

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ**

**ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ  
«ДОНСКОЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»**

**(ДГТУ)**

Факультет Информатика и вычислительная техника

Кафедра Кибербезопасность информационных систем

**ОТЧЕТ ПО ЛАБОРАТОРНЫМ РАБОТАМ**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Автор |  | | |  | Ковалев Д. П. | | | |
|  | (подпись, дата) | | |  |  | | | |
| Обозначение | ИиВТ.10.05.01.13 | | Группа | | | | ВКБ32 |  |
| Направление подготовки | | 10.05.01 Компьютерная безопасность | | | | | |  |
| Профиль | Математические методы защиты информации | | | | | | |  |
| Проверил |  | | |  | |  | |  |
|  | (подпись, дата) | | |  | |  | |  |

Ростов-на-Дону

2025

Содержание

[Лабораторная работа №1 3](#_Toc179124024)

[Лабораторная работа №2 6](#_Toc179124025)

[Лабораторная работа №3 11](#_Toc179124026)

[Лабораторная работа №4 13](#_Toc179124027)

[Лабораторная работа №5 21](#_Toc179124028)

[Лабораторная работа №6 30](#_Toc179124029)

[Лабораторная работа №7 41](#_Toc179124030)

[Лабораторная работа №8 57](#_Toc179124031)

# **Лабораторная работа №1**

**Тема:** «Изучение базового функционала Cisco Packet Tracer»

**Цель:** научиться создавать простые сетевые соединения.

**Задание 1**. Изучить режим симуляции в Cisco Packet Tracer.

Нам нужно построить сеть, которая содержит: 4 узла, сервер, принтер и два концентратора. Концентраторы меж собой соединяются кроссоверным кабелем.

Изображение выглядит как диаграмма, текст, линия, карта

Автоматически созданное описание

Рисунок 1 – схема, которую надо построить по условию

Наша задача заключается в том, чтобы посмотреть, как проходит пакет через разные узлы в сети, а также посмотреть, как пакет проходится по уровням модели OSI.

Для этого мы нажмем “Shift + S” для входа в режим мониторинга. Для тестирования нагрузки используется протокол ICMP, который обычно передает ошибки и тому подобное. Он работает вообще на 3 уровне OSI – сетевой. Поэтому отключим остальные протоколы, которые будут использоваться для передачи пакета. Нажмите “Edit Filters”, а потом уберите все галочки. Должно получиться, как на рисунке 2.

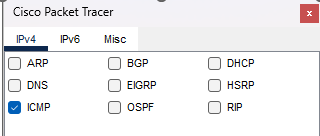


Рисунок 2 – протоколы, которые будут использоваться

Теперь запустите анимацию и можете нажимать на каждый event, в котором описывается в каком моменте сейчас оказывается пакет в сети. Получается, что у нас в ping вернет разницу по времени за какой период пришел этот пакет. Почему у нас иногда есть второй уровень OSI? Потому что MAC адреса работают на этом уровне. Обратите внимание на рисунок 3, где показано на каком сейчас моменте находится действие в модели OSI.

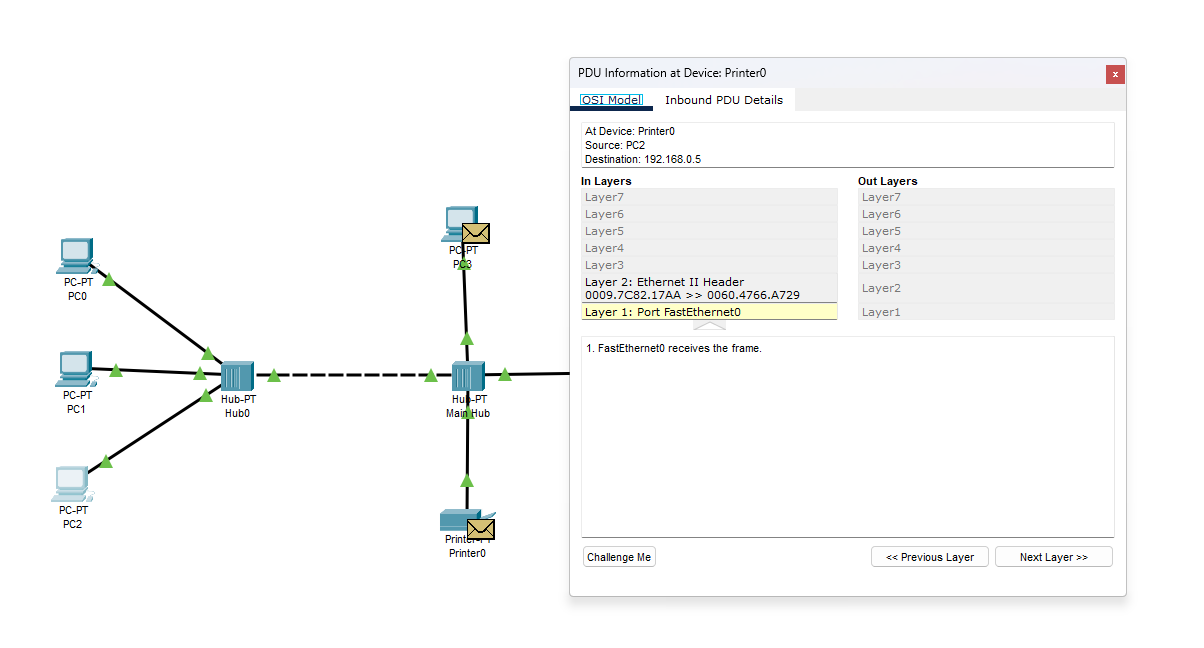


Рисунок 2 – состояние системы, где показан 1 OSI уровень

Также мы можем посмотреть структуру пакета, для этого нужно нажать кнопку “Inbound PDU Details”. На рисунке 3 можем обратить внимание, что показываются различные параметры Headers, Content – Body, Footer.

