя не требуется.

8.4 Выполнение работы:

Топология сети

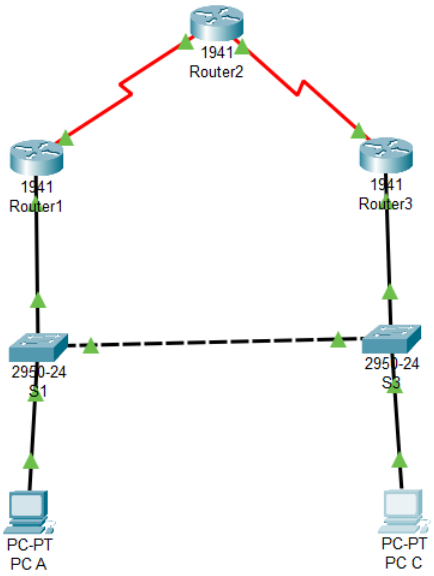


Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
R1	G0/1	192.168.1.1	255.255.255.0	N/A
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	N/A
R2	S0/0/0	10.1.1.2	255.255.255.252	N/A
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	N/A
	Lo1	209.165.200.225	255.255.255.224	N/A
R3	G0/1	192.168.1.3	255.255.255.0	N/A
	S0/0/1	10.2.2.1	255.255.255.252	N/A
S1	VLAN 1	192.168.1.11	255.255.255.0	192.168.1.1
S3	VLAN 1	192.168.1.13	255.255.255.0	192.168.1.3
PC-A	NIC	192.168.1.31	255.255.255.0	192.168.1.1
PC-C	NIC	192.168.1.33	255.255.255.0	192.168.1.3

Рисунок 8.1 – Таблица адресации

Часть 1. Построение сети и проверка соединения

Часть 2. Настройка обеспечения избыточности на первом хопе с помощью HSRP

8.4.1 Часть 1. Построение сети и проверка соединения

В первой части вам предстоит настроить топологию сети и выполнить базовые настройки, например, IP-адреса интерфейса, статическую маршрутизацию, доступ к устройствам и пароли.

Шаг 1: Подключите кабели в сети в соответствии с топологией. Подключите устройства в соответствии с диаграммой топологии и выполните разводку кабелей по необходимости.

```
Router>
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#router ospf 1
Router(config-router)#do show ip route connected
 C    10.1.1.0/30  is directly connected, Serial0/1/0
 C    192.168.1.0/24  is directly connected, GigabitEthernet0/1

Router(config-router)#network 10.1.1.0 0.0.0.3 area 0
Router(config-router)#192.168.1.0 0.0.0.255 area 0
                     ^
% Invalid input detected at '^' marker.

Router(config-router)#network 192.168.1.0 0.0.0.255 area 0
Router(config-router)#
01:04:06: %OSPF-5-ADJCHG: Process 1, Nbr 209.165.200.225 on Serial0/1/0 from LOADING to FULL, Loading Done

01:07:27: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.1.3 on GigabitEthernet0/1 from LOADING to FULL, Loading Done
```

Рисунок 8.2 – Настройка Роутера 1

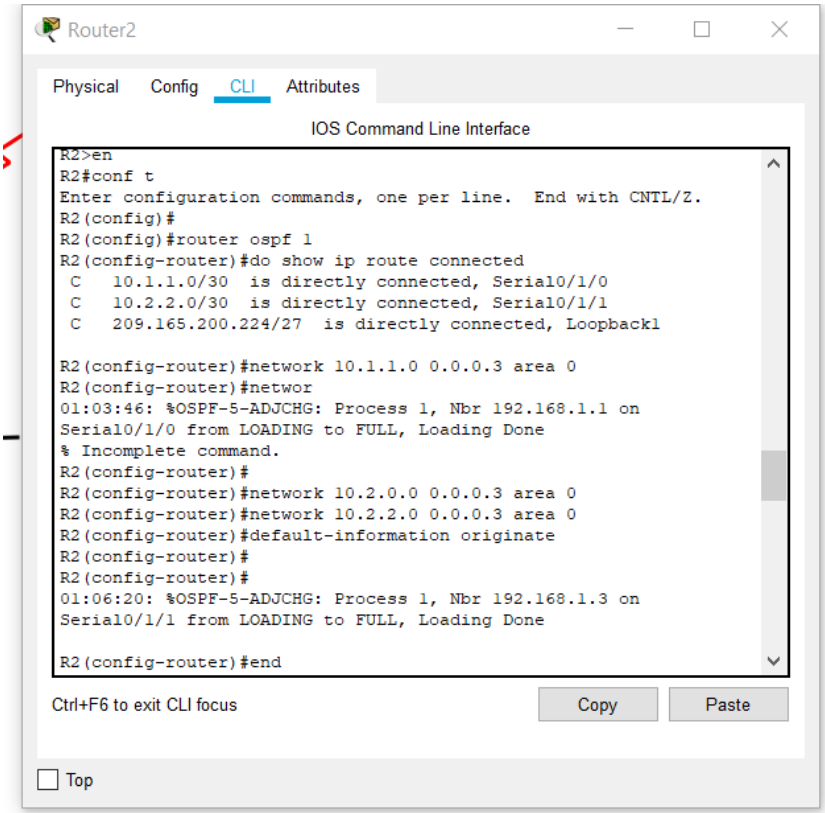


Рисунок 8.3 – Настройка Роутера 2

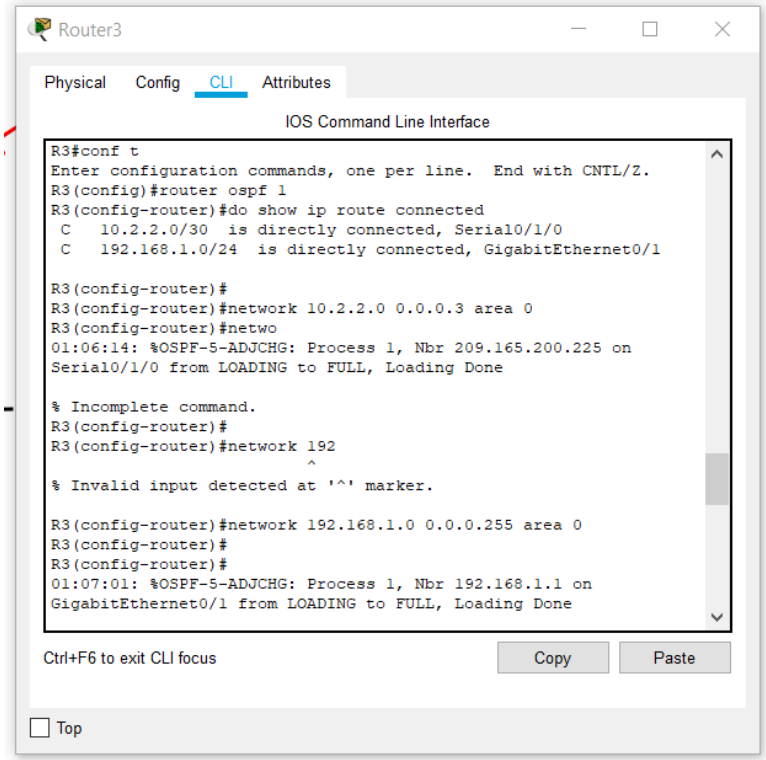


Рисунок 8.4 – Настройка Роутера 3

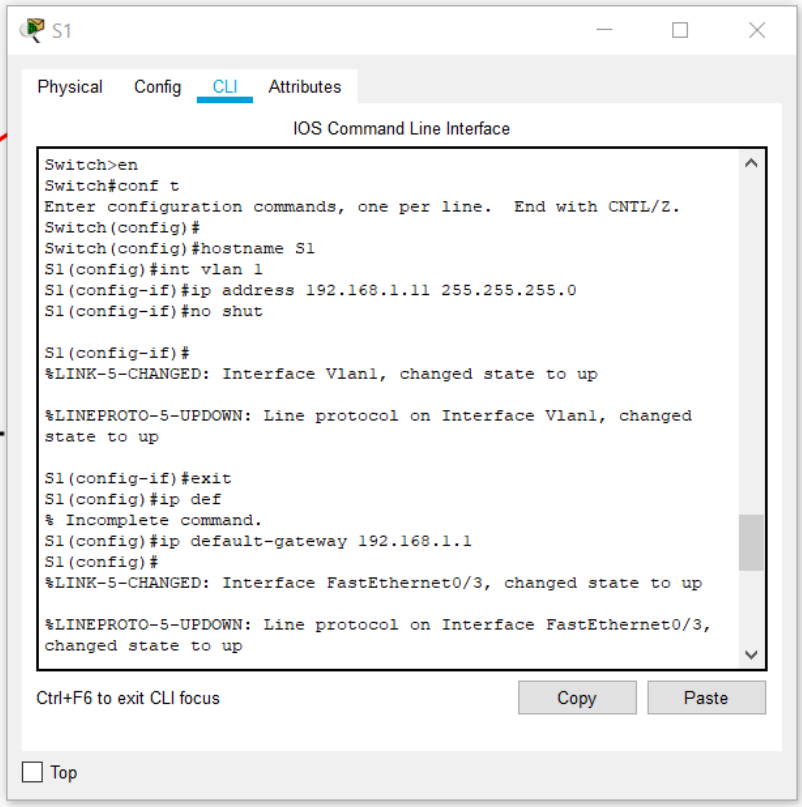


Рисунок 8.5 – Настройка коммутатора S1

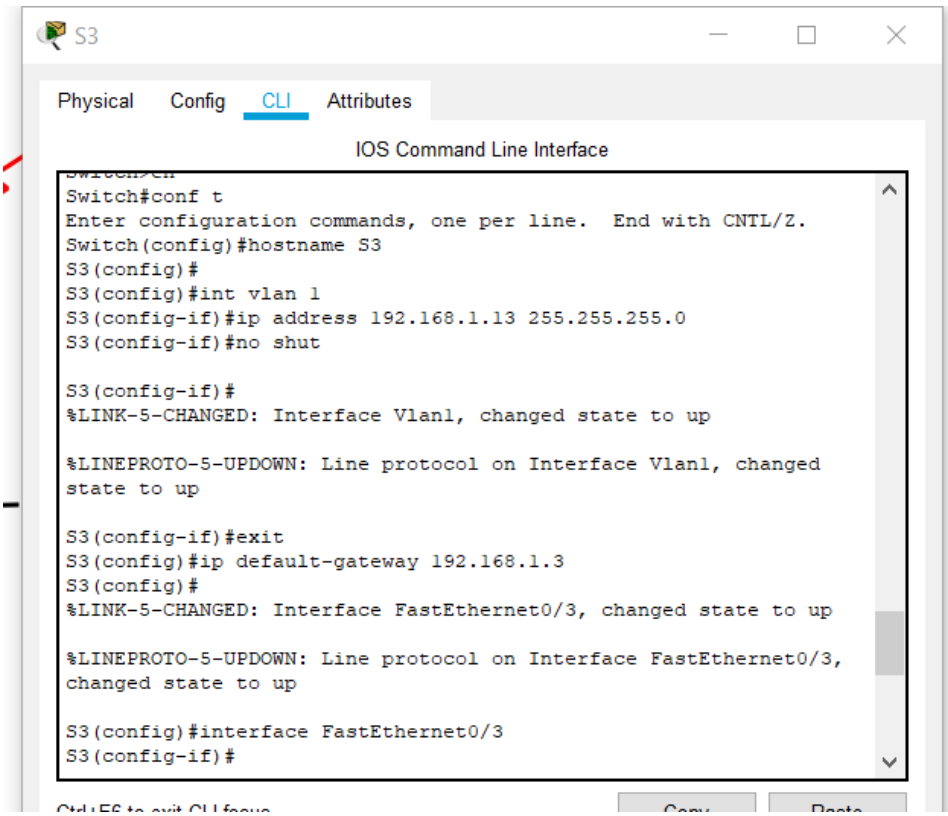


Рисунок 8.6 – Настройка коммутатора S3

Шаг 2: Настройте узлы ПК.

Шаг 3: Выполните инициализацию и перезагрузку маршрутизатора и коммутаторов.

Шаг 4: Настройте базовые параметры каждого маршрутизатора.

a. Отключите поиск DNS.

b. Присвойте имена устройствам в соответствии с топологией.

c. Настройте IP-адреса для маршрутизаторов, указанных в таблице адресации.

d. Установите тактовую частоту на 128000 для всех последовательных интерфейсов маршрутизатора DCE.

e. Назначьте class в качестве зашифрованного пароля доступа к привилегированному режиму EXEC. f. Назначьте cisco в качестве пароля виртуального терминала VTY и активируйте вход.

g. Настройте logging synchronous, чтобы сообщения от консоли не могли прерывать ввод команд.

h. Сохраните текущую конфигурацию в загрузочную конфигурацию.

Шаг 5: Настройте базовые параметры каждого коммутатора.

a. Отключите поиск DNS.

b. Присвойте имена устройствам в соответствии с топологией.

c. Назначьте class в качестве зашифрованного пароля доступа к привилегированному режиму EXEC.

d. Настройте IP-адреса для коммутаторов, указанных в таблице адресации.

e. На каждом коммутаторе настройте шлюз по умолчанию.

f. Назначьте cisco в качестве пароля виртуального терминала VTY и активируйте вход.

g. Настройте logging synchronous, чтобы сообщения от консоли не могли прерывать ввод команд.

h. Сохраните текущую конфигурацию в загрузочную конфигурацию.

Шаг 6: Проверьте подключение между PC-A и PC-C.

Отправьте эхо-запрос с компьютера PC-A на компьютер PC-C.

Если эхо-запросы не проходят, выполните отладку основных настроек устройства.

Примечание. Для успешной передачи эхо-запросов может потребоваться отключение брандмауэра.

Шаг 7: Настройте маршрутизацию.

a. Настройте протокол EIGRP на маршрутизаторах и используйте значение административной дистанции, равное 1. Добавьте в процесс EIGRP все сети, кроме 209.165.200.224/27.

1. Добавьте в процесс EIGRP все сети, кроме 209.165.200.224/27.

b. Настройте маршрут по умолчанию на R2, используя Lo1 в качестве выходного интерфейса к сети 209.165.200.224/27, и перераспределите этот маршрут в процесс EIGRP.

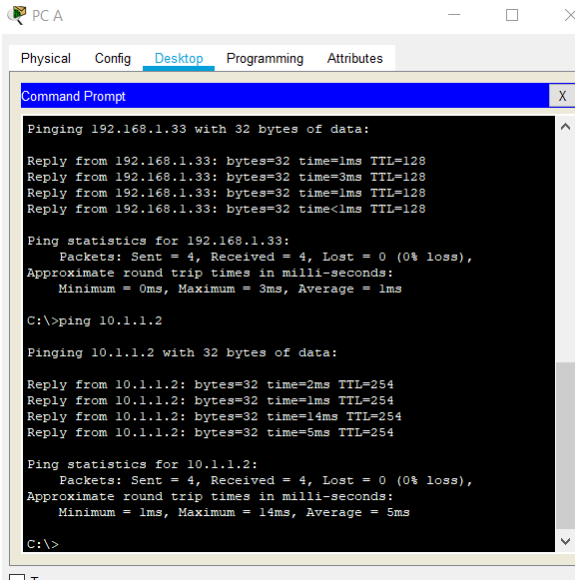
Шаг 8: Проверьте соединение.

a. Эхо-запросы, отправленные от PC-A в каждый интерфейс на R1, R2, R3 и PC-C, должны быть успешными.

b. Все эхо-запросы выполнены успешно? _____

c. b. Эхо-запросы, отправленные от PC-C в каждый интерфейс на R1, R2, R3 и PC-A, должны быть успешными. Все эхо-запросы выполнены успешно?

Успешно идут трафики от двух компьютеров друг в друга и на роутеры.



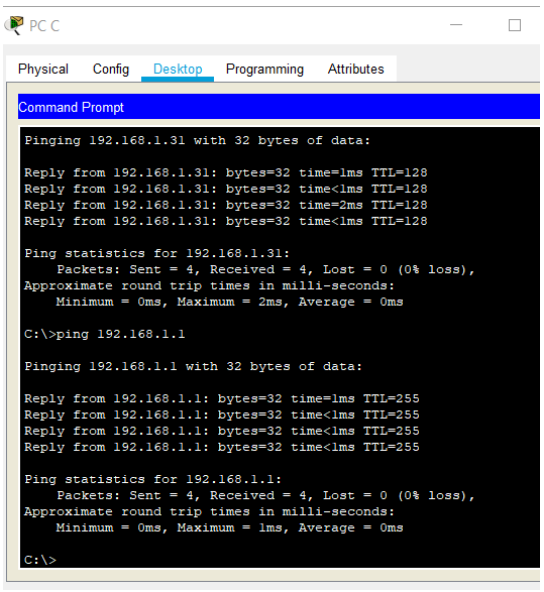


Рисунок 8.7 – Проверка отправки пакетов

8.4.2 Часть 2. Настройка обеспечения избыточности на первом хопе с помощью HSRP

Даже если топология спроектирована с учетом избыточности (два маршрутизатора и два коммутатора в одной сети LAN), оба компьютера, PC-A и PC-C, необходимо настраивать с одним адресом шлюза. PC-A использует R1, а PC-C — R3. В случае сбоя на одном из этих маршрутизаторов или интерфейсов маршрутизаторов компьютер может потерять подключение к сети Интернет. В части 2 вам предстоит изучить поведение сети до и после настройки протокола HSRP. Для этого вам понадобится определить путь, по которому проходят пакеты, чтобы достичь loopback-адреса на R2.

Шаг 1: Определите путь интернет-трафика для PC-A и PC-C.

a. В командной строке на PC-A введите команду tracert для loopback-адреса 209.165.200.225 на маршрутизаторе R2.

b. В командной строке на PC-C введите команду tracert для loopback-адреса 209.165.200.225 на маршрутизаторе R2.

Шаг 2: Запустите сеанс эхо-тестирования на PC-A и разорвите соединение между S1 и R1.

a. В командной строке на PC-A введите команду ping –t для адреса 209.165.200.225 на маршрутизаторе R2. Убедитесь, что окно командной строки открыто. Примечание. Чтобы прервать отправку эхо-запросов, нажмите комбинацию клавиш Ctrl+C или закройте окно командной строки.

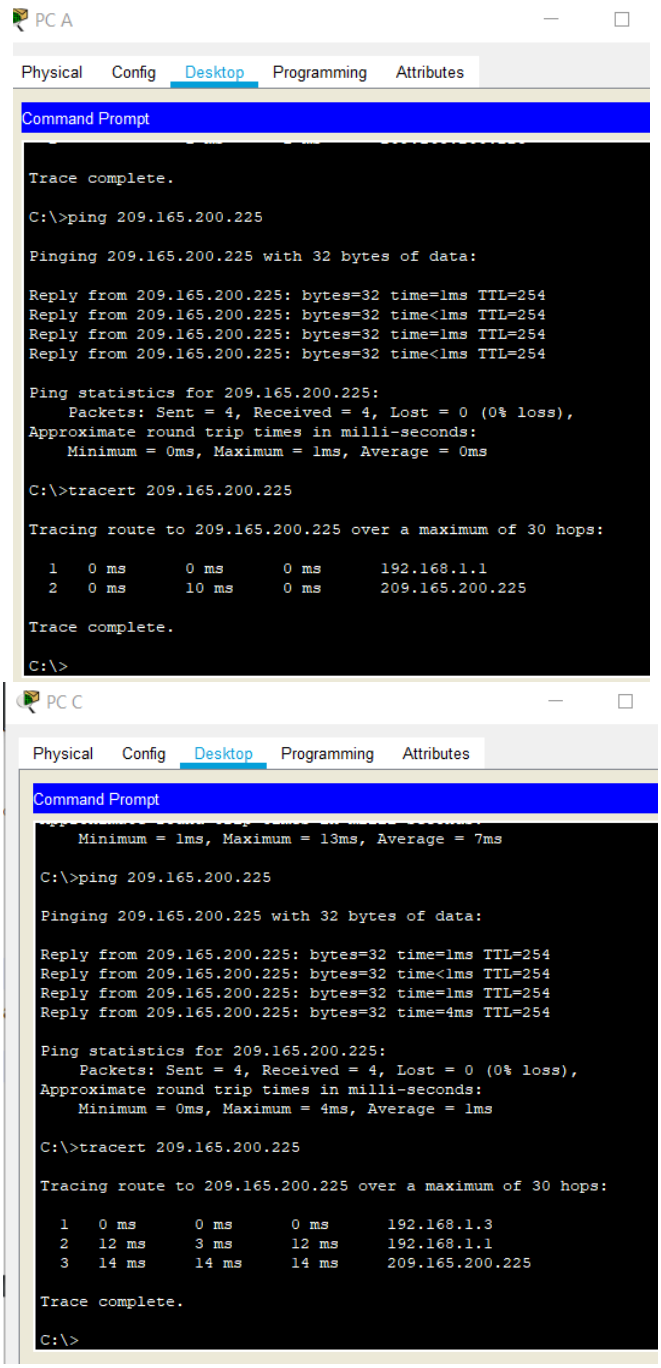


Рисунок 8.8 – Проверка отправки пакетов

Шаг 3: Настройте HSRP на R1 и R3. В этом шаге вам предстоит настроить HSRP и изменить адрес шлюза по умолчанию на компьютерах PC-A, PC-C, S1 и коммутаторе S2 на виртуальный IP-адрес для HSRP. R1 назначается активным маршрутизатором с помощью команды приоритета HSRP.