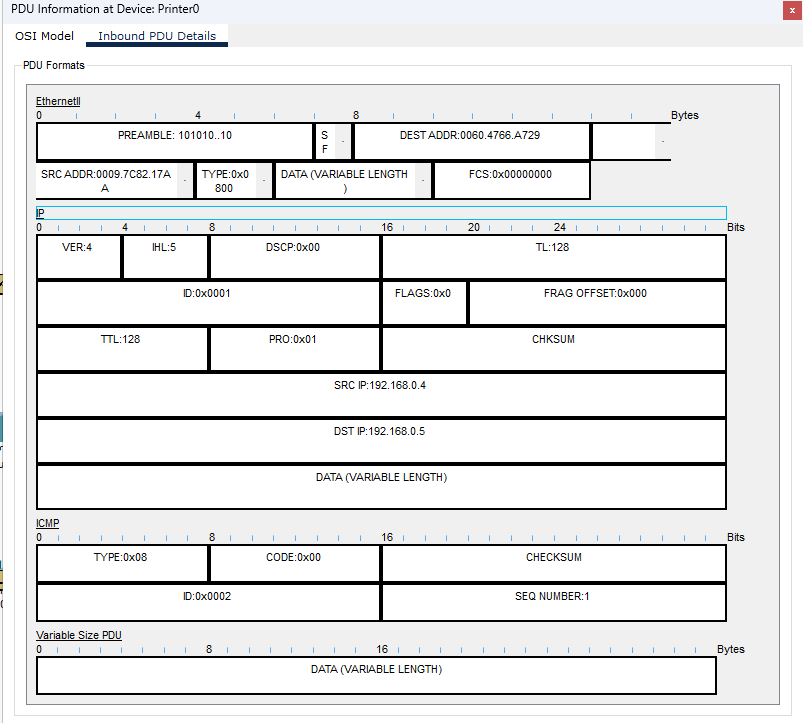


Рисунок 3 – структура пакета

**Контрольные вопросы:**

1. Для чего используется режим симуляции?

Режим симуляции в Cisco Packet Tracer используется для моделирования

работы сети и просмотра процесса передачи данных между устройствами. Это позволяет визуализировать и анализировать, как пакеты данных проходят через сеть, какие протоколы используются, и какие изменения происходят с пакетами на разных уровнях модели OSI.

1. Как просмотреть прохождение пакета по уровням модели OSI?

В режиме симуляции можно просмотреть прохождение пакета по уровням модели OSI, выбрав пакет в списке событий и наблюдая за его прохождением через различные уровни (Physical, Data Link, Network, Transport, и т.д.) в окне "Packet Details".

1. Можно ли определить причину того, что посланный в режиме симуляции пакет не дошел до адресата и на каком этапе произошел сбой работы сети?

Да, можно. В режиме симуляции можно отследить путь пакета и увидеть, на каком этапе произошел сбой. Это можно сделать, просматривая список событий и анализируя сообщения об ошибках, которые могут указывать на проблемы с маршрутизацией, адресацией, или другими аспектами сети.

1. Укажите в составе пакета IP адреса отправителя и получателя.

В составе пакета IP адреса отправителя и получателя находятся в заголовке IP пакета. Адрес отправителя указывается в поле "Source IP Address", а адрес получателя — в поле "Destination IP Address".

1. Как изменить фильтры списка событий?

Фильтры списка событий можно изменить, используя панель фильтров в режиме симуляции. Можно фильтровать события по типу (например, ICMP, TCP, UDP), по устройствам, или по другим параметрам, чтобы упростить анализ и отслеживание пакетов.

1. Как в режиме симуляции определить, какие протоколы были задействованы в работе сети?

В режиме симуляции можно определить, какие протоколы были задействованы, просматривая список событий и детали пакетов. В окне "Packet Details" можно увидеть, какие протоколы используются на разных уровнях модели OSI.

1. Как в режиме симуляции проследить изменение содержимого пакета при прохождении его по сети?

В режиме симуляции можно проследить изменение содержимого пакета, выбирая пакет в списке событий и просматривая его детали на каждом этапе прохождения через сеть. В окне "Packet Details" можно увидеть, как изменяются заголовки и данные пакета на разных уровнях модели OSI.

8. Перечислите основные возможности режима симуляции.

·      Визуализация прохождения пакетов через сеть.

·      Анализ работы сети на разных уровнях модели OSI.

·      Отслеживание изменений в содержимом пакетов.

·      Фильтрация событий для упрощения анализа.

·      Определение причин сбоев и ошибок в сети.

·      Просмотр задействованных протоколов и их взаимодействия.

**Задание 2.** Настройка сетевых сервисов.

Создадим теперь схему, на которой будет два сервера, свитч и ПК. В нашем случае Server1 будет выступать в роли DNS и Web сервера, а Server2 – DHCP сервер. Компьютер будет получать параметры протокола из стека TCP/IP c DHCP сервера и открывать сайт на сервере 1. Строение схемы представлено на рисунке 4.

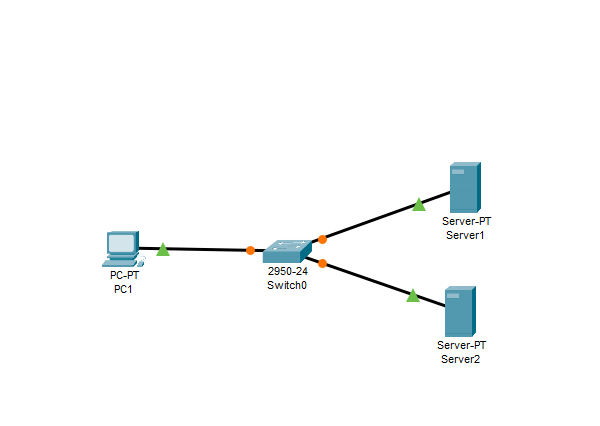


Рисунок 4 – результат подключения устройств

Для начала зайдем в настройки PC1, там выставим параметры на протокол DHCP, чтобы наш сервер выдавал нужный IP адрес на наши устройства, которые подключаются по протоколу DHCP. Как это сделать? Заходим (Config -> IP Configuration -> DHCP), выставляем все, как на рисунке 5.

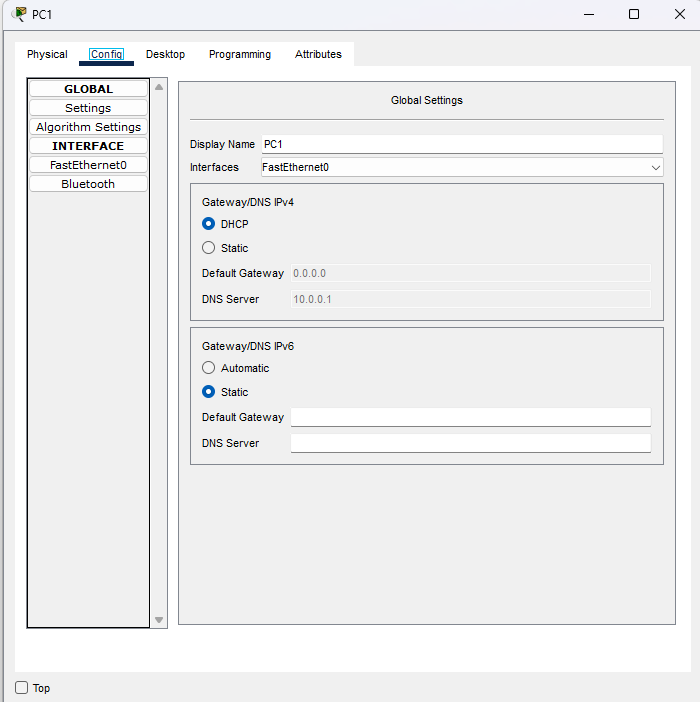


Рисунок 5 – настройки подключения по IP у PC1

Для Server1, Server2 выставим статические IP адреса вручную. Также заходим в (Config -> Ip Configuration -> Static). Результат настройки у Server1 можете увидеть на рисунке 6.

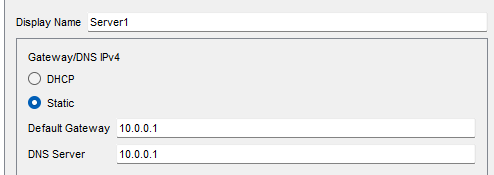


Рисунок 6 – параметры настройки для

Настроим службу DNS на Server1. Для этого нажмите на “Server1”, потом войдите во вкладку “Services”. Там будет служба “DNS”, её нужно включить, а потом создать несколько ресурсных записей, которые показывают, что и как куда перенаправлять. Возникают следующие вопросы, а что же такое типы ресурсных записей.

Ресурсная запись “типа А” нужна, чтобы указывать с корневого домена на нужный IP адрес, куда будет перенаправляться запрос. Ресурсная запись типа “CNAME” нужна, чтобы другие субдомены отправляли на корневой домен, который в свою очередь через ресурсную запись типа А отправляла на IP. У вас должно получиться, как на рисунке 7.

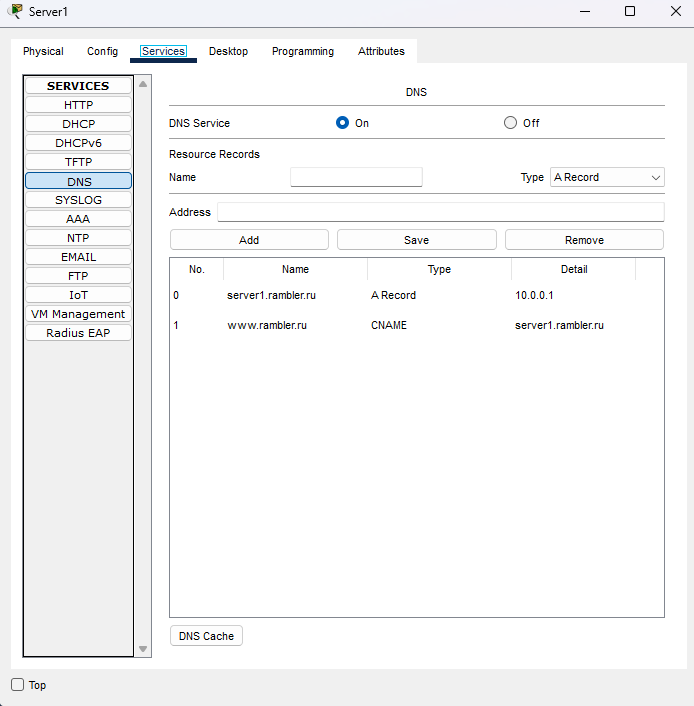


Рисунок 7 – настройки DNS сервера

Теперь на Server1 в Service/HTTP нужно создать index.html файл, на который будет отображать нашу страницу при входе. Теперь нам нужно проверить на Server1, что DNS адекватно настроился. Для этого откройте консоль на Server1 (Desktop -> Command Prompt -> nslookup www.rambler.ru).

Теперь нам надо настроить DHCP службу, которая выдает IP адрес на наш ПК. Для этого заходим на Server2, задаем DNS сервер, начальный IP адрес, максимальное количество пользователей и все. У Вас должно получиться, как на рисунке 8.

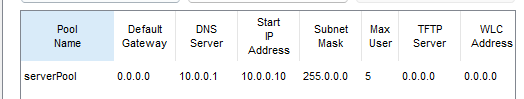


Рисунок 8 – параметры DNS сервера

Теперь остается на ПК получить только параметры с DHCP сервера. Для этого в консоли нужно ввести команды (ipconfig /release (сброс настроек) -> ipconfig /renew (новые данные с DHCP)). Должно у Вас все получиться, как на рисунке 9.