а. Настройте протокол HSRP на маршрутизаторе R1.

```
R1(config)# interface g0/1
R1(config-if)# standby 1 ip 192.168.1.254
R1(config-if)# standby 1 priority 150
R1(config-if)# standby 1 preempt
```

b. Настройте протокол HSRP на маршрутизаторе R3.

```
R3(config)# interface g0/1
R3(config-if)# standby 1 ip 192.168.1.254
```

c. Проверьте HSRP, выполнив команду show standby на R1 и R3.

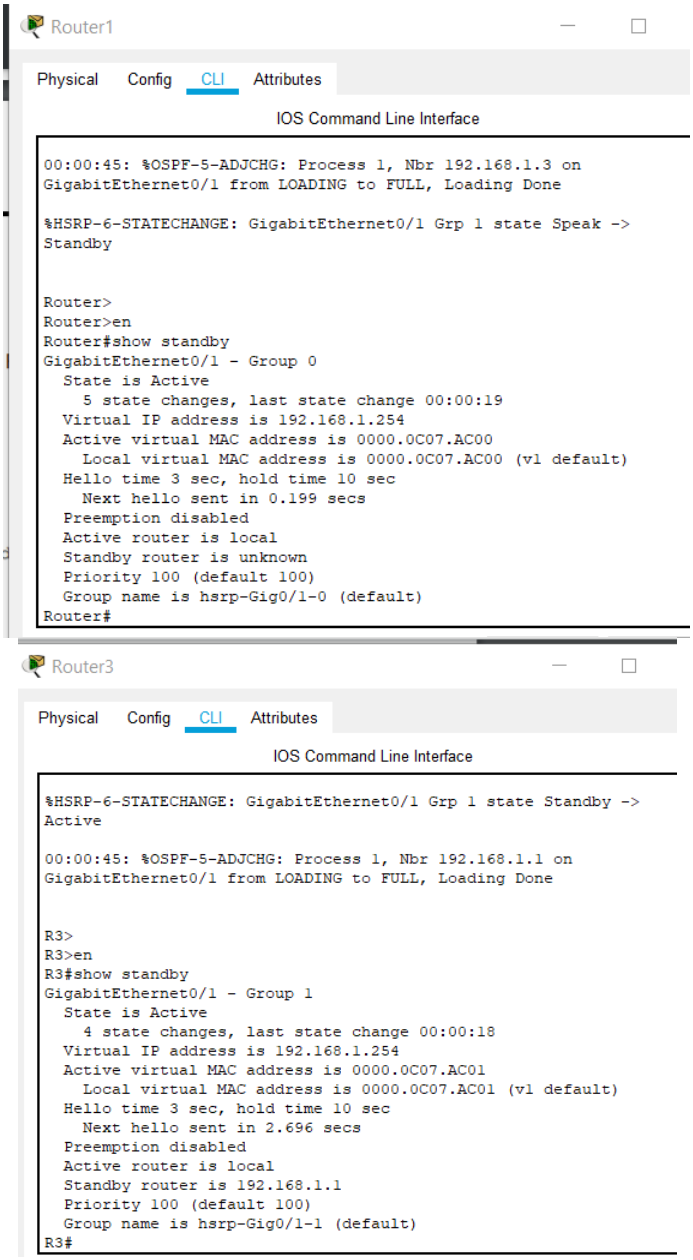


Рисунок 8.9 – Проверка HSRP R1 и R3 (standby)

d. Используйте команду show standby brief на R1 и R3, чтобы просмотреть сводку состояния HSRP. Пример выходных данных приведен ниже.

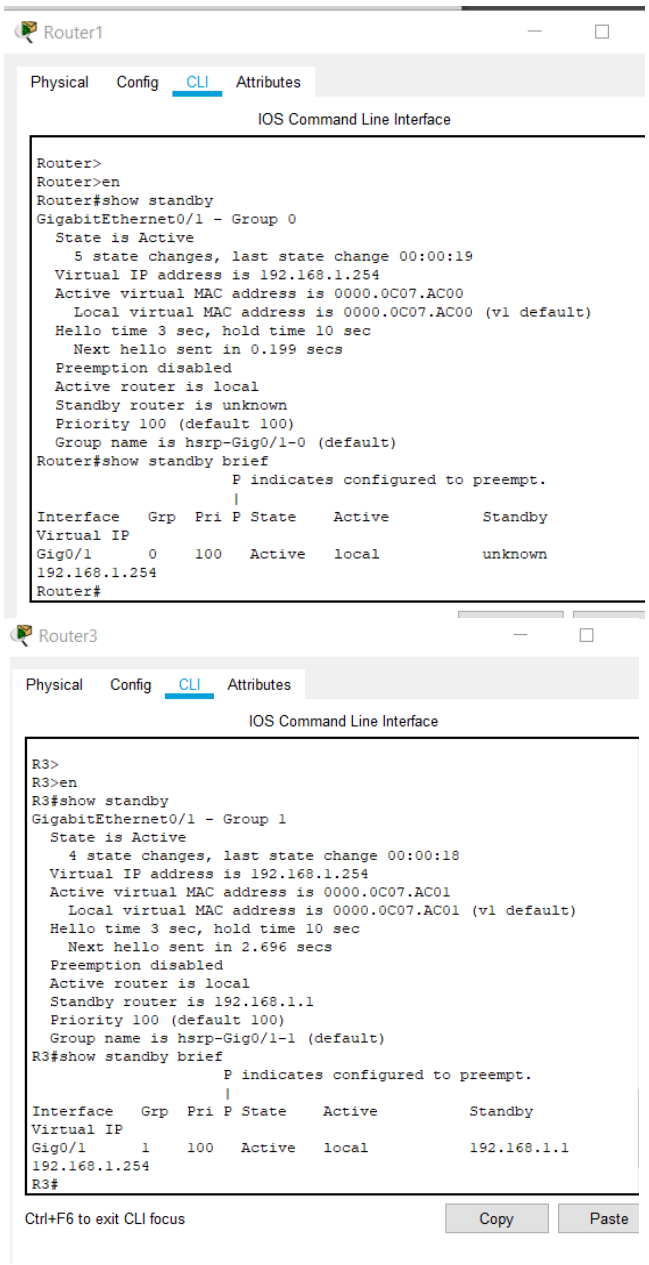


Рисунок 8.10 – Проверка HSRP R1 и R3 (brief)

8.5 Задания для самостоятельной работы

8.5.1 Поменять ip-адреса маршрутизаторах.

8.5.2 Поменять ip-адреса коммутаторах.

8.5.3 Проверить работоспособность сети через show standby и show standby brief.

8.5.4 Сделать отчет и ответить на контрольные вопросы

8.5 Контрольные вопросы

1 Опишите протокол GLBP.

2 В чем разница между протоколами GLBP и HSLP?

3 В чем преимущества GLBP протокола?

Лабораторная работа № 9. Исследование настройки NAT с помощью Access list.

9.1 Цель работы: исследование настройки NAT.

9.2 Подготовка к работе:

Повторить разделы: создание стандартных технологий локальных сетей; коммутация сообщений, назначение IP-протокола, модель OSI, различие между сообщением и сигналом, определение пакета, кадра, фрейма.

Теоретическое описание

NAT (от англ. Network Address Translation — «преобразование сетевых адресов») — это механизм в сетях TCP/IP, позволяющий преобразовывать IP-адреса транзитных пакетов. Также имеет названия IP Masquerading, Network Masquerading и Native Address Translation.

Существует 3 базовых концепции трансляции адресов: статическая (Static Network Address Translation), динамическая (Dynamic Address Translation), маскарадная (NAPT, NAT Overload, PAT).

Статический NAT — отображение незарегистрированного IP-адреса на зарегистрированный IP-адрес на основании один к одному. Особенно полезно, когда устройство должно быть доступным снаружи сети.

Динамический NAT — отображает незарегистрированный IP-адрес на зарегистрированный адрес из группы зарегистрированных IP-адресов. Динамический NAT также устанавливает непосредственное отображение между незарегистрированными и зарегистрированными адресами, но отображение может меняться в зависимости от зарегистрированного адреса, доступного в пуле адресов, во время коммуникации.

Перегруженный NAT (NAPT, NAT Overload, PAT, маскарадинг) — форма динамического NAT, который отображает несколько незарегистрированных адресов в единственный зарегистрированный IP-адрес, используя различные порты. Известен также как PAT (Port Address Translation). При перегрузке каждый компьютер в частной сети транслируется в тот же самый адрес, но с различным номером порта.

9.3 Описание лабораторной работы

В данной лабораторной работе используются маршрутизаторы, коммутаторы, ПК через програмное обеспечение Cisco. В данной лабораторной работе вы должны построить сеть доступа с технологиями NAT (PAT), научиться настраивать серверы и коммутаторы. После всех выполненных команд нужно проверить работоспособность сети.

9.4 Рабочее задание:

Осуществить настройку PAT и настройку Static NAT.

9.4.1 Схема подключения

Соберем сеть с двумя серверами и коммутатором. Настроить NAT и публичный сервер для интернет-провайдера.

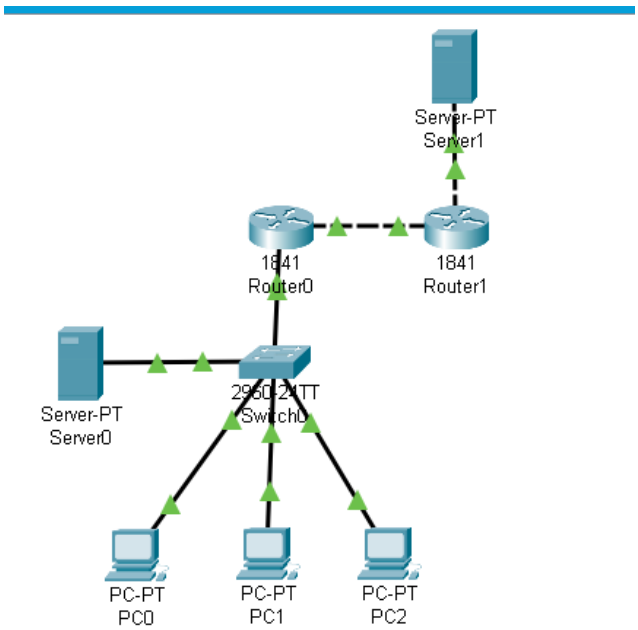


Рисунок 9.1 – Схема соединения

Для начала на локальную сеть нужно настроить все ПК и Server -PT 0 и задать ip-адреса.

Для PC0 ping 192.168.2.2
Для PC1 ping 192.168.2.3
Для PC2 ping 192.168.2.4
Для Server0 ping 192.168.3.2

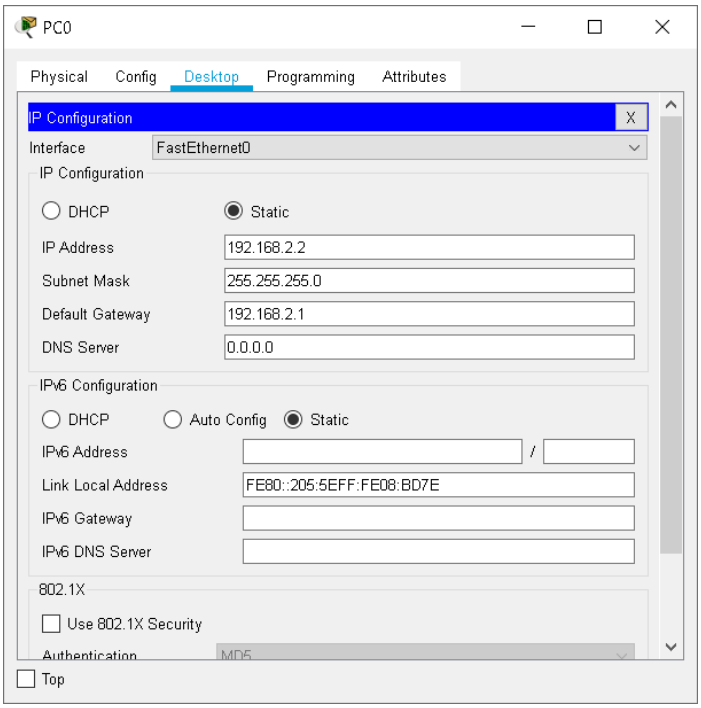


Рисунок 9.2 – Конфигурация IP-адресов

Заходим в CLI интерфейс коммутатора Switch0 и пишем следующие команды.

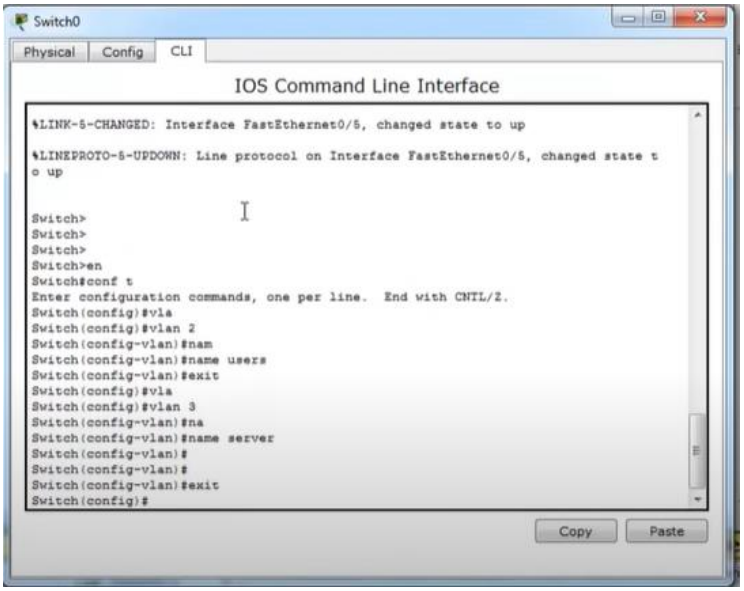


Рисунок 9.3 – CLI интерфейс коммутатора Switch0

Vlan 2 –для пользователей (будут относиться порты fa 0/3, fa 0/4, fa 0/5).

Vlan 3 – для серверов (будет относиться порт fa 0/2).

Fa 0/1 порт будет транкинговым, так как оба vlan будут приземляться к маршрутизатору.

```
Switch(config)#int fa0/1
Switch(config-if)#sw
Switch(config-if)#switchport mod
Switch(config-if)#switchport mode tr
Switch(config-if)#switchport mode trunk
Switch(config-if)#sw
Switch(config-if)#switchport tr
Switch(config-if)#switchport trunk vl
Switch(config-if)#switchport trunk a
Switch(config-if)#switchport trunk allowed lv
Switch(config-if)#switchport trunk allowed vl
Switch(config-if)#switchport trunk allowed vlan 2,3
Switch(config-if)#
Switch(config-if)#
Switch(config-if)#end
```

Рисунок 9.4 – Настройки vlan 2, 3

Затем проверяем порты через команду *show run*.

```
Switch0
Physical  Config  CLI
IOS Command Line Interface
!
interface FastEthernet0/1
 switchport trunk allowed vlan 2-3
 switchport mode trunk
!
interface FastEthernet0/2
 switchport access vlan 3
 switchport mode access
!
interface FastEthernet0/3
 switchport access vlan 2
 switchport mode access
!
interface FastEthernet0/4
 switchport access vlan 2
 switchport mode access
!
interface FastEthernet0/5
 switchport access vlan 2
 switchport mode access
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
 --More--
Copy  Paste
```

Рисунок 9.5 – Проверка работспособности vlan 2, 3

Затем заходим на маршрутизатор Router0 и прописываем для vlan 2.

```
Router0
Physical  Config  CLI
IOS Command Line Interface
Router(config-if)#exit
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#int fa0/1.2
Router(config-subif)#
%LINK-5-CHANGED: Interface FastEthernet0/1.2, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1.2, changed state
 to up

Router(config-subif)#
Router(config-subif)#
Router(config-subif)#enc
Router(config-subif)#encapsulation do
Router(config-subif)#encapsulation dot1Q 2
Router(config-subif)#ip add
Router(config-subif)#ip address 192.168.2.1 255.255.255.0
Router(config-subif)#
Router(config-subif)#no shut
Router(config-subif)#no shutdown
Router(config-subif)#exit
Router(config)#
Router(config)#
Router(config)#
Copy  Paste
```

Рисунок 9.6 – Настройки для vlan 2

Затем заходим на маршрутизатор Router 0 и прописываем для vlan 3.

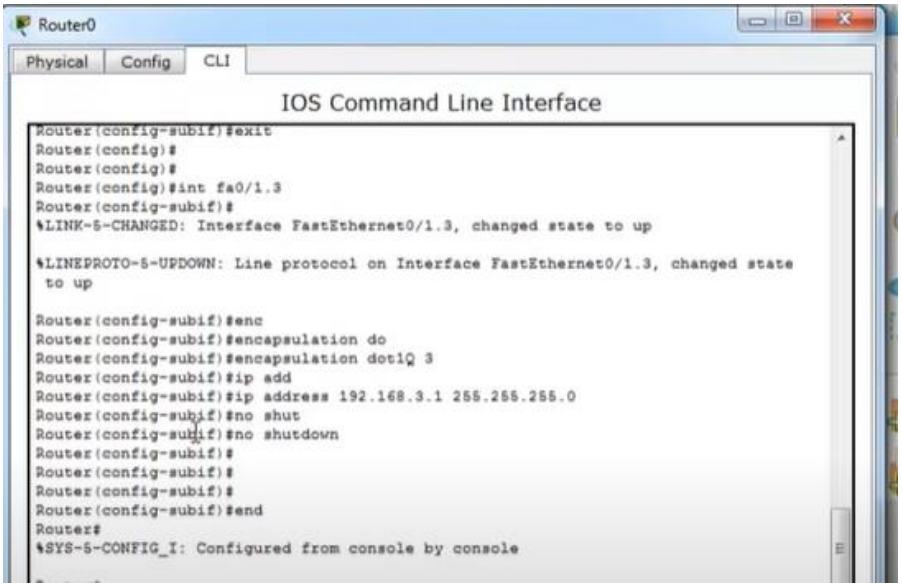


Рисунок 9.7 – Настройки для vlan 3

Далее проверяем через команду *show run*.

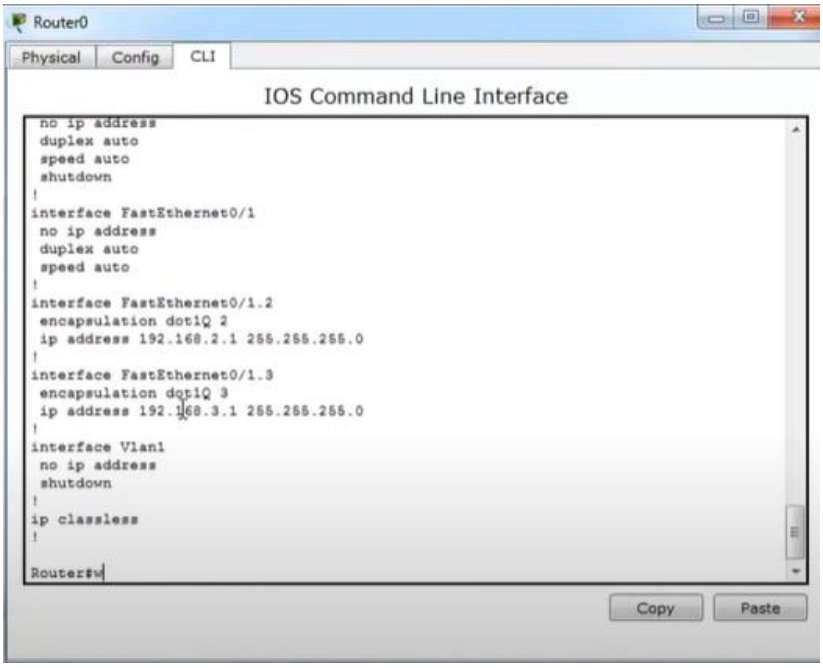


Рисунок 9.8 – Проверка работоспособности vlan 2, 3

Чтобы проверить правильность настройки прописания команд заходим в ПК и проверяем сервер и шлюз.

.

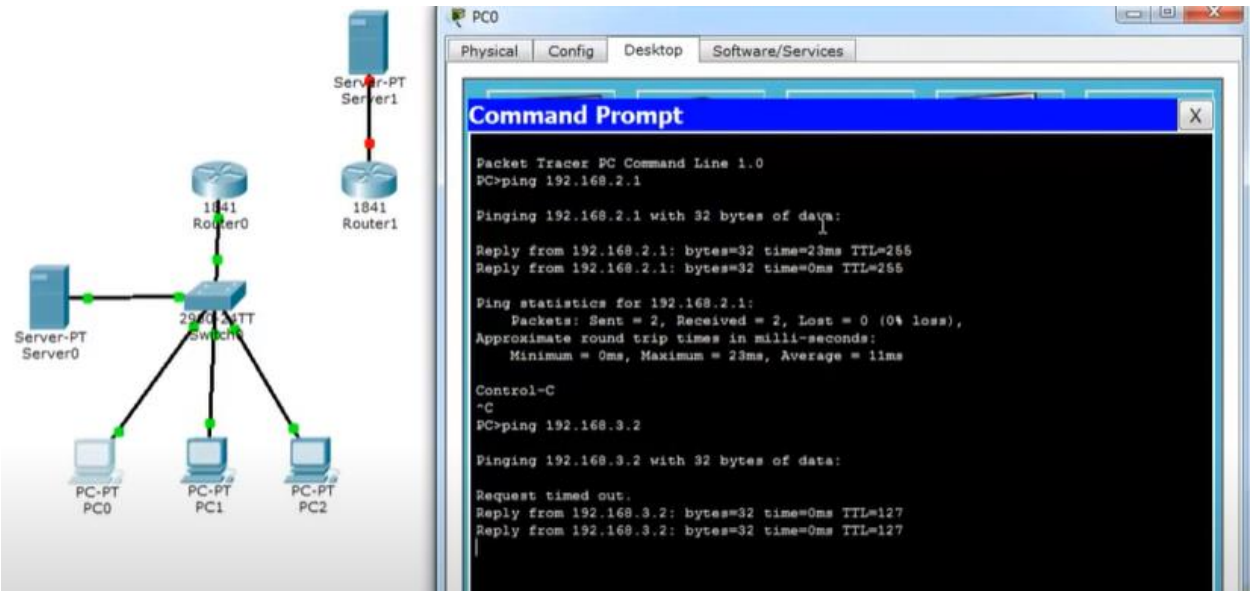


Рисунок 9.9 – Проверка работоспособности сервера и шлюза

После успешного пинга можно убедиться, что правильно настроили локальную сеть.

9.4.2 Локальную сеть подключаем к сети Интернет (прописываем белые ip адреса).

Для начала соединяем два маршрутизатора через порты fa 0/0.

Для маршрутизатора R1 прописываем следующие команды:

enable
configure terminal
interface fa0/0
ip address 213.234.10.1 255.255.255.252
no shurdown
exit

Далее прописываем белый ip адрес для Server1
configure terminal
interface fa0/1
ip address 213.234.10.1 255.255.255.252
no shurdown
exit

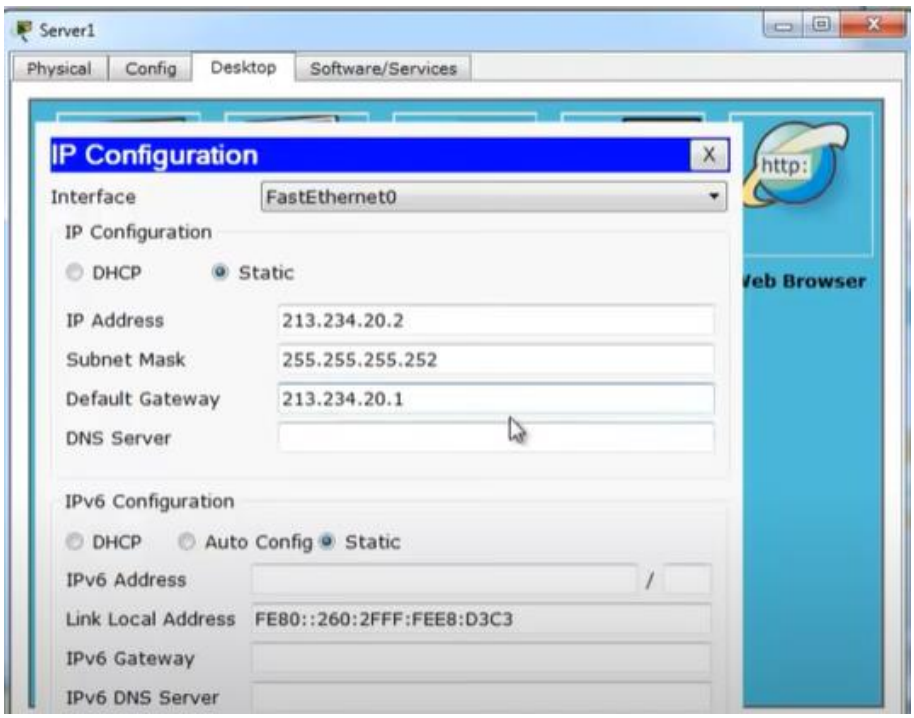


Рисунок 9.10 – Статистический режим для сервера1

Далее заходим в CLI Router 0, прописываем ip-адреса, которые нам провайдер выделил.

configure terminal
interface fa0/0
ip address 213.234.10.1 255.255.255.252
end

Добавляем шлюз по умолчанию
configure terminal
ip route 0.0.0.0 0.0.0.0 213.234.10.1
end
Далее проверяем связь между интернет-провайдером.

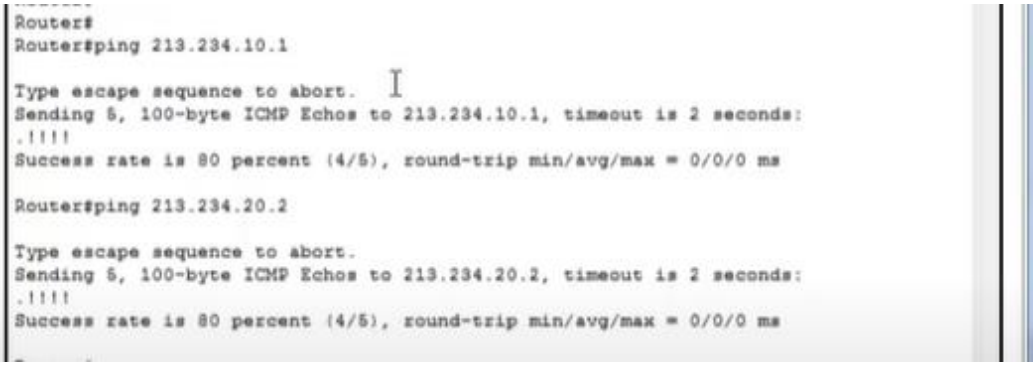


Рисунок 9.11 – Проверка связи между интернет-провайдером

На Router 0 настраиваем NAT для внешней и внутренней связи

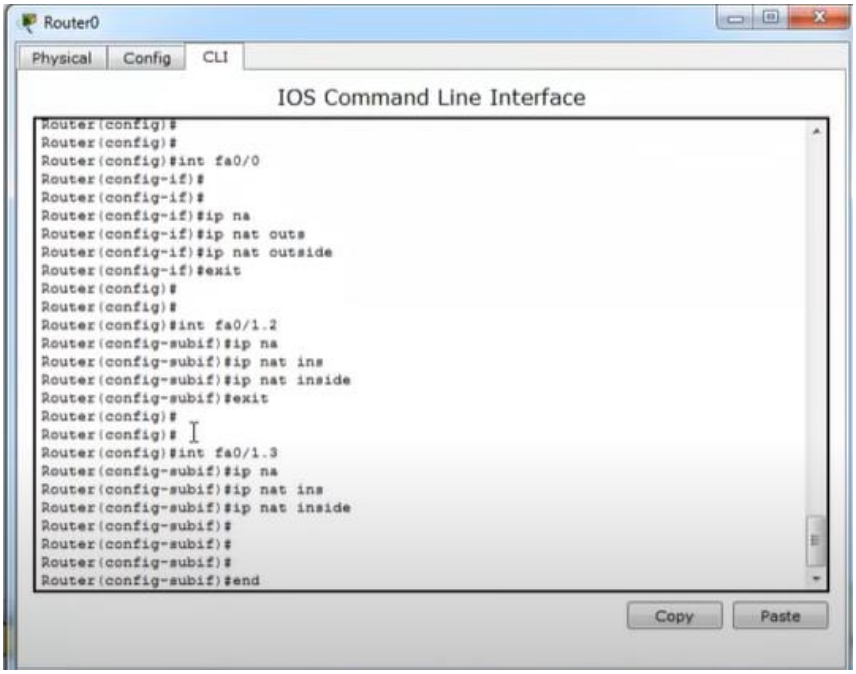
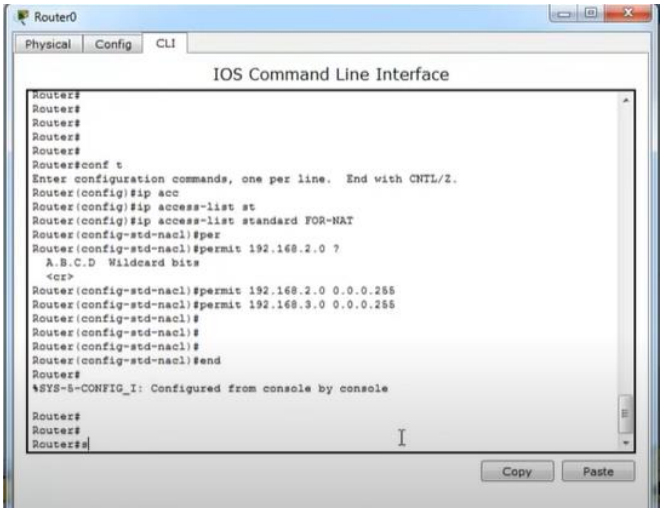


Рисунок 9.12 – Настройки NAT

Далее прописываем Access-list.



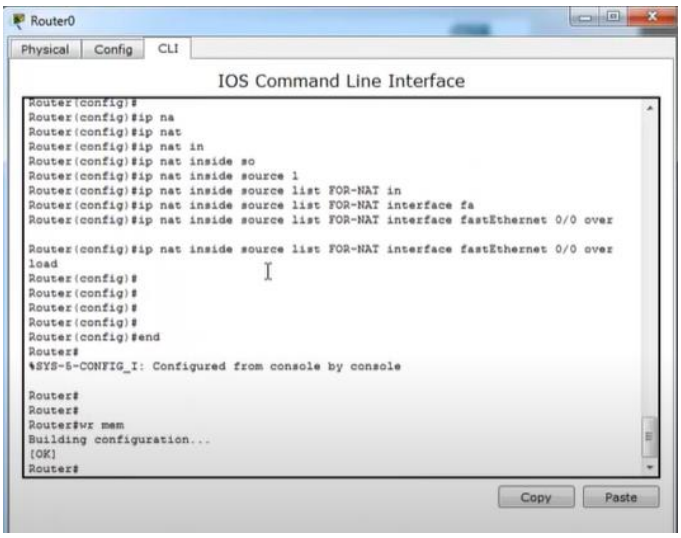


Рисунок 9.13 – Настройки Access-list

Проверям пинг на публичный сервер через ПК.

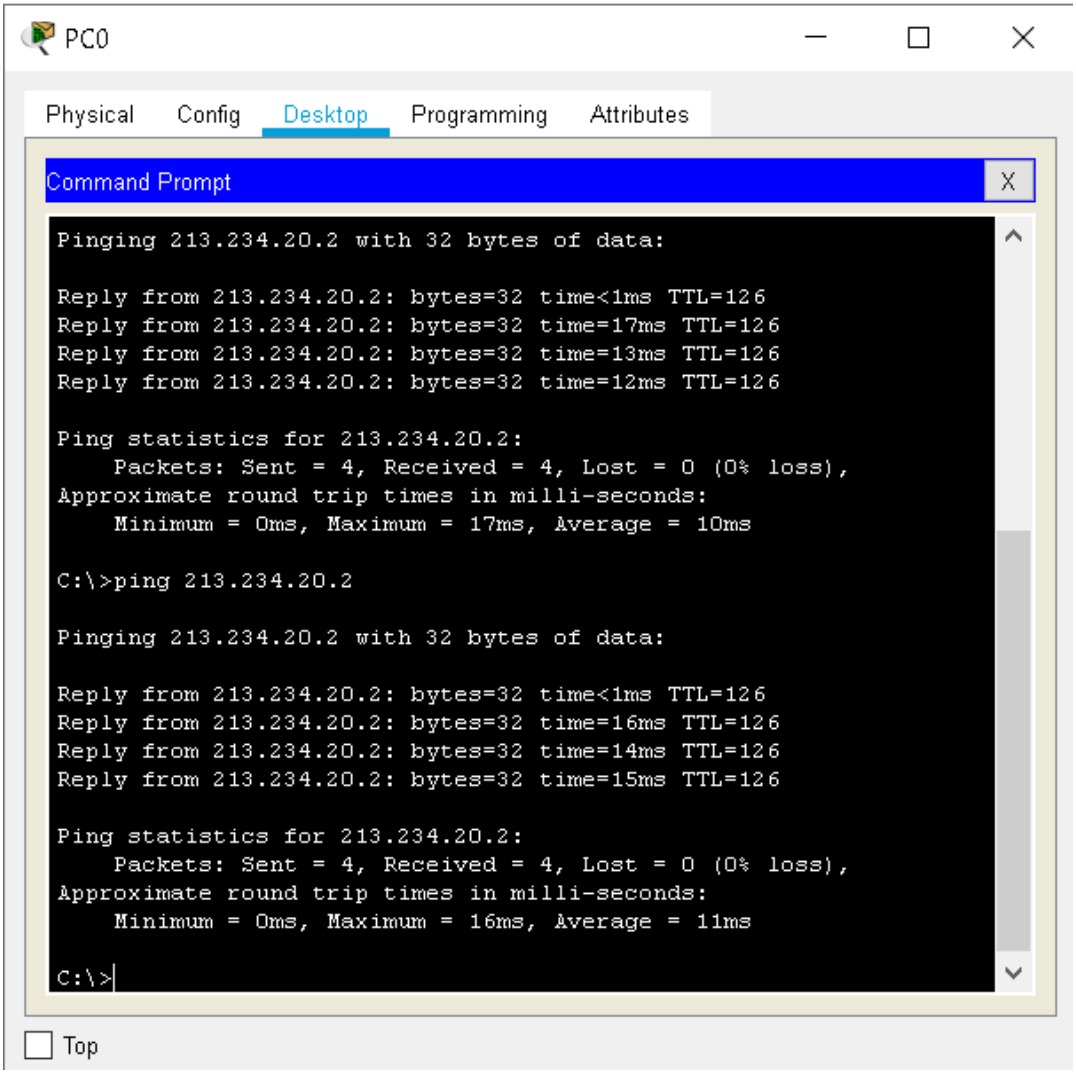


Рисунок 9.14 – Проверка работы публичного сервера

9.5 Контрольные вопросы:

1. Опишите PAT.
2. Преимущества и недостатки NAT.
3. Что подразумевает NAT loopback?
4. Отличия между статистическим и динамическим NAT.

Лабораторная работа № 10. Настройка списка доступа Access lis

10.1 Цель работы: научиться настроить список доступа для маршрутизаторов.

10.2 Подготовка к работе:

Повторить разделы: создание стандартных технологий локальных сетей; коммутация сообщений, назначение IP-протокола, модель OSI, различие между сообщением и сигналом, определение пакета, кадра, фрейма.

Теоретическое описание

ACL (Access Control List) — это набор текстовых выражений, которые что-то разрешают либо что-то запрещают. Обычно ACL разрешает или запрещает IP-пакеты, но помимо всего прочего он может заглядывать внутрь IP-пакета, просматривать тип пакета, TCP и UDP порты. Также ACL существует для различных сетевых протоколов (IP, IPX, AppleTalk и так далее). В основном применение списков доступа рассматривают с точки зрения пакетной фильтрации, то есть пакетная фильтрация необходима в тех ситуациях, когда у вас стоит оборудование на границе Интернет и вашей частной сети и нужно отфильтровать ненужный трафик.

Access List-ы используются для:

- Пакетной фильтрации
- NAT
- VPN
- QoS
- Разграничения доступа к оборудованию
- Policy Based Routing

Виды Access List-ов:

- Стандартыне
- Расширенные
- Динамические
- Рефлексивные
- Временные

Access List-ы применяются в двух направлениях:

1. На входящий трафик
2. На исходящий трафик

10.3 Описание лабораторной работы

В данной лабораторной работе используется маршрутизаторы, коммутаторы, ПК через програмное обеспечение Cisco. В данной лабораторной

работе вы должны настроить список доступа. После всех выполненных команд нужно проверить работоспособность сети.

10.4 Рабочее задание:

Осуществить настройку ACL.

10.4.1 Схема подключения

Соберем сеть с двумя серверами, маршрутизаторами и коммутатором. Настроить ACL и публичный сервер для интернет-провайдера. У нас имеется 4 сегмента: администрация, бухгалтерия, админ и сегмент 1С.

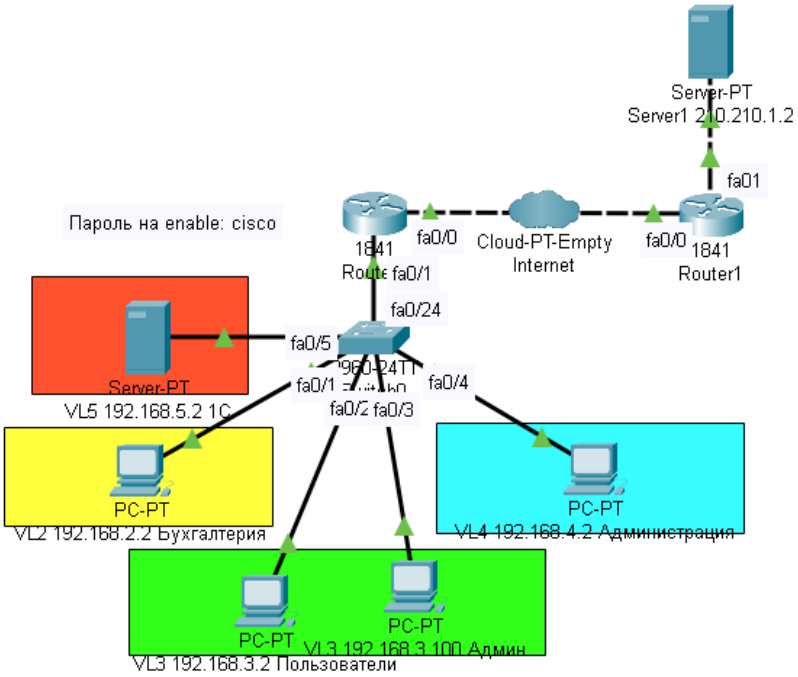


Рисунок 10.1 – Схема соединения

Для начала нужно соединить коммутатор со всеми vlan.

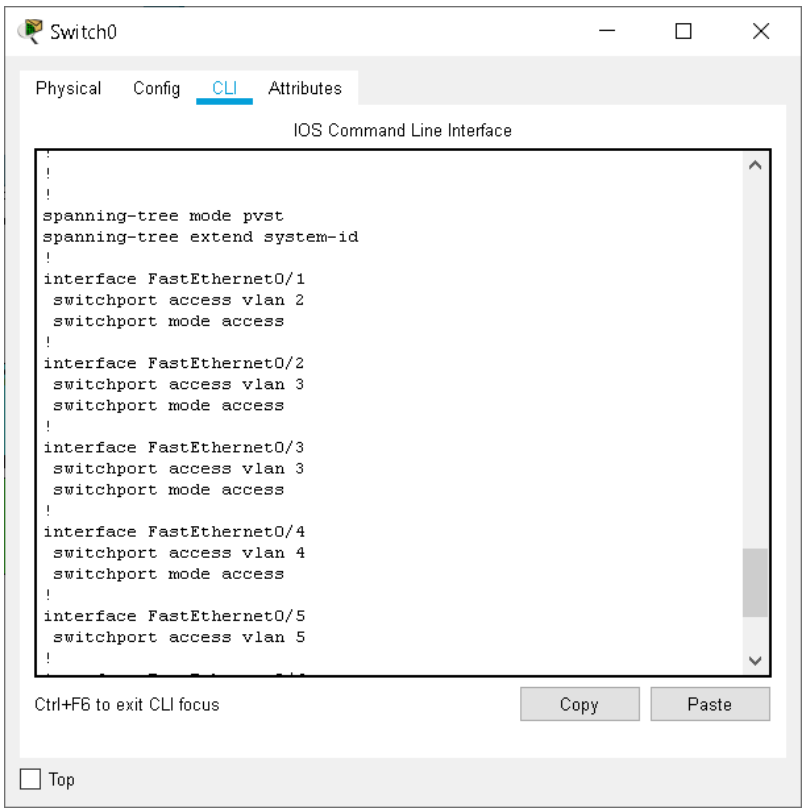


Рисунок 10.2 – Соединения коммутаторов

Назначим на R0 – NAT inside и outside команды

Conf t
Int fa0/0
Ip nat outside
Exit

Int range fa0/1.2-4
Int range fa0/1.2
Ip nat inside
Exit

Int fa0/1.3
Ip nat inside
Exit

Int fa0/1.4
Ip nat inside
Exit

Далее на этом же маршрутизаторе устанавливаем сеть доступа стандартную с названием FOR-NAT для сегментов бухгалтерии, админа и администрации. Для сегмента 1С нарочно не должны установить сеть к интернету.