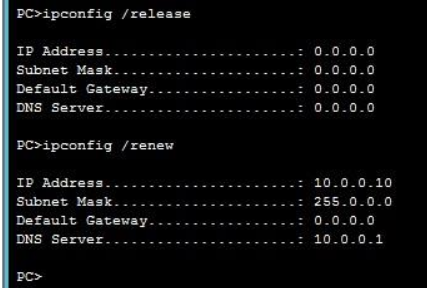


Рисунок 9 – результат команд

Теперь на клиенте можем сделать запрос, чтобы получить данные с Application Server, где находится index.html.

**Контрольные вопросы**:

1. Что такое рекурсивный запрос DNS и какова схема его работы?

Рекурсивный запрос DNS — это запрос, в котором DNS-сервер обязуется вернуть окончательный ответ клиенту, даже если для этого ему придется обратиться к другим DNS-серверам. Схема работы:

·      Клиент отправляет запрос на локальный DNS-сервер.

·      Локальный DNS-сервер проверяет свой кэш и зоны.

·      Если информации нет, сервер отправляет запрос на корневые DNS-серверы.

·      Корневые серверы направляют запрос на соответствующие TLD (Top-Level Domain) серверы.

·      TLD серверы направляют запрос на авторитетные DNS-серверы домена.

·      Авторитетные серверы возвращают окончательный ответ локальному DNS-серверу, который передает его клиенту.

2. Укажите назначение типов ресурсных записей в прямой и обратной зонах DNS.

Прямая зона:

* A (Address): сопоставляет доменное имя с IPv4 адресом.
* AAAA (IPv6 Address): сопоставляет доменное имя с IPv6 адресом.
* CNAME (Canonical Name): указывает alias одного имени на другое.
* MX (Mail Exchange): указывает почтовые серверы для домена.
* TXT (Text): содержит текстовую информацию для домена.

Обратная зона:

* PTR (Pointer): сопоставляет IP-адрес с доменным именем.

3. Как на DNS сервере настраивается пересылка пакетов на другие DNS сервера?

Через ресурсные записи

4. Опишите работу службы DHCP.

Служба DHCP (Dynamic Host Configuration Protocol) автоматически назначает IP-адреса и другие сетевые параметры устройствам в сети. Работа DHCP: (DORA - первые буквы)

* Клиент отправляет широковещательный запрос DHCP DISCOVER.
* DHCP-сервер отвечает предложением DHCP OFFER.
* Клиент выбирает предложение и отправляет запрос DHCP REQUEST.
* Сервер подтверждает назначение параметров ответом DHCP ACK.

5. Как настраивается клиент DHCP?

В службах сервера необходимо заполнить колонки по типу: имя пула, основной шлюз, DNS-server, начальный IP-adress, маска, макс. кол-во пользователей, …

6. Укажите местоположения папки с контентом Web-узла и FTP сервера.

Web-узел: Контент обычно хранится в папке, указанной в конфигурации веб-сервера. Например, **/var/www/html** для Apache на Linux или **C:\inetpub\wwwroot** для IIS на Windows).

FTP сервер: Контент обычно хранится в папке, указанной в конфигурации FTP-сервера (например, **/var/ftp** для vsftpd на Linux или **C:\inetpub\ftproot** для IIS FTP на Windows)

7. Как определяется состав обратных зон DNS сервера в корпоративной сети?

Состав обратных зон DNS сервера определяется на основе IP-адресов, используемых в сети. Обратные зоны создаются для каждого диапазона IP-адресов, и в них содержатся PTR записи, которые сопоставляют IP-адреса с доменными именами.

**Задание 3.** Знакомство с командами IOS.

Для начала создадим схему, которая будет состоять из 3 роутеров, где с помощью консоли мы будем дальше работать. Схема представлена на рисунке 10.

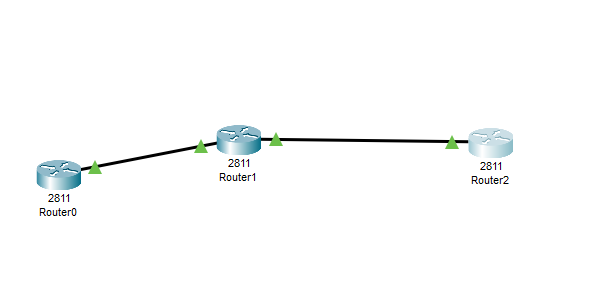


Рисунок 10 – строение схемы для 3 задания

Как посмотреть список всех доступных команд? Ответ: “?”, у нас получится, как на рисунке 11.

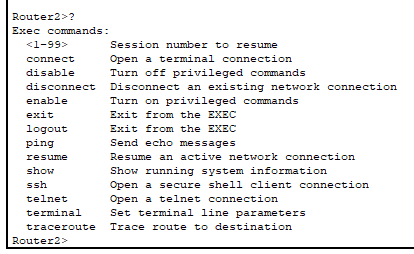


Рисунок 11 – список команд для управления роутером

Теперь войдем в привилегированный режим, используя следующий набор команд (“en” -> “?”), чтобы посмотреть список там возможных команд, результат операций представлен на рисунке 12.

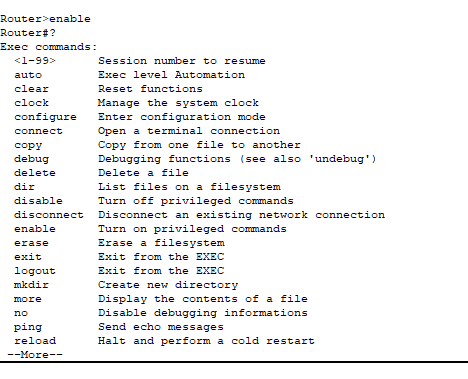


Рисунок 12 – список команд в привилегированном режим

Теперь перейдем в режим конфигурации, для этого нужно ввести команду “config terminal”. Теперь для Router1 зададим имя хоста – “hostname Router1”. На фото кажется, что ничего толком не поменялось. На самом деле так, потому что я операции проводил под Router1, а не на Router0. Команда по установке хоста показана на рисунке 13.