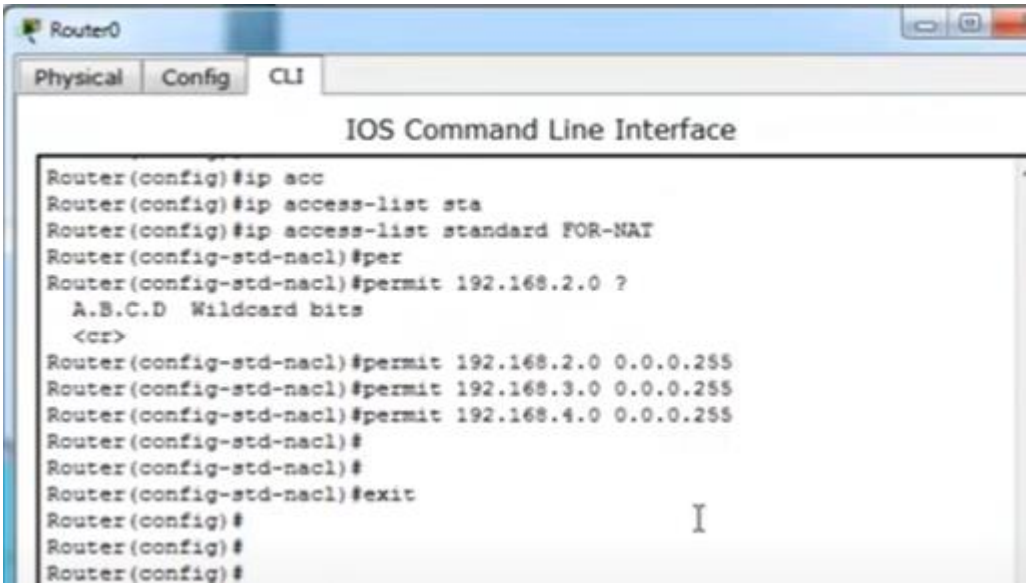


Рисунок 10.3 – Настройка ACL для роутера

После настраиваем команду и проверям работу сегмента к серверу.

ip nat inside source list FOR-NAT interface fa0/0 overload

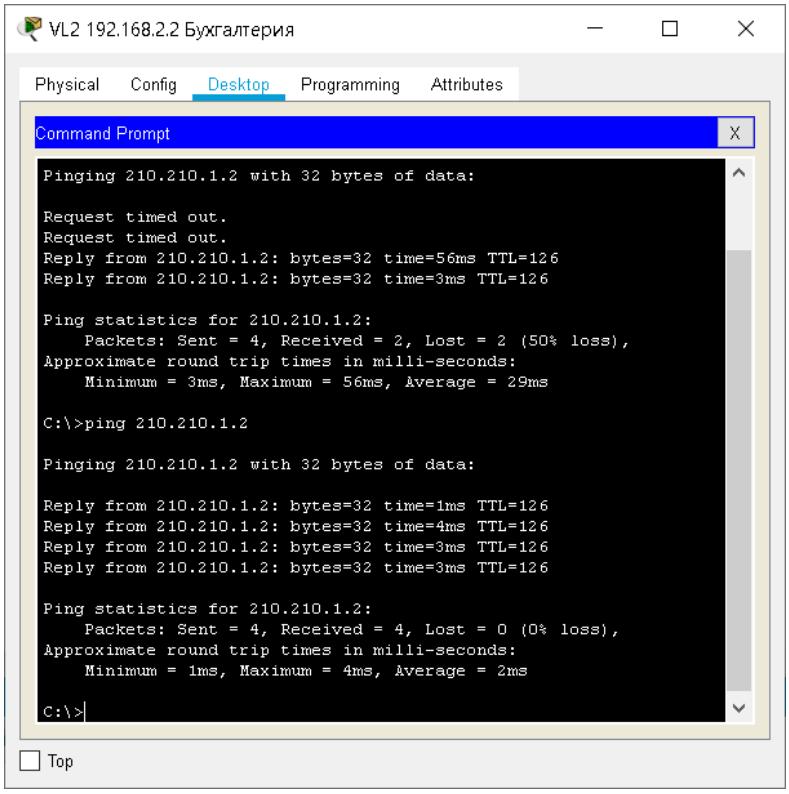


Рисунок 10.4 – Проверка пинга к серверу

Как видим, пинг успешно идет, значит правильно настроили все сегменты.

1.4.2 Настроим расширенный доступ для входящий сети.

Для начала через команду deny запрещаем заходить в наши серверы всем злоумышленникам.

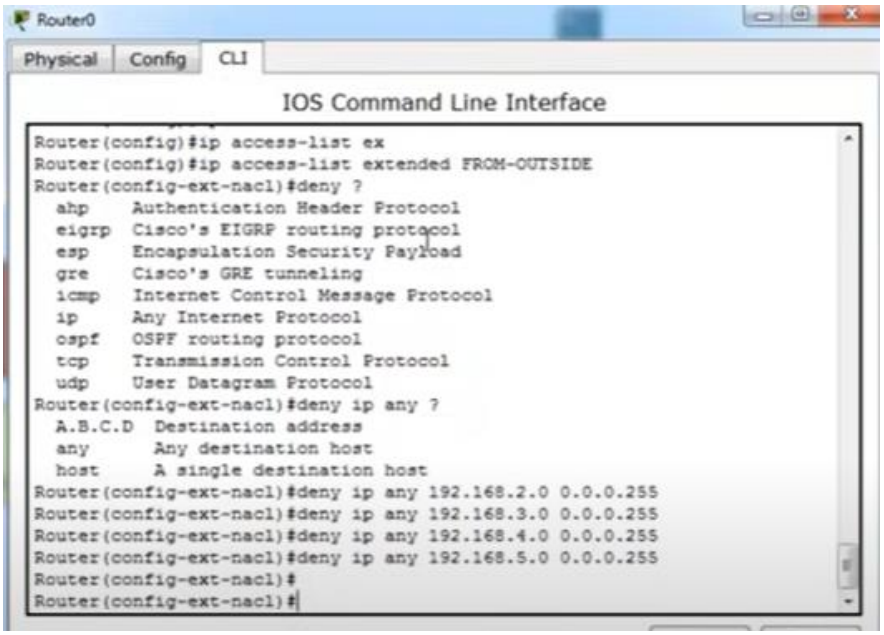


Рисунок 10.5 – Настройка расширенного ACL

Теперь данный ACL нужно привязать к интерфесу:

Int fa0/0

Ip access-group FROM-OUTSIDE in

End

На маршрутизаторе R1 проверяем сеть к сегментам.

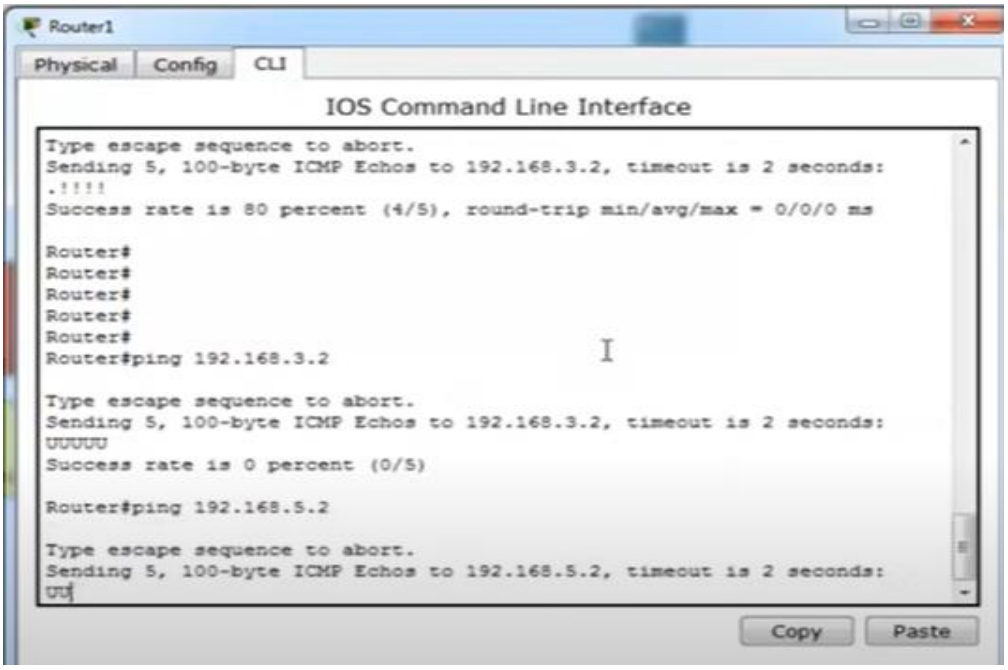


Рисунок 10.6 – Ограничение доступа к сегментам

10.4.3 Настроим доступ бухгалтерии к сегменту 1 С.

Ip access-list standard TO-1C
Permit 192.168.2.0 0.0.0.255
Exit

Привязываем ACL к интерфейсу
Int fa0/1.5
Ip access-group TO-1C outside
End

Далее проверяем пинг от бухгалтерии до 1С.

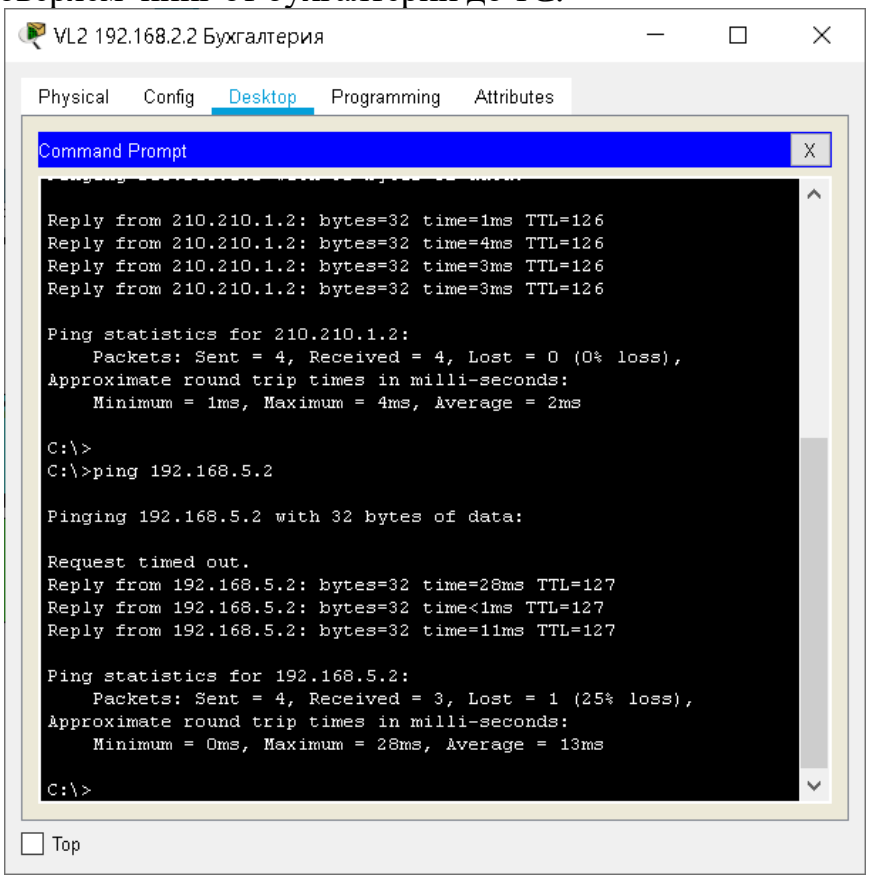


Рисунок 10.7 – Проверка пинга 1С

Как видим, пинг идет успешно.

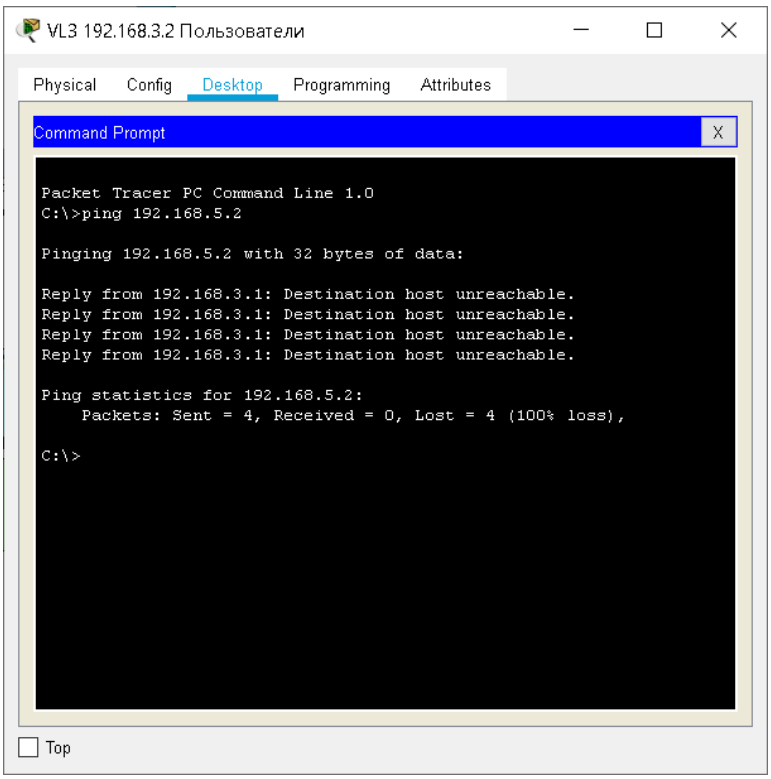


Рисунок 10.8 – Пинг от пользователей

Пинг от пользователей к сегменту 1С не идет, так как доступ есть только у сегмента бухгалтерии.

10.5 Контрольные вопросы:

1. Опишите ACL.
2. Преимущества и недостатки ACL.
3. Приведите примеры для всех видов ACL.
4. Для какой цели используется ACL?
5. Как работает инвертированная маска (wildcard mask)?
6. Как сделать так, чтобы внутренние пользователи имели полноценный доступ ко всем серверам и в то же время запретить серверам доступ во внутреннюю сеть?
7. Разница между входящим и исходящим трафиком.

Лабораторная работа № 11. Обеспечение сетевой безопасности на платформе Cisco packet tracer.

11.1 Цель работы: изучить межсетевой экран ASA и построить сеть.

11.2 Подготовка к работе:

Повторить разделы: создание стандартных технологий локальных сетей; коммутация сообщений, назначение IP-протокола, модель OSI, различие между сообщением и сигналом, определение пакета, кадра, фрейма.

Теоретическое описание

Cisco ASA (Adaptive Security Appliance) — серия аппаратных межсетевых экранов, разработанных компанией Cisco Systems.

Является наследником следующих линеек устройств:

- Межсетевых экранов Cisco PIX;
- Систем обнаружения вторжений Cisco IPS 4200;
- VPN-концентраторов Cisco VPN 3000.

Так же, как и PIX, ASA, основаны на процессорах x86. Начиная с версии 7.0 PIX и ASA, используют одинаковые образы операционной системы (но функциональность зависит от того, на каком устройстве она запущена).

Функциональность зависит от типа лицензии, который определяется введенным серийным номером.

Интерфейс командной строки напоминает (но не повторяет) интерфейс Cisco IOS. Управлять устройством можно через telnet, SSH, веб-интерфейс либо с помощью программы ASDM.

Возможности

- Межсетевое экранирование с учётом состояния соединений;
- Глубокий анализ протоколов прикладного уровня;
- Трансляция сетевых адресов;
- IPsec VPN;
- SSL VPN (подключение к сети через веб-интерфейс);
- Протоколы динамической маршрутизации (RIP, EIGRP, OSPF).

11.3 Описание лабораторной работы

В данной лабораторной работе используются маршрутизаторы, коммутаторы, ПК через програмное обеспечение Cisco. В данной лабораторной работе вы должны настроить список доступа. После всех выполненных команд нужно проверить работоспособность сети.

11.4 Рабочее задание:

Познакомиться с межсетевым экраном.

11.4.1 Схема подключения

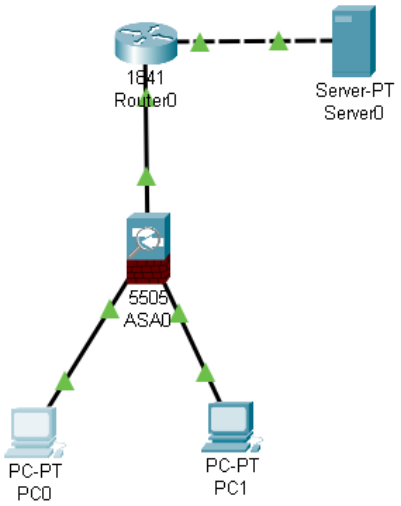


Рисунок 1 – Блок схема

Далее заходим на ASA и проверяем версию. Пароль пустой, можно дальше продолжать работу с enter-ом либо паролем cisco.

Набираем команду #show version.

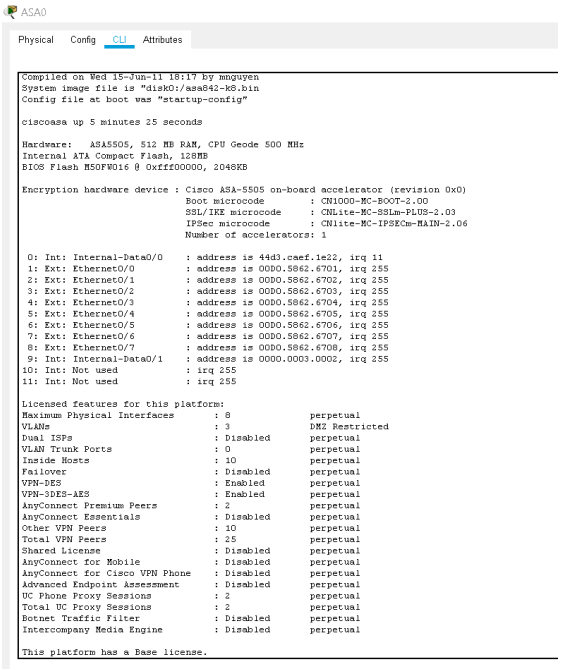


Рисунок 2 – Проверка версии

Задаем пароль для межсетевого экрана.

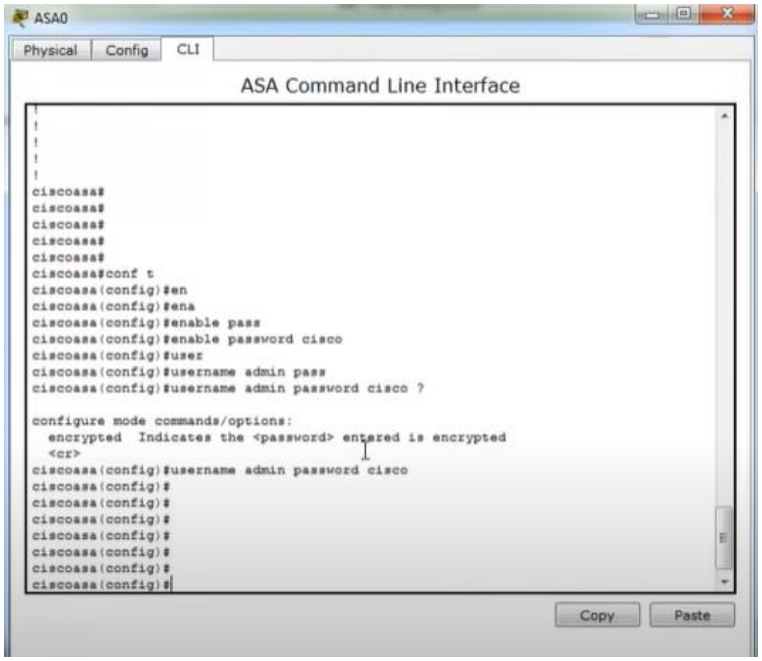


Рисунок 3 – Описание пароля для ASA

Далее выбираем протокол для того, чтобы считать удаленное подключение. В данном случае – протокол ssh, так как он безопасный. Указываем внутреннюю сеть для доступа.

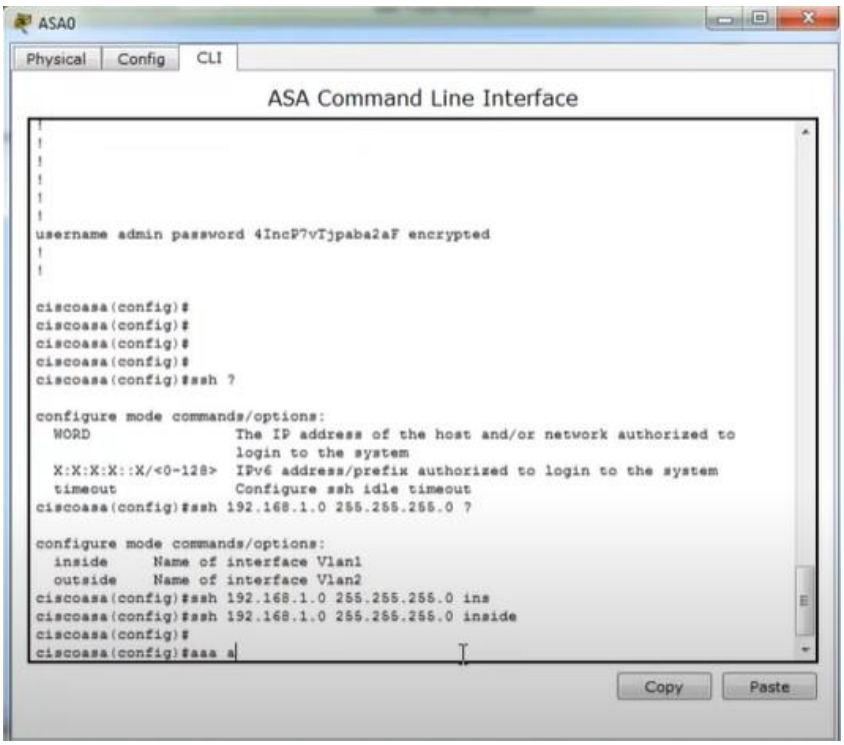


Рисунок 4 – Команда SSH

Указываем параметры аутентификации. Тем самым мы указываем локальную базу пользователя.

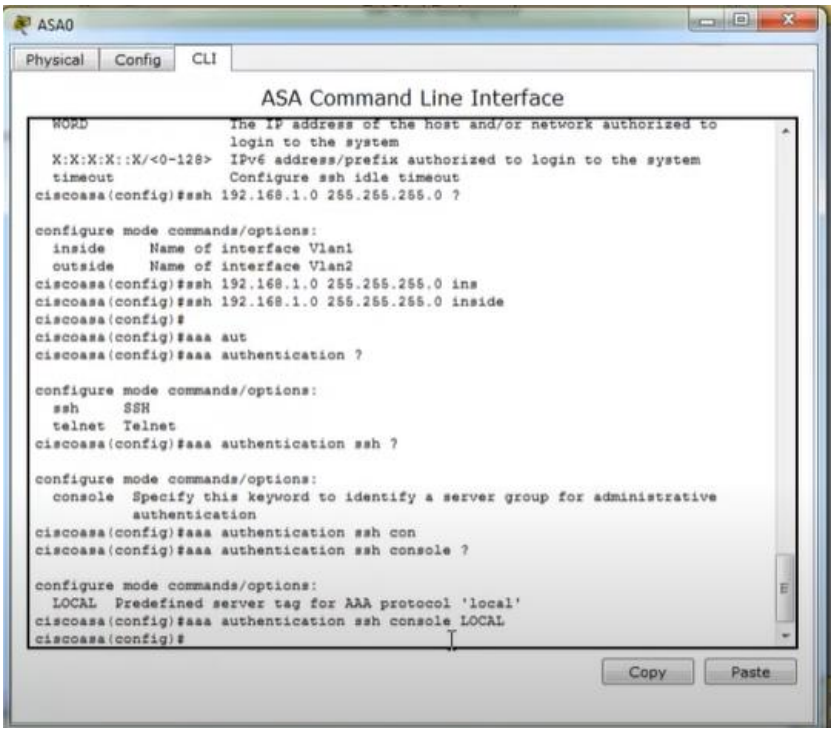


Рисунок 5 – Параметры аутентификации

Проверяем удаленный доступ через ПК.
Команды:

ssh
Ssh – 1 admin 192.168.1.1
Пароль cisco
En
Пароль cisco
Show run

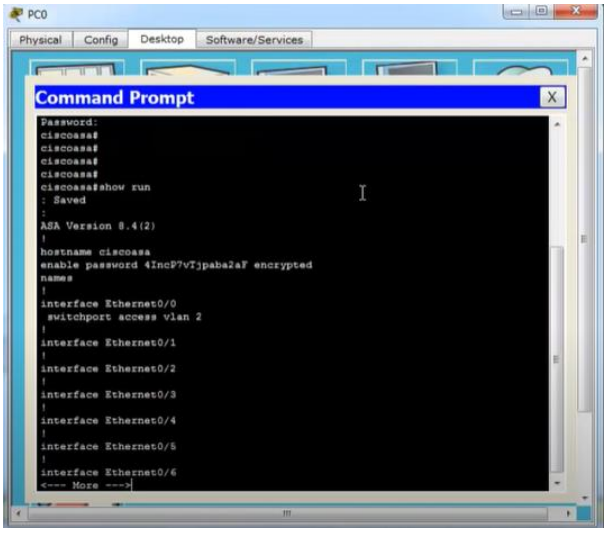


Рисунок 6 – Удаленный доступ настроен

11.4.2 Настройка Security Level
Чем выше Security Level, тем самым выше будет доверие.

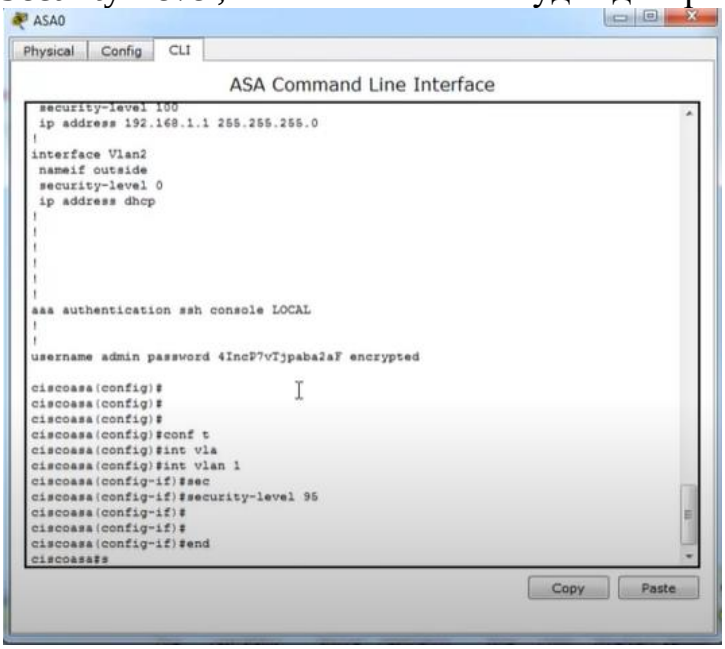


Рисунок 7 – Настройка security level

Далее настроем внешний интерфейс.

```
!
!
username admin password 4IncP7vTjpaba2aF encrypted

ciscoasa#conf t
ciscoasa(config)#int vlan
ciscoasa(config)#int vlan 2
ciscoasa(config-if)#
ciscoasa(config-if)#ip add
ciscoasa(config-if)#ip address 210.210.0.2 255.255.255.252
ciscoasa(config-if)#no shut
ciscoasa(config-if)#no shutdown

ciscoasa(config-if)#exit
```

Copy Paste

Рисунок 8 – Настройка внешного интерфейса

Далее прописываем маршрутизатор для интерфейсов fa0/0, fa0/1.

Router0

Physical Config CLI

IOS Command Line Interface

```
Router#
Router#
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#int fa0/0
Router(config-if)#ip add
Router(config-if)#ip address 210.210.0.1 255.255.255.252
Router(config-if)#no shut
Router(config-if)#no shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to
up

Router(config-if)#
Router(config-if)#
Router(config-if)#
Router(config-if)#exit
Router(config)#int fa0/1
Router(config-if)#no shut
Router(config-if)#no shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to
up
```

Copy Paste

```
Router(config-if)#
Router(config-if)#
Router(config-if)#ip add
Router(config-if)#ip address 210.210.1.1 255.255.255.0
Router(config-if)#
Router(config-if)#end
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#wr mem
Building configuration...
[OK]
Router#
```

Copy Paste

Рисунок 9 – Настройка маршрутизатора

Далее задаем статистические IP-адреса для сервера.

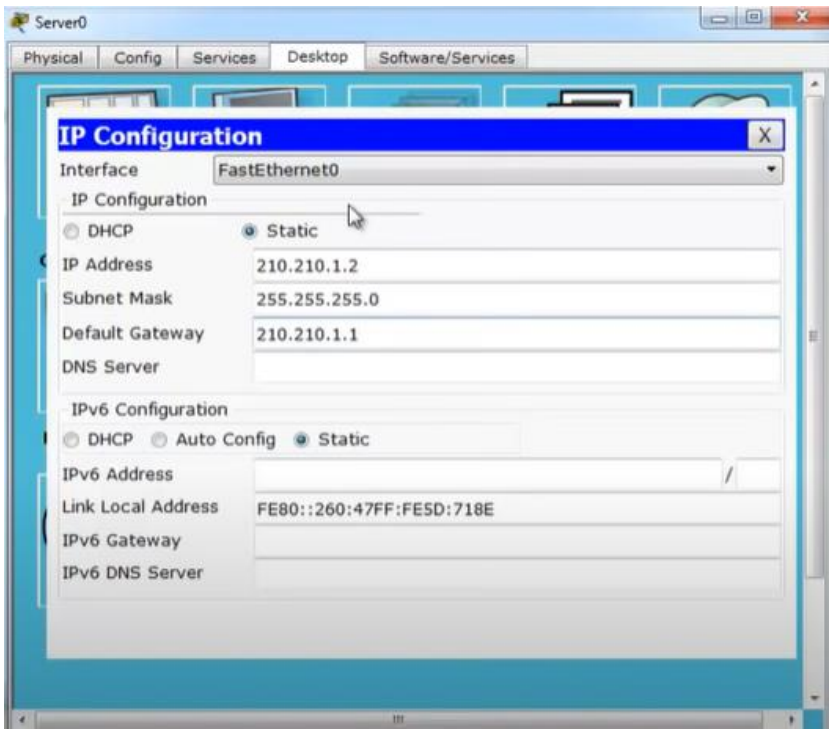


Рисунок 10 – Настройка сервера

Проверяем через ASA пинг интернета провайдера.

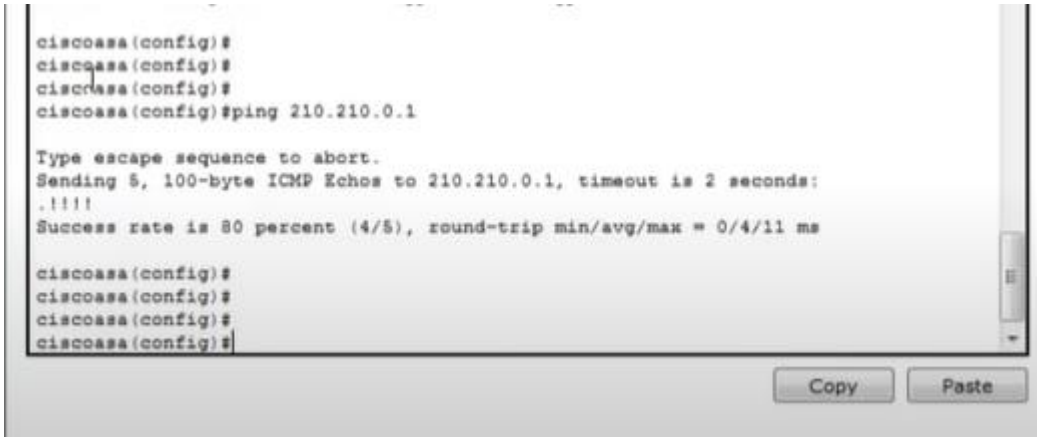


Рисунок 11 – Пинг идет успешно

Далее прописываем маршрут по умолчанию.

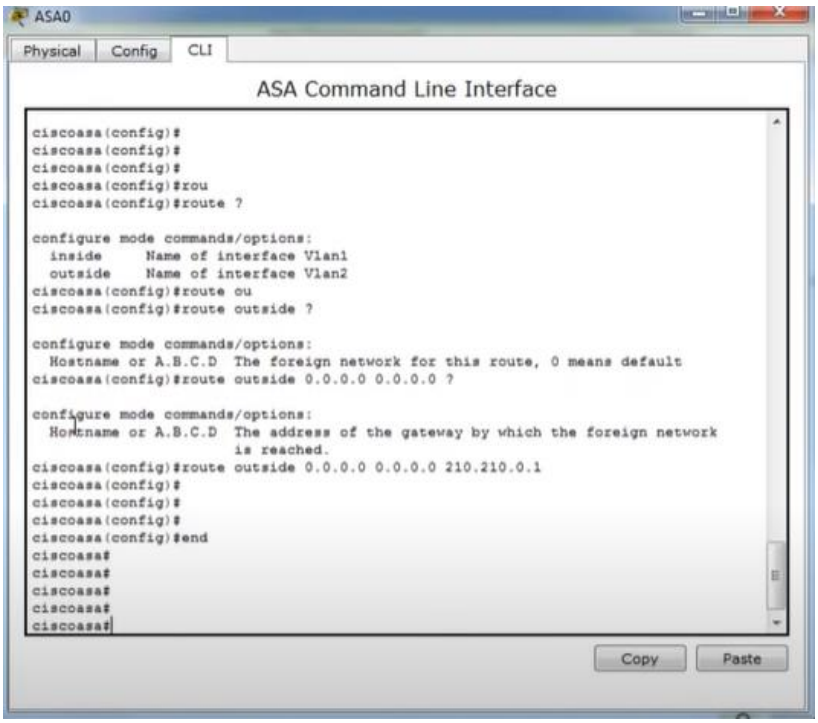


Рисунок 12 – Маршрут по умолчанию

После проверяем через ASA сервер.

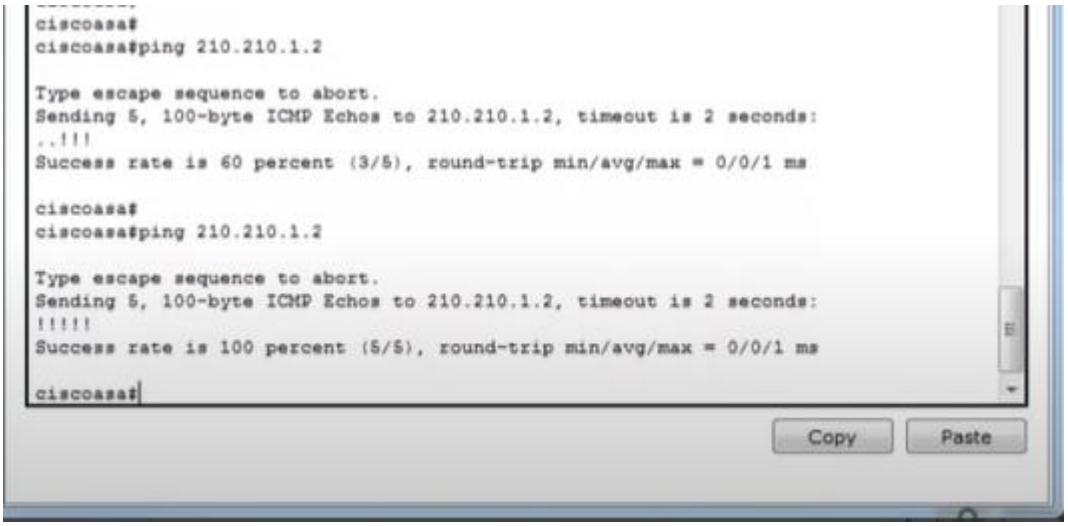


Рисунок 13 – Пинг успешно идет

11.4.3 Настройка инспектирования трафика

Определяем тип трафика, который мы исследуем.

ciscoasa(config)#class-map inspection default

ciscoasa(config-cmap)#match default-inspection-traffic

ciscoasa(config- cmap)#exit

Определяем действие.

ciscoasa(config)#policy-map global_policy

ciscoasa(config- pmap)#class inspection_default

ciscoasa(config)#service-policy global_policy global

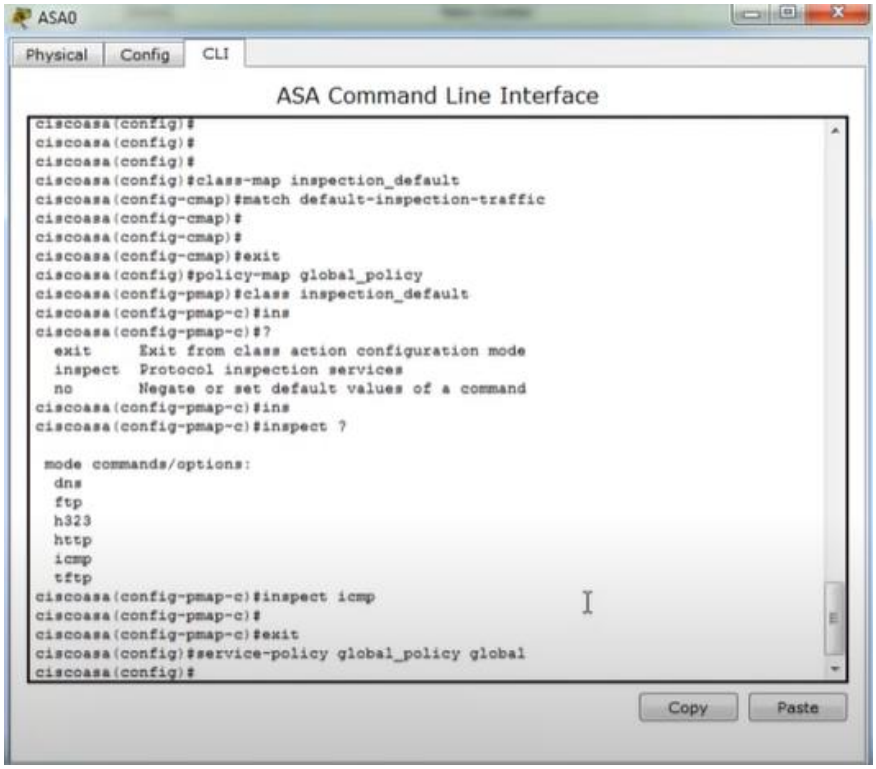


Рисунок 14 – Настройка инспектирования трафика

Далее проверяем сеть через ПК.

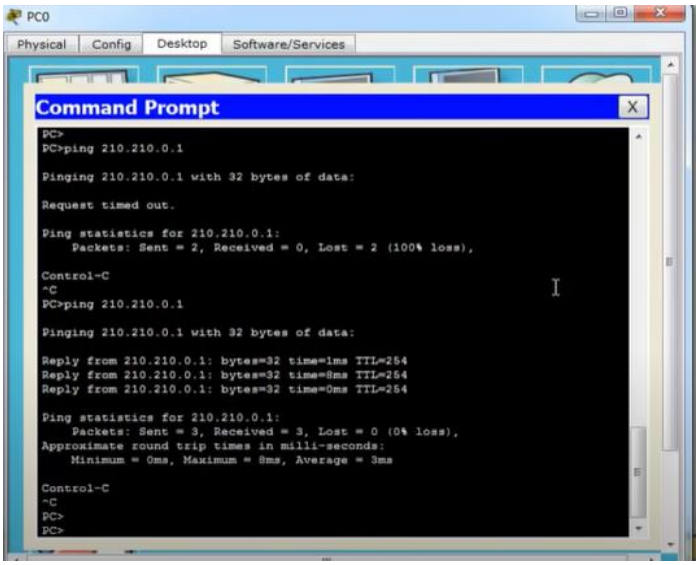


Рисунок 15 – Пинг успешно идет

Чтобы работал web browser, мы должны прописать в ASA команду:

ciscoasa(config- pmap-c)#inspect http

После комнады проверяем браузер.

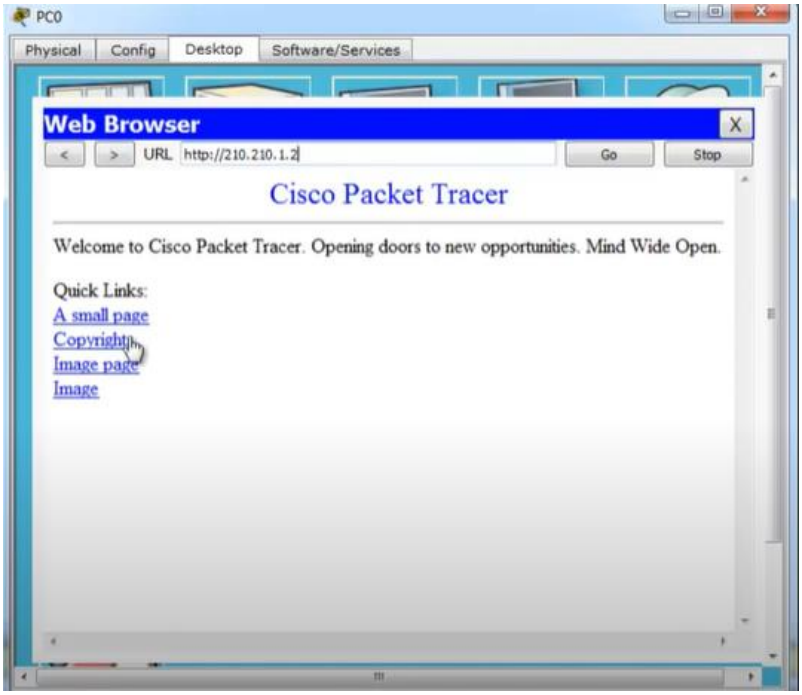


Рисунок 16 – Браузер работает успешно

11.5 Контрольные вопросы:

1. Принцип назначения ASA и какие виды существует?
2. Какую функцию выполняет межсетевой экран?
3. Что означает Security level?
4. Назовите протоколы динамической маршрутизации?