Рисунок 13 – результат команды по установлению имени хоста

Теперь можем установить пароль на наш роутер, чтобы не каждый мог входить в привилегированный режим. Для этого мы в “config terminal”, вводим “enable password parol”.

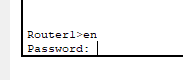


Рисунок 14 – ввод пароля для роутера

Теперь мы выйдем в пользовательский режим. Для этого используем команду “disable”. Теперь мы введем все show команды, которые просят по методичке. Все подсказки команд видны на рисунке 15.

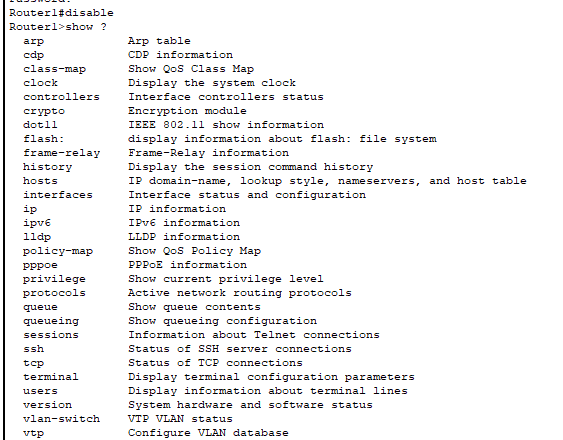


Рисунок 15 – подсказка для show

Давайте введем команду для просмотра времени “show clock”. Результат представлен на рисунке 16.



Рисунок 16 – время на устройстве

Давайте теперь просмотр флэш память на устройстве. Для этого введем команду “show flash”, результат представлен на рисунке 17.

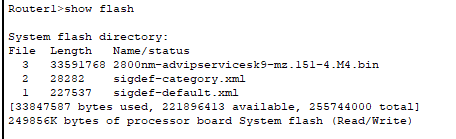


Рисунок 17 – параметры ОС в роутере

Теперь просмотрим историю команд, введя “show history”. Результат представлен на рисунке 18.

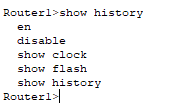
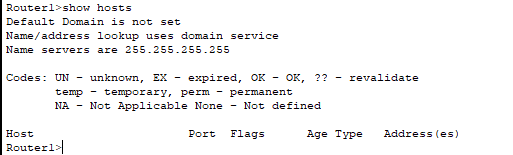


Рисунок 18 – история команд

Можно увидеть список хостов и IP адресов всех их интерфейсов. Результат представлен на рисунке 19.



Результат 19 – параметры хостов и IP адресов

Теперь введем команду для просмотра детальной информации о каждом интерфейсе. Здесь можно использовать команду “show interfaces”, результат можно увидеть на рисунке 20.

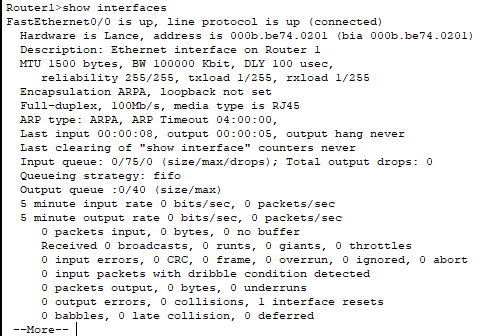


Рисунок 20 – просмотр всех интерфейсов

Теперь воспользуемся командой для вывода информации о каждой telnet сессии. Нам нужна команда “show sessions”. Результат представлен на рисунке 21.



Рисунок 21 – показывает информацию о сессиях

Теперь просмотрим следующие конфигурационные параметры терминала. Для этого воспользуемся командой “show terminal”. Результат на рисунке 22.

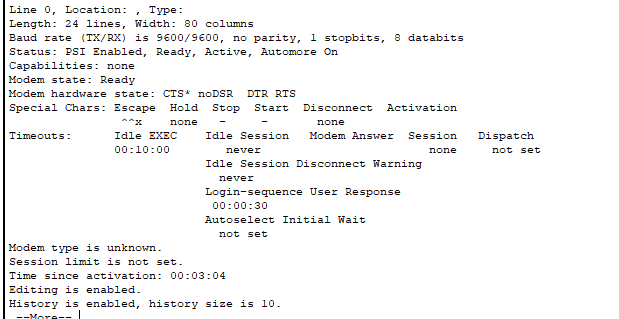


Рисунок 22 – результат вывода команды “show terminal”

Просмотрим теперь всех пользователей, которые присоединились к устройству по терминальным линиям. Для этого воспользуемся командой “show users”. Результат представлен на рисунке 23.



Рисунок 23 – результат вывода команды “show users”

Давайте теперь воспользуемся командой для просмотра контроллеров интерфейсов. У нас есть команда “show controllers”. Результат представлен на рисунке 24.

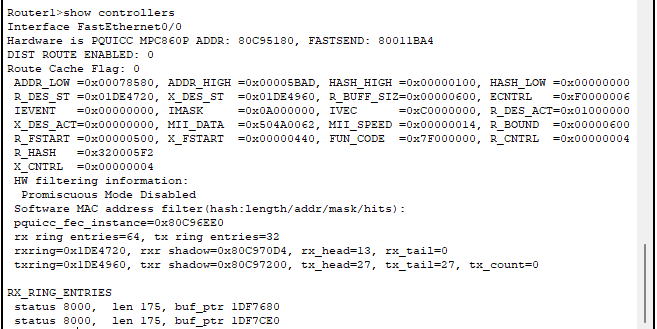


Рисунок 24 – команда для просмотра параметров контроллера

Просмотрим теперь в привилегированном режиме все команды, воспользуемся в начале командой “en”, а потом “show ?”. Результат представлен на рисунке 25.