Лабораторная работа № 12. Демилитаризованная зона (DMZ)

12.1 Цель работы: создать общую доступную корпоративную сеть.

12.2 Подготовка к работе: Повторить разделы: создание стандартных технологий локальных сетей; коммутация сообщений, назначение IP-протокола, модель OSI, различие между сообщением и сигналом, определение пакета, кадра, фрейма.

Теоретическое описание

DMZ – (Demilitarized Zone) – это дополнительная возможность Интернет-маршрутизаторов серии DI-XXX, предназначенная для предоставления доступа к внутренним (то есть находящимися за маршрутизатором и защищенных NAT-ом) серверам (таким, как почтовый, WWW, FTP) пользователям из Интернета. Но, в отличие от "Virtual Servers", когда отображается только один порт, в

данном случае запрос извне на любой порт внешнего (WAN) интерфейса отображается на такой же порт компьютера, указанного в настройках DMZ.

То есть, все открытые порты на этом компьютере доступны снаружи. Это может создать угрозу безопасности для данного компьютера, поэтому на данном компьютере, возможно, будет необходимо установить программный межсетевой экран для защиты. Рекомендуется использовать данный метод только тогда, когда другими способами не удается обеспечить правильную работу сервисов на этом компьютере.

Например, для работы некоторых игровых серверов требуется обеспечить отображение большого количества портов или адреса портов назначаются таким сервером динамически в широком диапазоне.

12.3 Описание лабораторной работы

В данной лабораторной работе используются маршрутизаторы, коммутаторы, ПК через програмное обеспечение Cisco. В данной лабораторной работе вы должны настроить список доступа. После всех выполненных команд нужно проверить работоспособность сети.

12.4 Рабочее задание:

Изучить и настроить доступ DMZ.

12.4.1 Настройка ASA

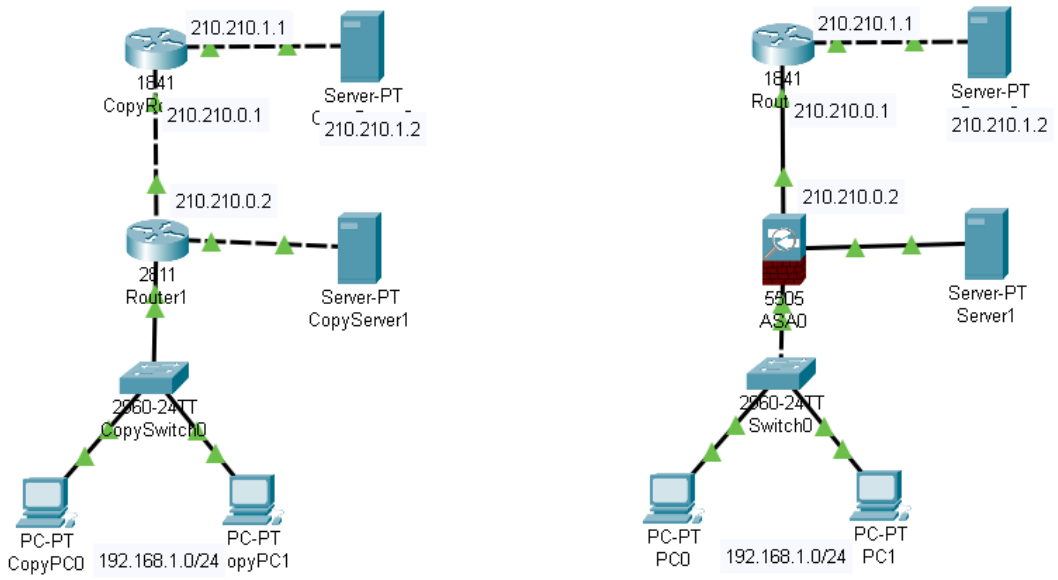


Рисунок 1 – Блок-схема

Для создания корпартивной сети необходимо будет создавать 3 политики доступа:

1) Политика доступа из локальной сети к интернету
2) Политика доступа из локальной сети к сети DMZ
3) Политика доступа из интернета к сегменту DMZ

Для начала будем использовать межсетевой экран, используя 11 лабораторную работу.

Сначала создаем статический IP- адрес для сервера 1.

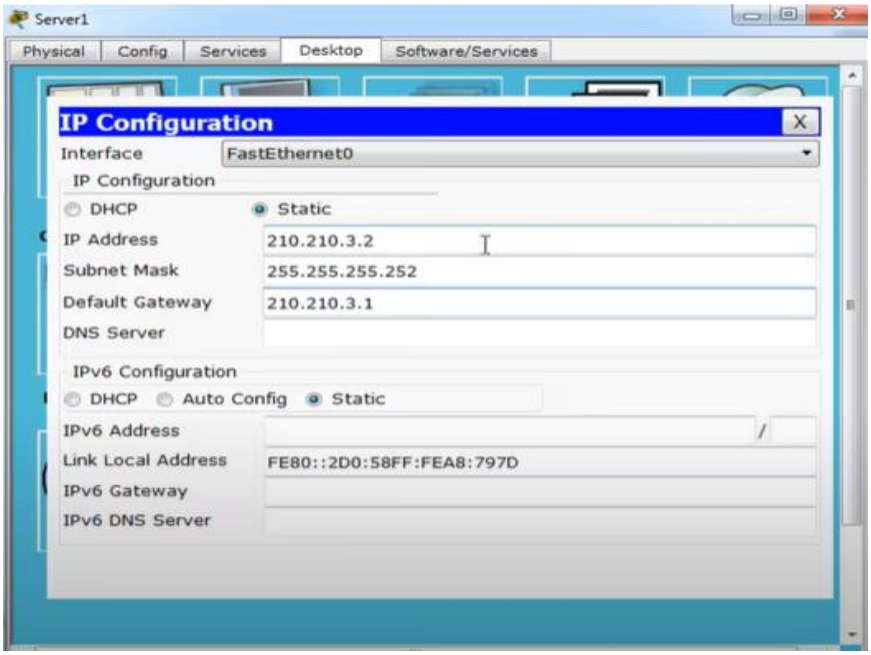


Рисунок 2 – Настройка сервера 1

Далее прописываем через машрутизатор интернет-провайдера маршрут.

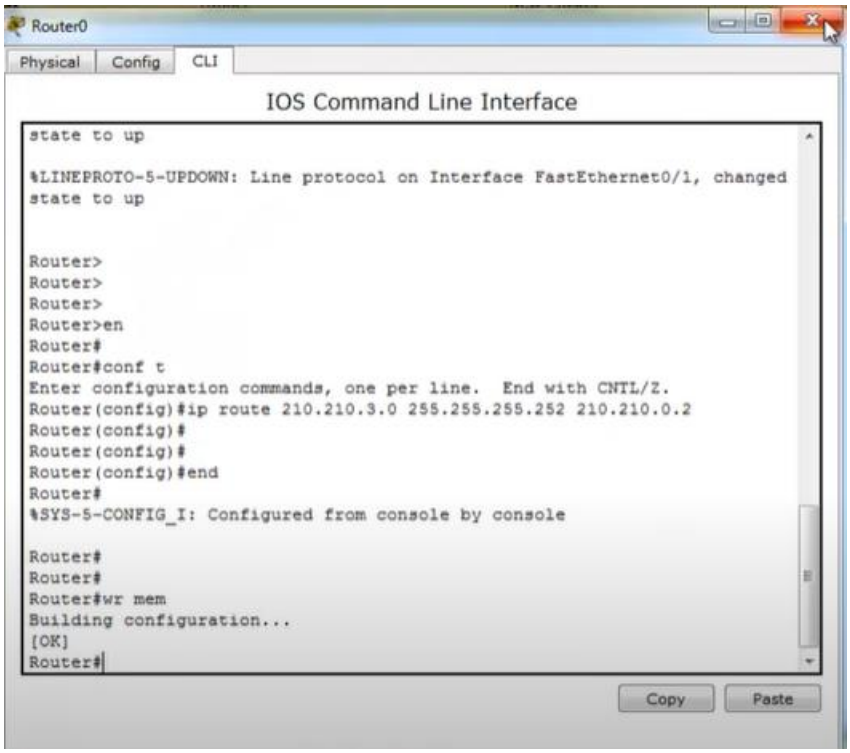


Рисунок 3 – Маршрут от маршрутизатора

Далее на ASA создаем новый сегмент.

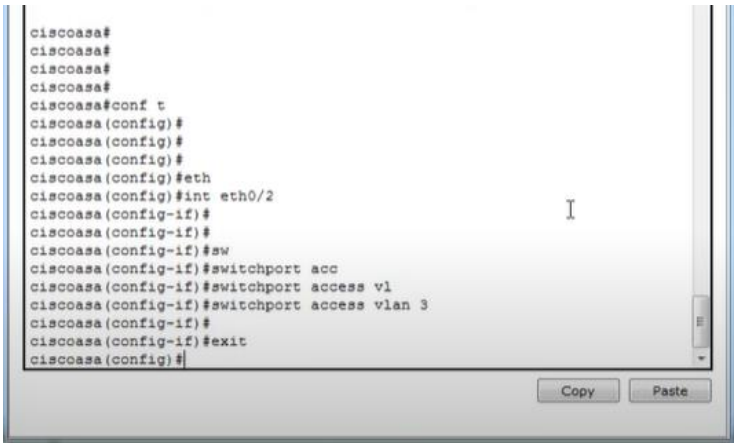


Рисунок 4 – Создание нового сегмента

Для настройки виртуального интерфейса один из серверов требует, чтобы трафик не проходил через интерфейс DMZ.

ciscoasa(config-if)#no forward interface vlan 1

Далее создаем интерфейс через DMZ.

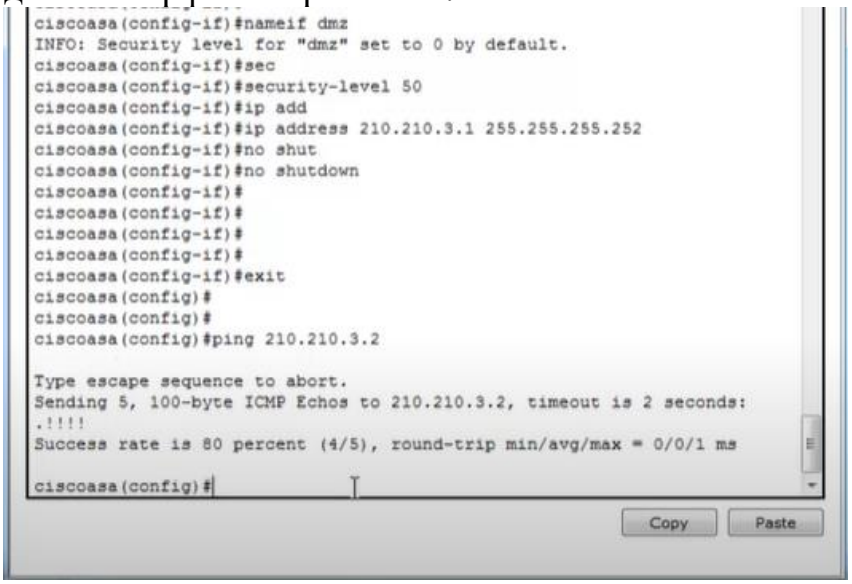


Рисунок 5 – Настройка интерфейса

На ASA даем разрешение на внешний сервер через команду access-list:

ciscoasa(config)#access-list FROM-OUTSIDE extended permit icmp any host 210.210.3.2

ciscoasa(config)#access-list FROM-OUTSIDE extended permit tcp any host 210.210.3.2 eq www 80

ciscoasa(config)#exit

Далее необходимо будет создать access group

ciscoasa(config)#access-group FROM-OUTSIDE in interface outside

ciscoasa(config)#exit

Проверяем пинг сервера 0.

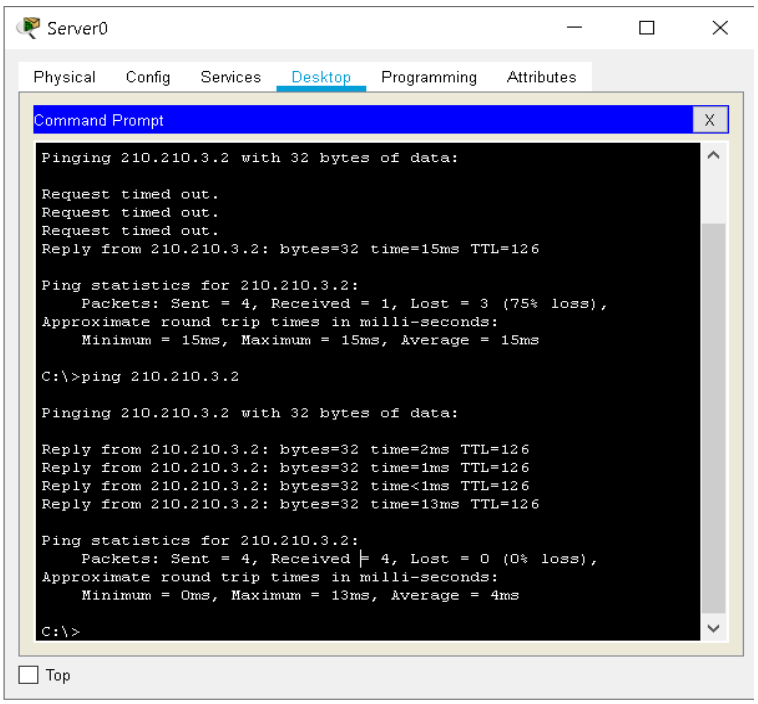
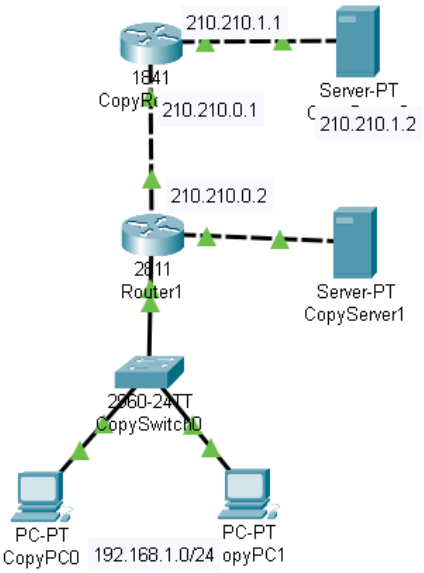


Рисунок 6 – Пинг идет успешно

12.4.2 Настройка маршрутизатора



Далее приступим к настройке маршрутизатора. Прописываем для fa0/0.

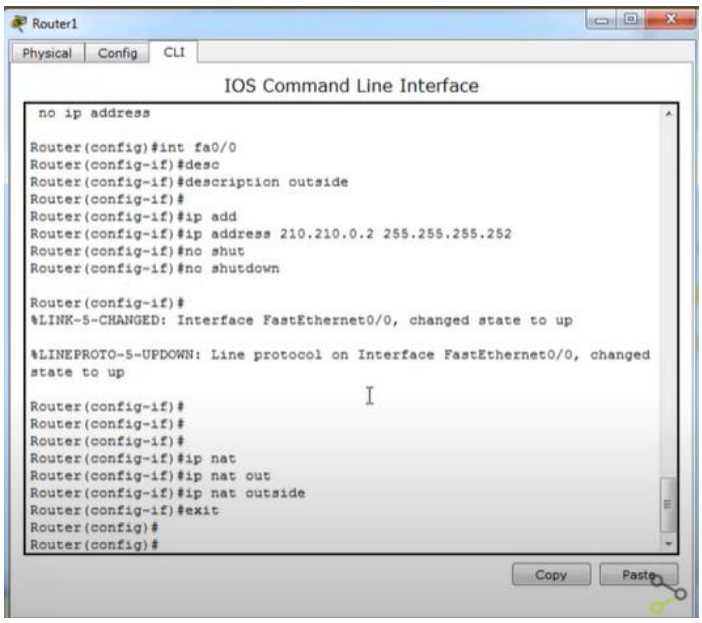
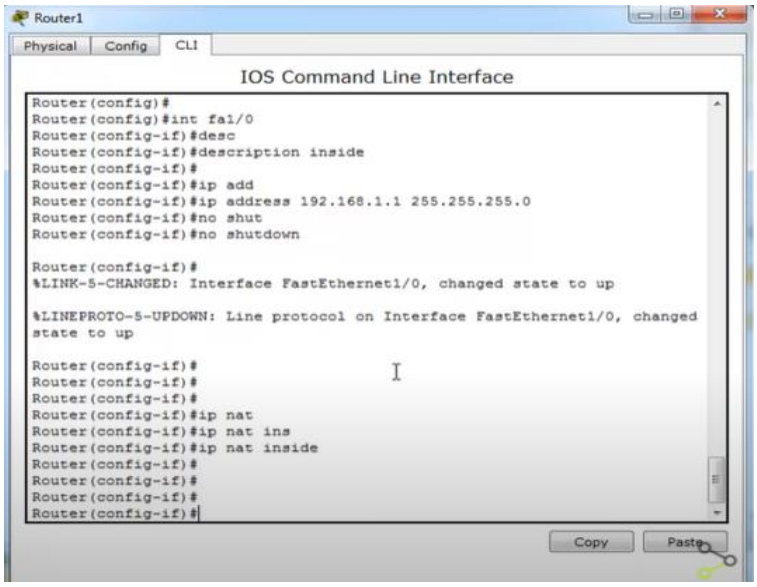


Рисунок 7 – Настройка роутера

После прописывем fa0/1.

Рисуок 8 – Настройка роутера

После прописывем fa1/0.



Рисуок 9 – Настройка роутера

Router(config)#ip access-list standard FOR-NAT
Router(config)#permit 192.168.1.0 0.0.0.255
Router(config)#exit
Router(config)#ip nat inside source list FOR-NAT interface fa0/0 overload
Router(config)#end

После прописания статического IP-адреса для ПК0 конфигурация IP-адреса показана на рисунке 10.

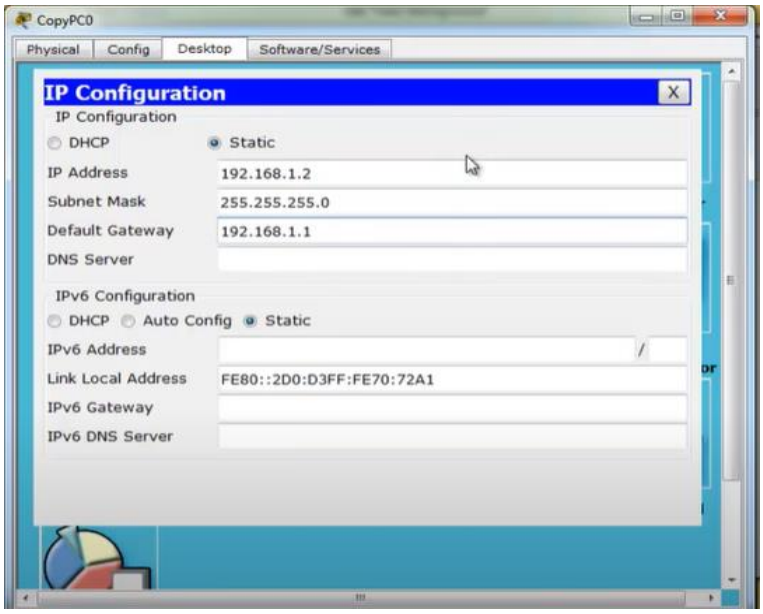


Рисунок 10 – Статический IP-адрес для ПК0

После прописания статического IP-адреса для ПК1 конфигурация IP-адреса показана на рисунке 11.

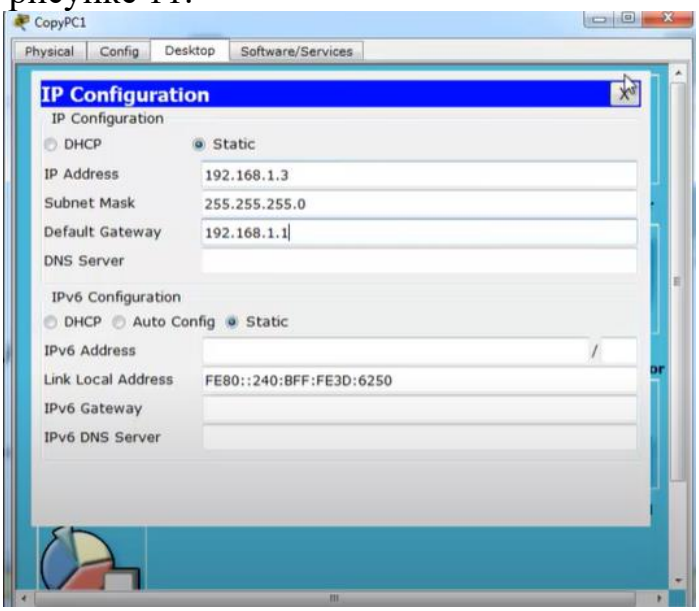


Рисунок 11 – Статический IP-адрес для ПК1

Далее проверяем интернет провайдер, веб браузер и локальную сеть.

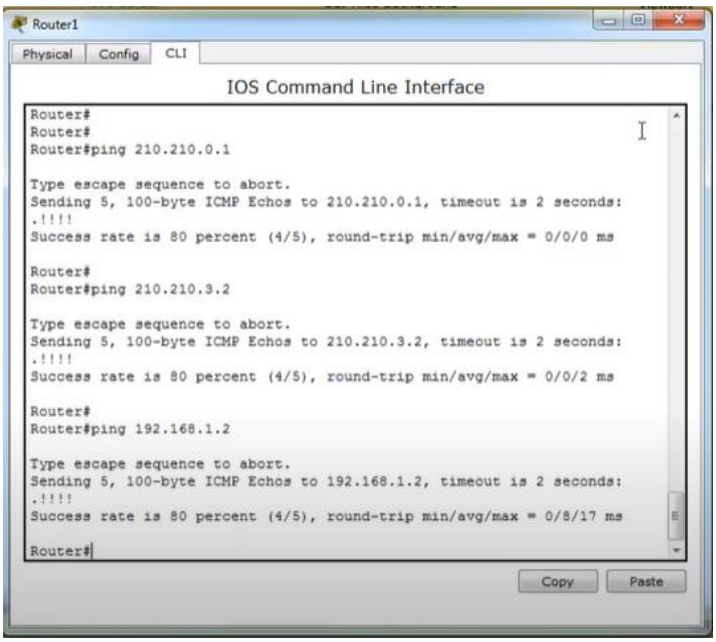


Рисунок 12 – Пинг идет успешно

Прописываем IP-адрес для роутера через интернет провайдер.
Router(config)#ip route 0.0.0.0 0.0.0.0 210.210.0.1
Router(config)#end
Проверяем через ПК0 доступ к интернету провайдеру

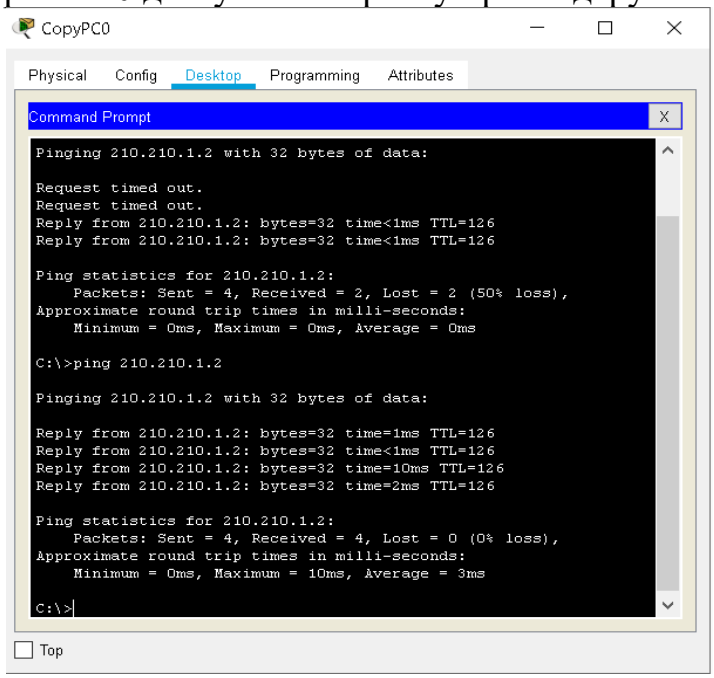


Рисунок 13 – Пинг идет успешно

12.5 Контрольные вопросы

1. Что такое DMZ?
2. Какие настройки былы сделаны?
3. Отличия между ASA и DMZ?
4. Что такое Access list и NAT?

Лабораторная работа № 13. Исследование протокола syslog с помощью NTP .

13.1 Цель работы: исследование протоколов syslog, NTP.

13.2 Подготовка к работе:

Повторить разделы: создание стандартных технологий локальных сетей; коммутация сообщений, назначение IP-протокола, модель OSI, различие между сообщением и сигналом, определение пакета, кадра, фрейма.

Теоретическое описание

Протокол Syslog – это способ для сетевых устройств отправлять сообщения о событиях на сервер регистрации, обычно известный как Syslog сервер. Этот протокол поддерживается широким спектром устройств и может использоваться для регистрации различных типов событий. Например, маршрутизатор может отправлять сообщения о том, что пользователи подключаются через консоль, а веб-сервер может регистрировать события, которым отказано в доступе.

Большинство сетевых устройств, таких как маршрутизаторы и коммутаторы, могут отправлять сообщения системного журнала. Кроме того, серверы *nix также могут генерировать данные системного журнала, как и большинство брандмауэров, некоторые принтеры и даже веб-серверы, такие как Apache. Серверы на базе Windows изначально не поддерживают Syslog, но большое количество сторонних инструментов позволяет легко собирать данные журнала событий Windows или IIS и пересылать их на сервер Syslog.

В отличие от SNMP, Syslog не может использоваться для «опроса» устройств для сбора информации. Например, SNMP имеет сложную иерархическую структуру, которая позволяет станции управления запрашивать у устройства информацию о таких вещах, как данные о температуре или доступное дисковое пространство. Это невозможно с Syslog – он просто отправляет сообщения в центральное место, когда инициируются определенные события.

NTP (англ. *Network Time Protocol* — протокол сетевого времени) — сетевой протокол для синхронизации внутренних часов компьютера с использованием сетей с переменной латентностью.

Наиболее широкое применение протокол NTP находит для синхронизации серверов точного времени. Для достижения максимальной точности предпочтительна постоянная работа программного обеспечения NTP в режиме системной службы. В семействе операционных систем Microsoft Windows — это служба W32Time, Linux — демон Ntpd или chronyd.

Более простая реализация этого алгоритма известна как SNTP — простой протокол сетевого времени. Используется во встраиваемых системах и устройствах, не требующих высокой точности, а также в пользовательских программах точного времени.

13.3 Описание лабораторной работы

В данной лабораторной работе используются маршрутизатор, коммутатор, сервер, ПК через програмное обеспечение Cisco. В ней вы должны построить сеть доступа с использованием Syslog и NTP. После всех выполненных команд нужно проверить работоспособность сети.

13.4 Рабочее задание:

Осуществить настройку Syslog и настройку NTP.

13.4.1 Схема подключения

Соберем сеть с двумя ПК, которые подключены к комутатору и далее к маршрутизату. Подключаем наш сервер к маршрутизатору.

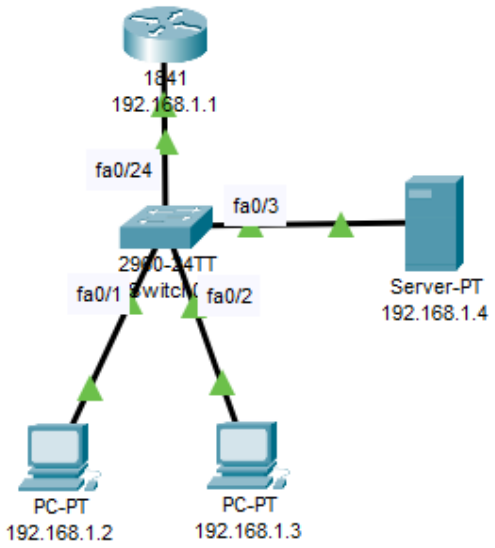


Рисунок 13.1 – Схема соединения

Для начала в локальную сеть нужно настроить все ПК и Server – PT 0 и задать ip адресов.

Для PC0 ping 192.168.1.2
Для PC1 ping 192.168.1.3
Для Server0 ping 192.168.1.4

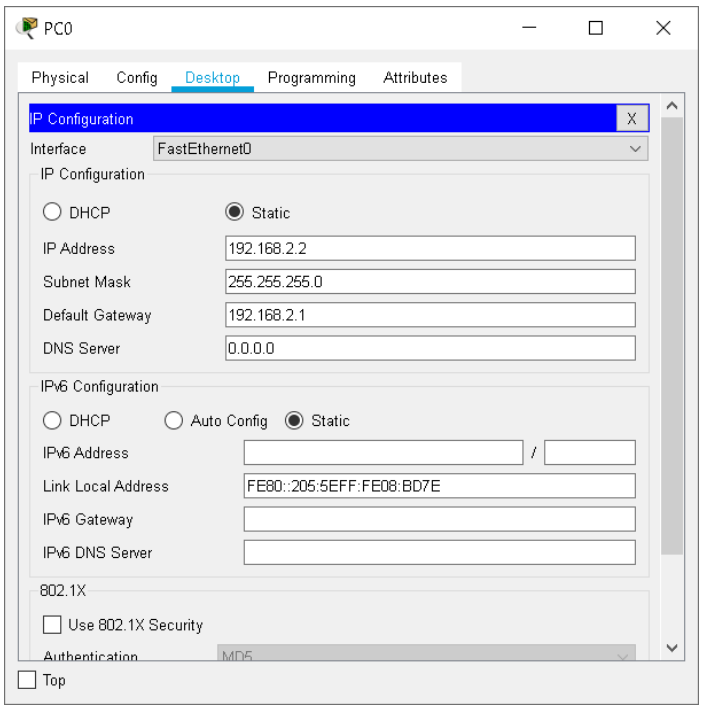


Рисунок 13.2 – Конфигурация IP-адресов

Заходим в CLI интерфейс коммутатора Switch0 и пишем следующие команды.

```
Switch#conf ter
Switch#conf terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#logging
Switch(config)#logging bu
Switch(config)#logging buffered
Switch(config)#logging trap debugging
Switch(config)#logging 192.168.1.4
Switch(config)#inter vlan 1
Switch(config-if)#ip addr 192.168.1.5 255.255.255.0
Switch(config-if)#no sh
Switch(config-if)#service timestamps log datetime msec
Switch(config)#
```

Рисунок 13.3 – Настройки logging и vlan 1 на коммутаторе.

С командой «show clock» мы можем увидеть настроенное время на нашем коммутаторе.

```
Switch#show
Switch#show clock
Switch#show clock
*1:25:31.32 UTC Mon Mar 1 1993
Switch#
Switch#
```

Рисунок 13.4 – Использование команды «show clock»

Как мы видим, время установлено неправильно. Его можно исправить вручную, но когда у нас на производстве будет большая сеть, это не целесообразно. Будем использовать NTP, но его можно настроить только на маршрутизаторе.

```
Router(config)#
Router(config)#
Router(config)#interface FastEthernet0/1
Router(config-if)# description inside
Router(config-if)# ip address 192.168.1.1 255.255.255.0
Router(config-if)#ex
Router(config)#ntp server 192.168.1.4
Router(config)#logging trap debugging
Router(config)#logging 192.168.1.4
Router(config)#service time
Router(config)#service timestamps log datetime msec
Router(config)#
Router#
*дек 11, 13:23:11.2323: %SYS-5-CONFIG_I: Configured from console by
console
```

Рисунок 13.5 – Настройки маршрутизатора

Теперь нам надо проверить наш syslog на коммутаторе и на маршрутизаторе.

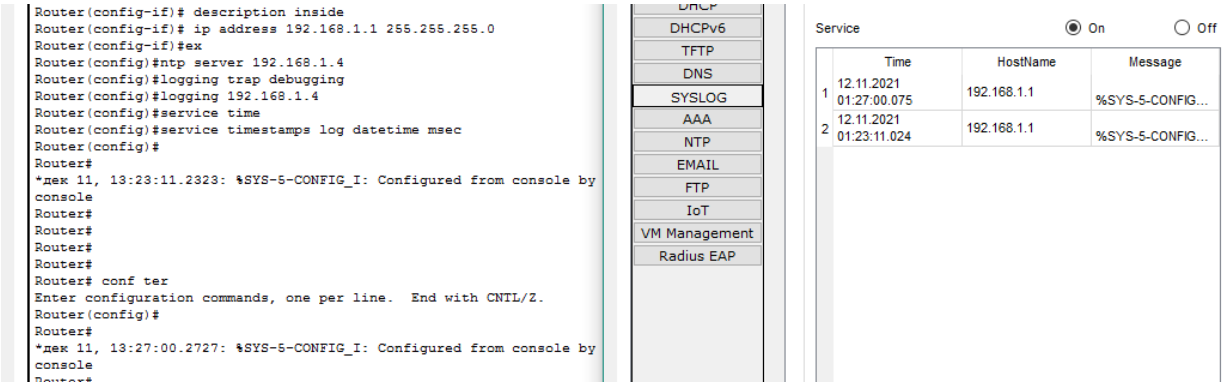


Рисунок 13.6 – Проверка Syslog на маршрутизаторе

Точно так же делаем на коммутаторе.

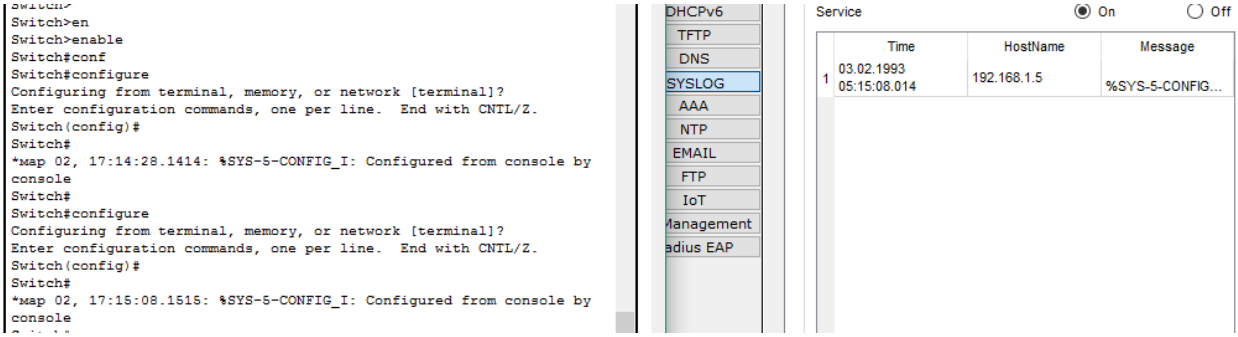


Рисунок 13.7 – Проверка Syslog на коммутаторе

13.5 Контрольные вопросы:

1. Опишите NTP.
2. Опишите SYSLOG.
3. Что такое SNMP?
4. Отличия между SNMP и SYSLOG.

Лабораторная работа № 14. Исследование WI-FI — беспроводной передачи данных

14.1 Цель работы: исследование WI-FI.

14.2 Подготовка к работе:

Повторить разделы: создание стандартных технологий локальных сетей; коммутация сообщений, назначение IP-протокола, модель OSI, различие между сообщением и сигналом, определение пакета, кадра, фрейма.

Теоретическое описание

Wi-Fi — технология беспроводной локальной сети с устройствами на основе стандартов IEEE 802.11. Логотип Wi-Fi является торговой маркой Wi-Fi Alliance. Под аббревиатурой Wi-Fi (от английского словосочетания Wireless Fidelity, которое можно дословно перевести как «беспроводная точность») в настоящее время развивается целое семейство стандартов передачи цифровых потоков данных по радиоканалам. Основными диапазонами Wi-Fi считаются 2.4 ГГц (2412 МГц-2472 МГц) и 5 ГГц (5160-5825 МГц). Сигнал Wi-Fi может передаваться на километры даже при низкой мощности передачи, но для приема Wi-Fi-сигнала с обычного Wi-Fi-маршрутизатора на далеком расстоянии нужна антенна с высоким коэффициентом усиления (например, параболическая антенна или Wi-Fi-пушка).

Любое оборудование, соответствующее стандарту IEEE 802.11, может быть протестировано в Wi-Fi Alliance и получить соответствующий сертификат и право нанесения логотипа Wi-Fi.

Обычно схема сети Wi-Fi содержит не менее одной точки доступа и не менее одного клиента. Также возможно подключение двух клиентов в режиме точка–точка (Ad-hoc), когда точка доступа не используется, а клиенты соединяются посредством сетевых адаптеров «напрямую». Точка доступа передаёт свой идентификатор сети (SSID) с помощью специальных сигнальных пакетов на скорости 0,1 Мбит/с каждые 100 мс. Поэтому 0,1 Мбит/с — наименьшая скорость передачи данных для Wi-Fi. Зная SSID сети, клиент может выяснить, возможно ли подключение к данной точке доступа. При попадании в зону действия двух точек доступа с идентичными SSID приёмник может выбирать между ними на основании данных об уровне сигнала. Стандарт Wi-Fi даёт клиенту полную свободу при выборе критериев для соединения. Более подробно принцип работы описан в официальном тексте стандарта.

Однако стандарт не описывает всех аспектов построения беспроводных локальных сетей Wi-Fi. Поэтому каждый производитель оборудования решает эту задачу по-своему, применяя те подходы, которые он считает наилучшими с той или иной точки зрения. Поэтому возникает необходимость классификации способов построения беспроводных локальных сетей.

По способу объединения точек доступа в единую систему можно выделить:

- Автономные точки доступа (называются также самостоятельные, децентрализованные, умные).
- Точки доступа, работающие под управлением контроллера (называются также «легковесные», централизованные).
- Бесконтроллерные, но не автономные (управляемые без контроллера).

По способу организации и управления радиоканалами можно выделить беспроводные локальные сети:

- со статическими настройками радиоканалов;
- с динамическими (адаптивными) настройками радиоканалов;
- со «слоистой», или многослойной, структурой радиоканалов.

14.3 Описание лабораторной работы

В данной лабораторной работе используются маршрутизатор, точка доступа и ПК через програмное обеспечение Cisco. В ней вы должны построить сеть доступа с технологиями тачки доступа, научиться настраивать серверы. После всех выполненных команд нужно проверить работоспособность сети.

14.4 Рабочее задание:

Осуществить настройку точки доступа.

9.4.1 Схема подключения

Соберем сеть с роутарам и с точкой доступа.