Рисунок 25 – команда для просмотра всех возможностей show в привел. режиме

Теперь попробуем узнать конфигурацию нашего роутера. Для этого есть команда “Show configuration” или “show running-config”. Результат выполнения команды представлен на рисунке 26.

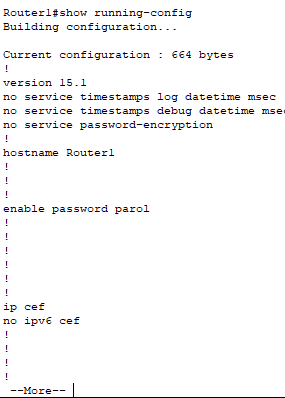


Рисунок 26 – конфигурация нашего роутера

Воспользуемся теперь командой для просмотра протоколов третьего уровня. Вот команда “show protocols”, а результат на рисунке 27.

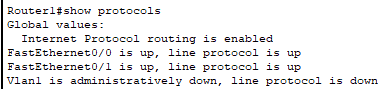


Рисунок 27 – результат команды для просмотра всех протоколов

Рассмотрим теперь команды настройки интерфейсов сетевого уровня. В самом начале нам нужно перейти в режим конфигурации. Для этого воспользуйтесь командой “conf t”. Результат представлен на рисунке 28.

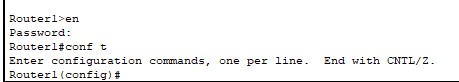


Рисунок 28 – переход в режим конфигурации

Теперь попробуем настроить Ethernet интерфейс, который у нас есть по умолчанию. Введем команду “interface FastEthernet0/0” для настройки. Результат ввода команды виден на рисунке 29.



Рисунок 29 – режим конфигурации интерфейса

Теперь с помощью команды “?” просмотрим какие возможности под данным пространством имен. Результат представлен на рисунке 30.

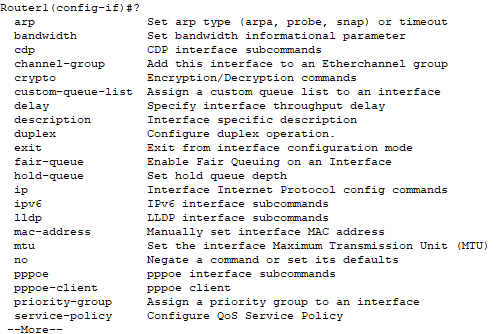


Рисунок 30 – возможные команды настройки интерфейса

Давайте теперь попробуем добавить описание на наш интерфейс и посмотреть, как и что там. Для этого мы можем воспользоваться командами (“no shutdown” -> “description Ethernet interface on Router 1” -> “end” -> “show interface”). Результат представлен на рисунке 31.

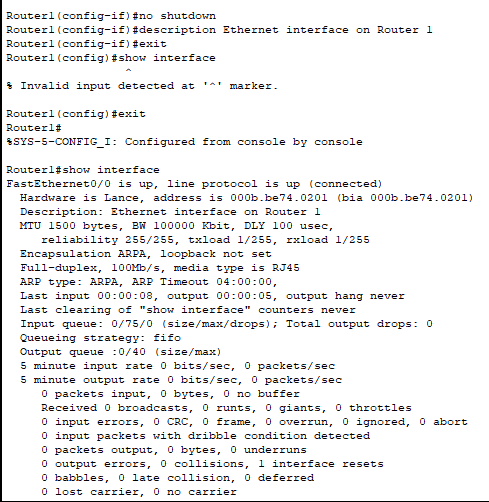


Рисунок 31 – вывод настроек Router0 на консоль

Теперь зайдем на Router2, поменяем его имя хоста, а также включим интерфейс. Для этого воспользуемся командами (“conf t”, “hostname Router2”, “interface fa0/0”, “no shutdown”).

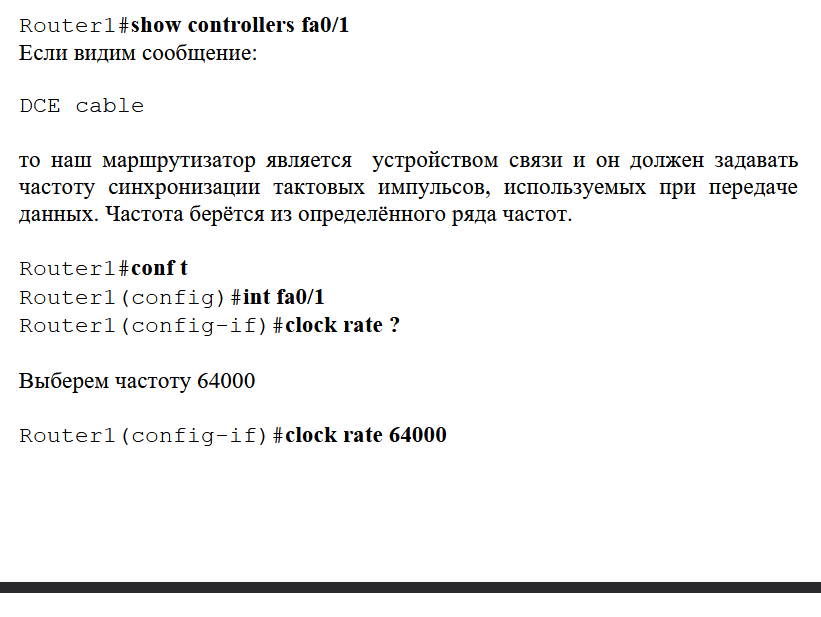


Рисунок 32 – настройка частоты тактовых импульсов

# **Контрольные вопросы.**

# 1. Какой командой можно посмотреть текущие настройки роутера?

Посмотреть можно текущие настройки роутера, используя следующую команду: “show running config”.

# Какими командами настраивается сетевой интерфейс роутера.

Сетевой интерфейс роутера настраивается с помощью следующей последовательности команд (interface -> ip address -> no shutdown).

# Как просмотреть конфигурационные настройки коммутатора?

Также можно воспользоваться командой “show running config”.

# Как определить распределение VLN по портам коммутатора?

Можно воспользоваться командой “show vlan brief”. VLN в свою очередь – это виртуальный номер телефона, который обычно используется для приема текстовых сообщений SMS или телефонных звонках.

# Перечислите основные режимы конфигурации при настройке коммутатора.

* User EXEC mode
* Privileged EXEC mode
* Global configuration mode
* VLAN configuration mode
* Interface configuration mode
* Line configuration mode

1. Перечислите основные режимы конфигурации при настройке роутера.

* User EXEC mode
* Privileged EXEC mode
* Global configuration mode
* Interface configuration mode
* Line configuration mode
* Router configuration mode (для настройки маршрутизации)

# Как посмотреть таблицу маршрутизации на роутере?

Можно воспользоваться командой “show ip route”.

# Какие команды формируют таблицу маршрутизации роутера?

* Статические маршруты: ip route
* Динамические маршруты: настройка протоколов маршрутизации, таких как RIP, OSPF, EIGRP. Например, router ospf 1, network area.

# Какими командами настраиваются VLN на коммутаторе?

Рассмотрим несколько сценариев, где настраивается VLN (VLAN). Первый случай – это создание VLAN. Тут надо зайти в режим конфигурации (configure terminal), потом ввести номер VLAN (vlan [Number of Vlan]), ну и имя (name [Name of Vlan].

Можно назначить порт для VLAN. Здесь мы в начале используем команду (interface), где мы преждевременно должны быть в режиме конфигурации. Теперь можно задать (switchport mode access), а потом (switchport access vlan [Number of VLAN]).

VLAN – это виртуальная локальная сеть. Это нужно для удобной связи элементов через тот же самый Switch. Грубо говоря, VLAN создает подсеть, чтобы мы соединили нужные нам устройства и только туда шли данные, а не на весь ПК. Как раз свитч умеет так работать.

# Какими командами настраивается взаимодействие между VLN?

Можно воспользоваться следующей последовательностью команд (interface -> switchport mode trunk -> switchport trunk allowed vlan).

**Задание 4.** Настройка протокола RIP.

Построим схему, которую указали в условии задания. Результат представлен на рисунке 33.

Изображение выглядит как диаграмма, снимок экрана, линия

Автоматически созданное описание

Рисунок 33 – строение схемы для сети

Я, так понимаю, что здесь мы определяем в какой подсети будет работать каждый switch, в методическом материале указано, что мы их должны установить в Switch1 – сеть 10.11.0.0/16, Switch2 – сеть 10.12.0.0/16.

Введем на устройствах теперь следующую адресацию для удобства на разные интерфейсы. Представлю лишь на фото настройку Switch1 на интерфейсе fa0/0, рисунок 34.

Изображение выглядит как текст, снимок экрана, программное обеспечение, число

Автоматически созданное описание

Рисунок 34 – настройка fa0/0 на switch1

После того, как мы выставили все нужные параметры по условию задачи, нам надо настроить протокол RIP на роутерах. Для чего нужен протокол RIP? Это протокол маршрутизации для небольших локальных внутренних сетей. Считается уже устаревшим.

Перейдем к настройке протокола. Для этого откроем у Router1 консоль, там впишем команды (“en” -> “conf t” -> “router rip” -> “network 10.11.0.0” -> “network 10.10.0.0” -> “version 2”). Порядок команд в терминале представлен на рисунке 35.

Изображение выглядит как текст, снимок экрана, Шрифт, документ

Автоматически созданное описание

Рисунок 35 – настройка rip для Router1

Аналогичные настройки надо проделать и для Router1. То же самое проделаем и для Router2, все команды представлю на рисунке 36.

Изображение выглядит как текст, Шрифт, белый, алгебра

Автоматически созданное описание

Рисунок 36 – настройка rip для Router2

Попробуем пингануть PC2 c PC1, результат представлен на рисунке 37.

Изображение выглядит как текст, снимок экрана, Шрифт, дизайн

Автоматически созданное описание

Рисунок 37 – результат пинга с PC1 на PC2

**Задание 5**. Многопользовательский режим работы.

Здесь нам нужно запустить две сессии (instance) приложения для параллельной работы. Задача заключается в том, чтобы подружить сети в разных сессиях между собой.

Построим сеть в 1 сессии, что вообще и как должно быть? Мы должны добавить соседнюю часть через Multiuser. Для этого, мы его должны добавить (внимательно смотрите снизу, где устройства). Результат представлен на рисунке 40.

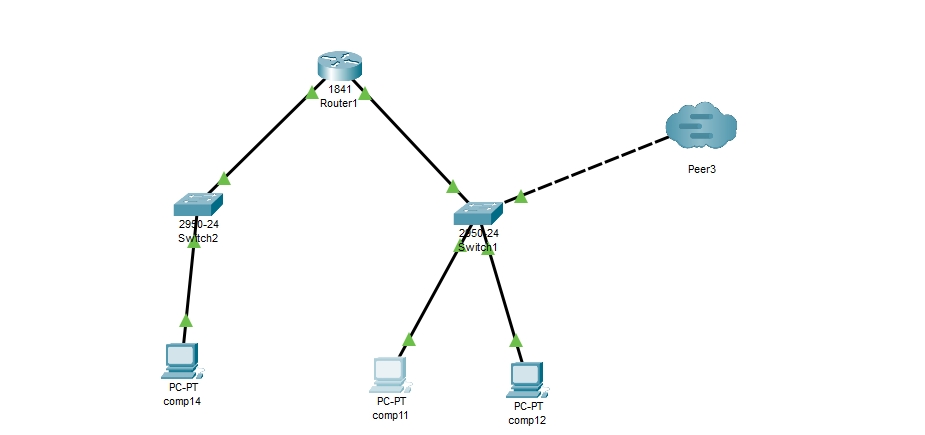


Рисунок 40 – подключение сетей из разных инстансов приложения

Как же была произведена настройка peer подключения? Все свои настройки прикрепляю на рисунке 41.