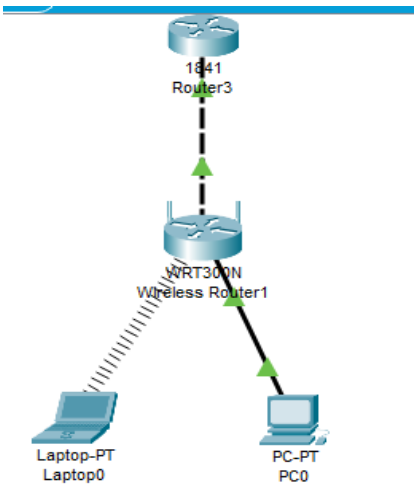


Рисунок 14.1 – Схема соединения

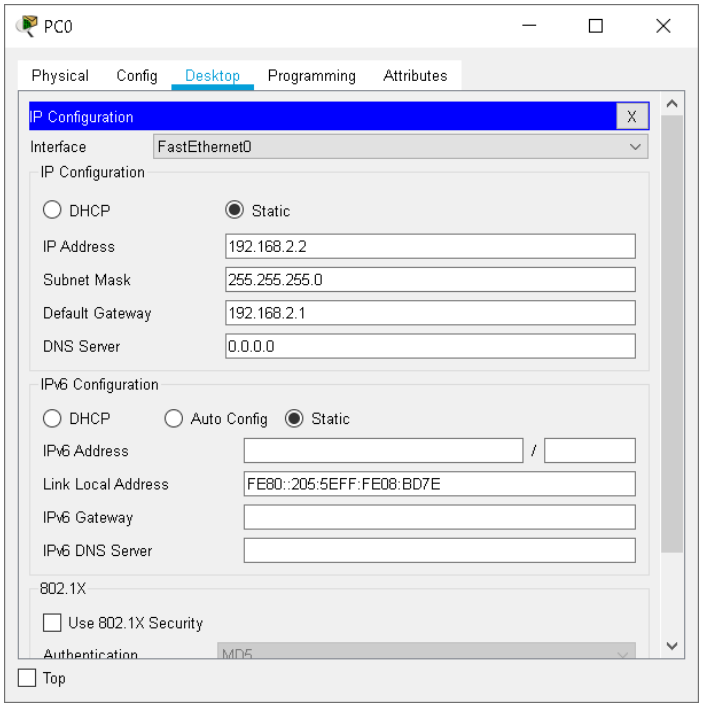


Рисунок 14.2 – конфигурация IP-адресов

Заходим в CLI интерфейс коммутатора Router3 и пишем следующие команды.

```
Router#conf terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface FastEthernet0/0
Router(config-if)# ip address 210.210.0.1 255.255.255.252
Router(config-if)#
Router(config-if)#
```

Рисунок 14.3 – CLI интерфейс коммутатора Router3

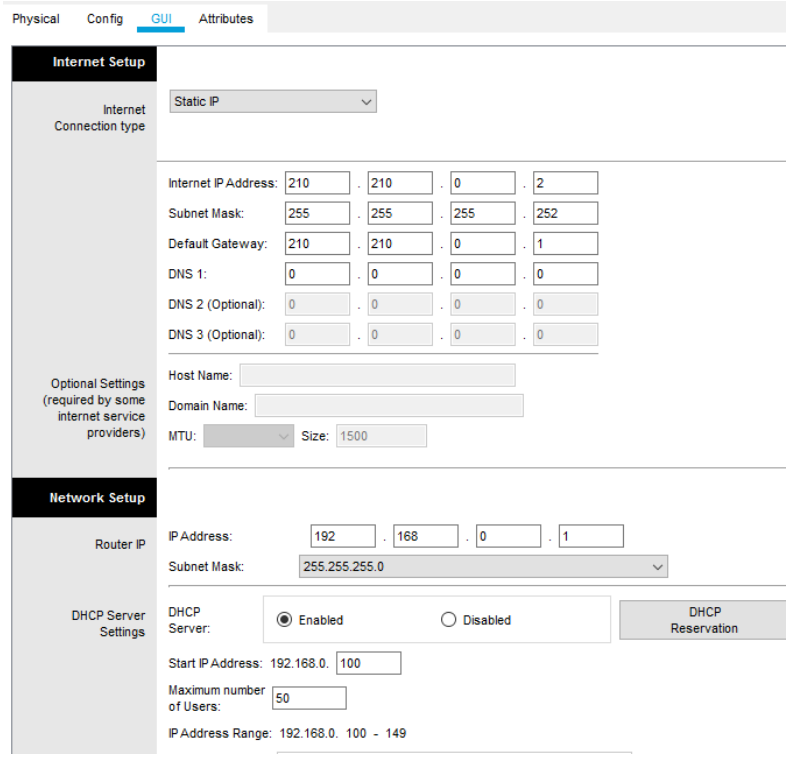


Рисунок 14.4 – Настройки ip addres точки доступа

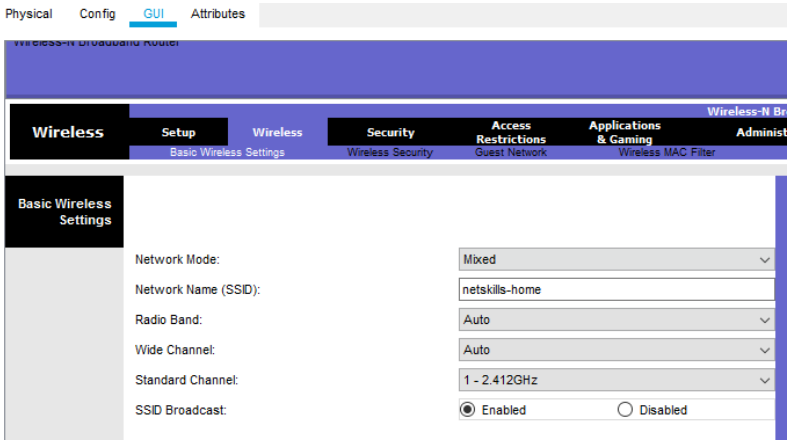


Рисунок 14.5 – Настройки wi-fi

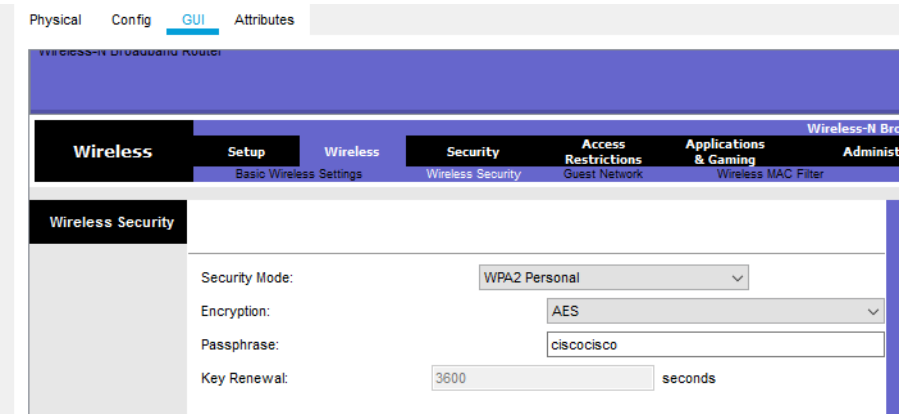


Рисунок 14.6 – Настройки wi-fi

Мы должны включить ноутбук и настроить беспроводную сеть.

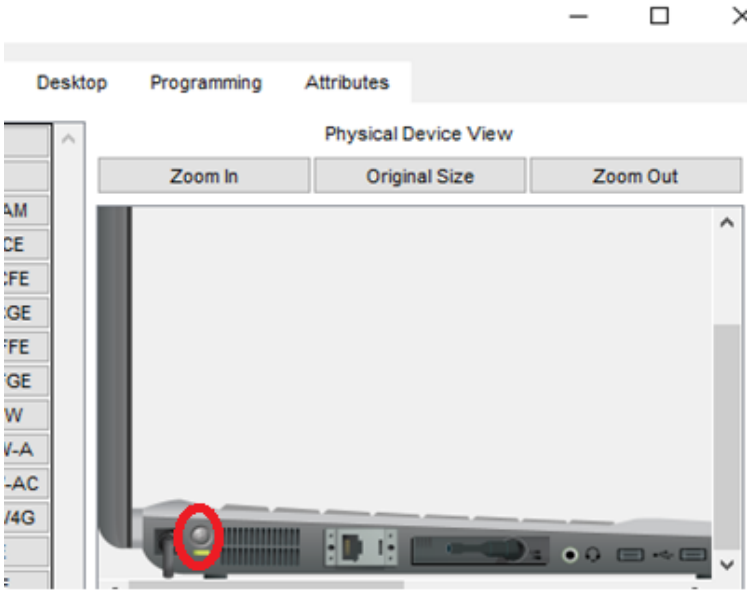


Рисунок 14.7 – Включение ноутбука

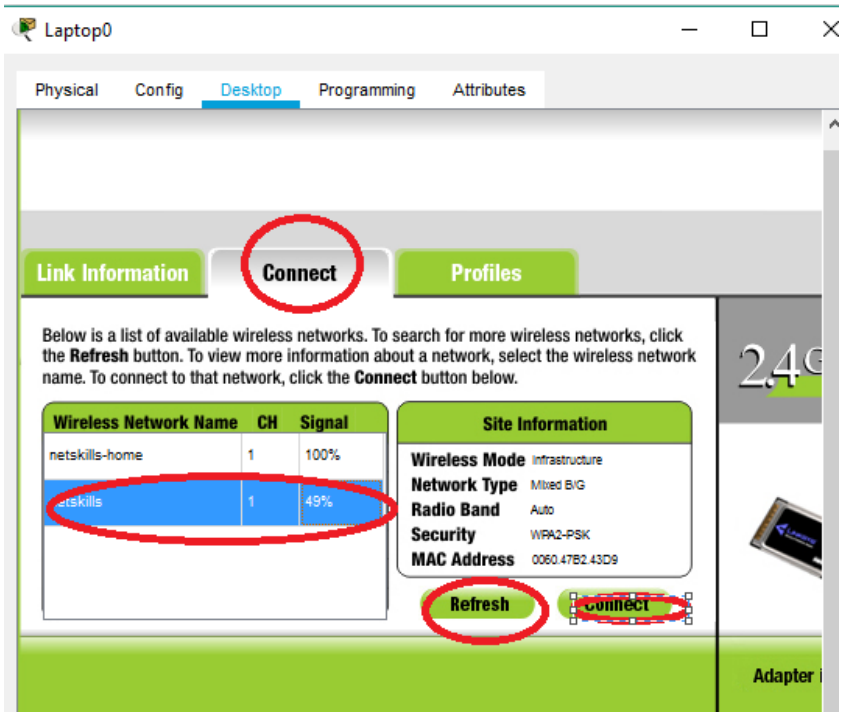


Рисунок 14.8 – Подключение к WiFI

Далее мы на pc0 и на Laptop0 настроим dhcp.

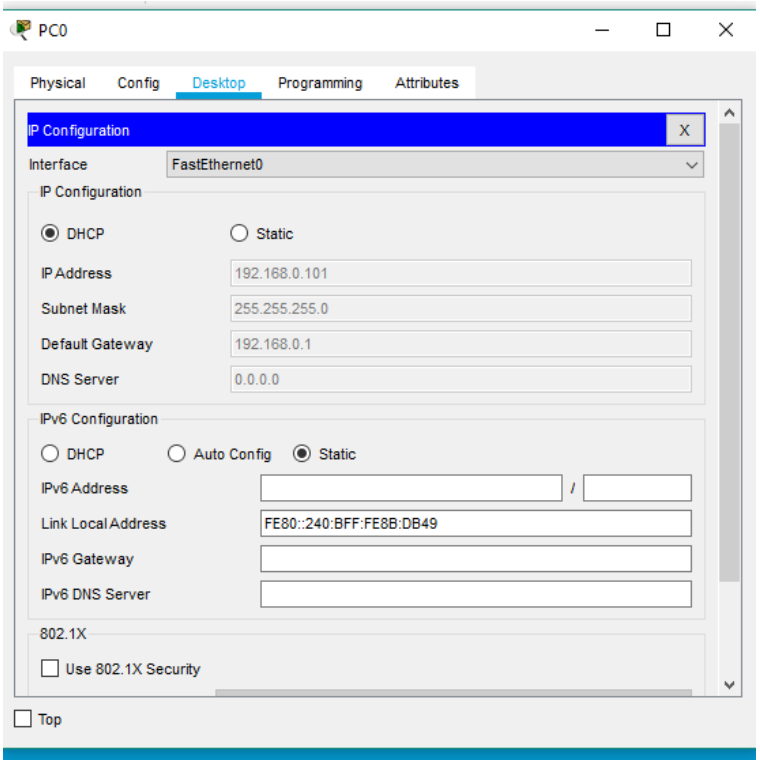


Рисунок 14.9 – Настройки ip addres

Проверяем

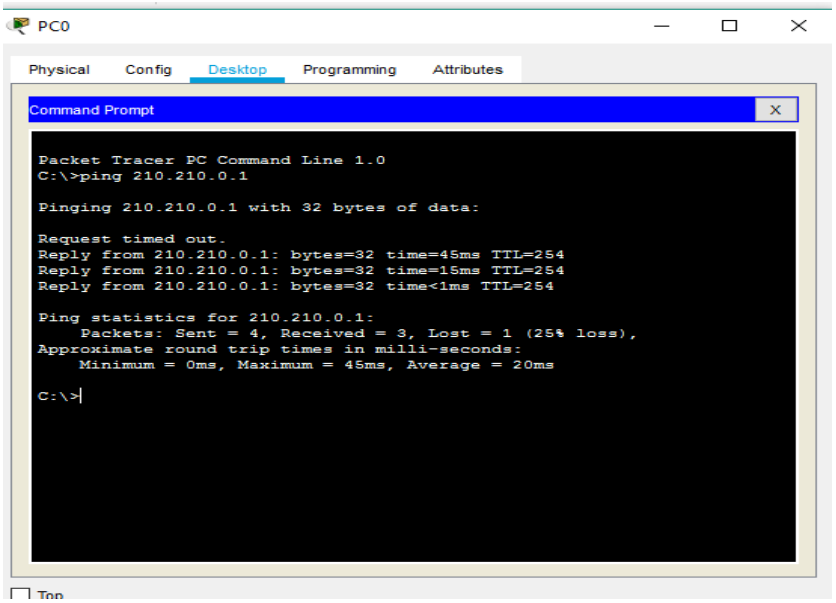


Рисунок 14.10 – Проверка сети

14.5 Контрольные вопросы:

1. Что такое WI-FI?
2. Преимущества WI-FI.
3. Недостатки WI-FI.

Лабораторная работа № 15. Траблшутинг корпоративной сети

15.1 Цель работы: исследование сети на неисправность.

15.2 Подготовка к работе:

Повторить разделы: создание стандартных технологий локальных сетей; коммутация сообщений, назначение IP-протокола, модель OSI, различие между сообщением и сигналом, определение пакета, кадра, фрейма.

Теоретическое описание

Траблшутинг (*troubleshooting* — устранение неполадок, работа над проблемой) — форма решения проблем, часто применяемая к ремонту неработающих устройств или процессов. Представляет собой систематический, опосредованный определённой логикой поиск источника проблемы с целью её решения. Траблшутинг как поиск и устранение неисправностей необходим для поддержания и развития сложных систем, где проблема может иметь множество различных причин.

DNS — компьютерная распределённая система для получения информации о доменах. Чаще всего используется для получения IP-адреса по имени хоста (компьютера или устройства), получения информации о маршрутизации почты и/или обслуживающих узлах для протоколов в домене (SRV-запись).

Распределённая база данных DNS поддерживается с помощью иерархии DNS-серверов, взаимодействующих по определённому протоколу.

Основой DNS является представление об иерархической структуре имени и *зонах*. Каждый сервер, отвечающий за имя, может *передать* ответственность за дальнейшую часть домена другому серверу (с административной точки зрения — другой организации или человеку), что позволяет возложить ответственность за актуальность информации на серверы различных организаций (людей), отвечающих только за «свою» часть доменного имени.

DNS обладает следующими характеристиками:

- *Распределённость администрирования*. Ответственность за разные части иерархической структуры несут разные люди или организации.
- *Распределённость хранения информации*. Каждый узел сети в обязательном порядке должен хранить только те данные, которые входят в его *зону ответственности*, и (возможно) адреса *корневых DNS-серверов*.
- *Кэширование информации*. Узел *может* хранить некоторое количество данных не из своей зоны ответственности для уменьшения нагрузки на сеть.
- *Иерархическая структура*, в которой все узлы объединены в дерево, и каждый узел может или самостоятельно определять работу нижестоящих узлов, или *делегировать* (передавать) их другим узлам.
- *Резервирование*. За хранение и обслуживание своих узлов (зон) отвечают (обычно) несколько серверов, разделённые как физически, так и

логически, что обеспечивает сохранность данных и продолжение работы даже в случае сбоя одного из узлов.

DNS важна для работы Интернета, так как для соединения с узлом необходима информация о его IP-адресе, а для людей проще запоминать буквенные (обычно осмысленные) адреса, чем последовательность цифр IP-адреса. В некоторых случаях это позволяет использовать виртуальные серверы, например, HTTP-серверы, различая их по имени запроса. Первоначально преобразование между доменными и IP-адресами производилось с использованием специального текстового файла hosts, который составлялся централизованно и автоматически рассылался на каждую из машин в своей локальной сети. С ростом Сети возникла необходимость в эффективном, автоматизированном механизме, которым и стала DNS.

15.3 Описание лабораторной работы

Рисунок 15.5 – Проверка получений ip-адреса ПК5 по DHCP

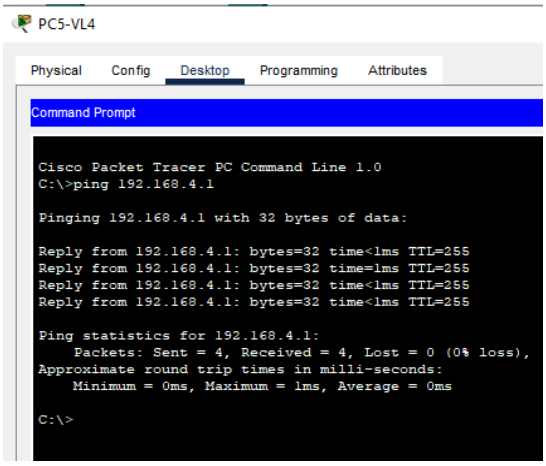


Рисунок 15.6 – Проверка пинга с ПК5 на шлюз

2. PC1 не видит шлюз по умолчанию.

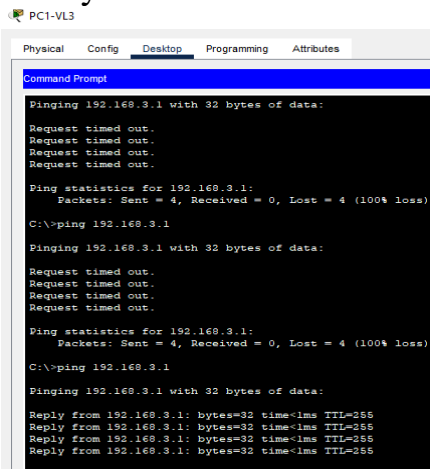


Рисунок 15.7 – Проверка пинга с ПК1 на шлюз

3. PC4 не пингуется.

```
C:\>
C:\>
C:\>ping 192.168.5.2

Pinging 192.168.5.2 with 32 bytes of data:

Request timed out.
Reply from 192.168.5.2: bytes=32 time<1ms TTL=127
Reply from 192.168.5.2: bytes=32 time=1ms TTL=127
Reply from 192.168.5.2: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.5.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Рисунок 15.8 – Проверка пинга с ПК1 на сервер1

15.5 Контрольные вопросы:

1. Опишите DNS.
2. Различия между ip-адресом и mac-адресом.
3. Что такое ARP?
4. Различия статического ip-адреса и динамического адреса.

Дополнительная информация

Решение

PC5 не получает адрес по DHCP

Нужно было прописать на switch1 команды.

interface FastEthernet0/3

switchport access vlan 4

switchport mode access

PC1 не видит шлюз по умолчанию

Нужно было прописать в switch0 на интерфейсе FastEthernet0/ Задать влан access, до этого он стоял как транк.

interface FastEthernet0/3

switchport access vlan 4

switchport mode access

PC4 не пингуется

Шлюз по умолчанию на ПК4 нужно изменить на 192.168.3.1.

Список использованной литературы

1. Леинванд. Конфигурирование маршрутизаторов Cisco / Леинванд, Аллан. – М.: Вильямс; Издание 2-е, 2001. – 368 с.

2. Пакет Создание сетей удаленного доступа Cisco / Пакет, Кэтрин. – М.: Вильямс, 2003. – 672 с.

3. Петушок – Золотой Гребешок. Little Cock Crimson Comb. – М.: Союз кинематографистов СССР, 1975. – 452 с.

4. Программа сетевой академии Cisco CCNA 1 и 2. Вспомогательное руководство (+ CD-ROM). – М.: Вильямс, 2007. – 895 с.

5. Чепмен, Д. Брандмауэры Cisco Secure PIX / Д. Чепмен, Э. Фокс. – М.: Вильямс, 2003. – 384 с.

6 www.netacad.kz

7 Cisco Documentation

8 *Configuring IPv6 for Cisco IOS* (Edgar Parenti, Jr., Eric Knnip, Brian Browne, Syngress, ISBN# 1928994849)

9 *Interconnections: Bridges & Routers, Second Edition* (Perlman, Addison Wesley, ISBN# 0201634481)

10"Internetworking Technology Overview" Available through Cisco Store under doc # DOC-785777

11*Internetworking with TCP/IP, Vol.1: Principles, Protocols, and Architecture (4th Edition)* (Comer, Prentice Hall, ISBN# 0130183806)

12*IPv6: Theory, Protocol, and Practice, 2nd Edition* (Pete Loshin, Morgan Kaufmann, ISBN# 1558608109)

13*LAN Protocol Handbook* (Miller, M&T Press, ISBN# 1558510990)

14*Routing In the Internet (2nd Edition)* (Huitema, Prentice Hall, ISBN# 0130226475)

15*TCP/IP Illustrated: Volumes 1, 2, and 3* (Stevens/Wright, Addison Wesley, ISBN# 0201633469, 020163354X, 0201634953)

16*Wi-Fi (802.11) Network Handbook* (Neil P. Reid, Ron Seide, McGraw Hill Osborne Media, ISBN# 0072226234)

Дополнительный план на 2022 г., поз. 16

Катипа Сламбаевна Чежимбаева

Современные методы измерений в телекоммуникациях

Методические указания к выполнению лабораторных работ для магистрантов по образовательной программе 7М06201 – «Радиотехника, электроника и телекоммуникации» Направление «Телекоммуникации»

Редактор Жанабаева Е.Б.
Специалист по стандартизации Ануарбек Ж.А.

Подписано в печать Формат 60×84 1/16
Тираж 50 экз. Бумага типографическая №
Объём 6,0 уч.-изд. л. Заказ Цена 3000 тг.

Копировально-множительное бюро
некоммерческого акционерного общества
«Алматинский университет энергетики связи»
050013, Алматы, ул. Байтурсынова, 126/1