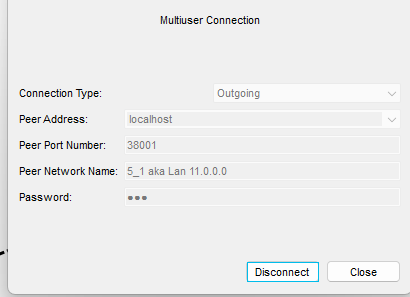


Рисунок 41 – топология звезда с использованием свитча

Самое главное – настроить все комплектующие. Теперь мы можем пропинговать с одного инстанса приложение на другое. Техника никак не меняется, результат представлен на рисунке 42.

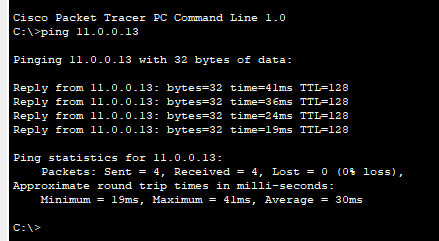


Рисунок 42 – пинг с 1 инстанса приложения на другое

**Задание 6.** Протоколы SMTP и POP3.

Для исследования данных протоколов построим схему, которая представлена на рисунке 43.

Изображение выглядит как линия

Автоматически созданное описание

Рисунок 43 – строение сети для задания

Рассмотрим по отдельности каждый протокол. Для чего они вообще нужны? Они оба нужны для взаимодействия с электронными письмами, в плане отправка, получение и т.п. Протокол POP3 является устаревшим, а SMTP стандартом индустрии прямо сейчас.

Произведем настройку, как указано в методичке. Все параметры для схемы представлены на рисунке 44.

Изображение выглядит как текст, снимок экрана, Шрифт, число

Автоматически созданное описание

Рисунок 44 – настройка сети

В качестве почтовых серверов выступают два сервера 172.16.0.20 и сервер 172.16.0.40. Каждый из этих серверов будет настроен и на SMTP протокол, и на POP3 протокол.

Настроим DNS на сервере 0, нам нужно сделать так, чтобы с доменов переводило на IP сразу. Для этого, у нас запись должна быть типа А. Результат представлен на рисунке 45.

Изображение выглядит как текст, снимок экрана, линия, Шрифт

Автоматически созданное описание

Рисунок 45 – настройка DNS

Теперь включим два протокола для email на сервере 176.16.0.20, должно получиться то же самое, что и на рисунке 46. Я сразу создал и пользователя

Изображение выглядит как текст, снимок экрана, программное обеспечение, дисплей

Автоматически созданное описание

Рисунок 46 – настройка почты

Теперь нам нужно настроить эти же два протокола на другом сервере, учитывая, что первый сервер ещё выступал в роли DNS сервера. Для этого у Server1 выставим параметры DNS, как на рисунке 47.

Изображение выглядит как текст, снимок экрана, программное обеспечение, дисплей

Автоматически созданное описание

Рисунок 47 – настройка DNS Server1

Создадим на Server1 пользователя также, как и сделали это ранее. После создания остается только отправить письмо на почту с одного аккаунта на другой. Для этого нам нужно на клиентах настроить аккаунты пользователей. С этой целью заходим на ПК, выбираем раздел “dektop”, там мы ставим значения, как на рисунке 48.

Изображение выглядит как текст, снимок экрана, программное обеспечение, число

Автоматически созданное описание

Рисунок 48 – настройка PC1

Те же самые действия проделываем и для другого ПК. Остается попробовать отправить только письмо, заранее проставлю фильтры только на SMTP и POP3, настройка представлена на рисунке 49.

Изображение выглядит как текст, снимок экрана, число, программное обеспечение

Автоматически созданное описание

Рисунок 49 – фильтры для протоколов

Теперь мы можем отправить с 1 ПК на другой ПК письмо. Здесь в результате при отправке получилось то, что представлено на рисунке 50.



Рисунок 50 – получили сообщение на 2 ПК

# **Лабораторная работа №2**

**Тема:** Настройка VPN по средствам IPsec протокола

**Цель работы:** является изучение технологии IPsec и практическая её реализация в организации VPN на имитации реальной сети.

**Задание 1.** Настроить VPN, как показано в методическом материале.

IPsec (IP Security) — набор протоколов для обеспечения защиты данных, передаваемых по межсетевому протоколу IP. Позволяет осуществлять подтверждение подлинности (аутентификацию), проверку целостности и/или шифрование IP-пакетов. IPsec также включает в себя протоколы для защищённого обмена ключами в сети Интернет. В основном, применяется для организации VPN-соединений. Состоит из двух фаз:

1-я фаза - ISAKMP (Internet Security Association and Key Management Protocol):

Сначала 2 конечных маршрутизатора аутентифицируют друг друга и договариваются какие алгоритмы шифрования будут использоваться для будущего IPSec туннеля, а также генерируют общий секретный ключ.

В 1-й фазе устройства должны договориться об использовании следующих параметров:

* Алгоритм шифрования.
* Метод аутентификации.
* Способ обмена секретными ключами.
* Срок жизни сессии (Security Association).

Набор данных параметров определяет политику ISAKMP. Каждая политика имеет свой приоритет. Когда устройства начинают договариваться друг с другом, то последовательно перебирают все установленные политики, начиная с высшего приоритета. Как только будет обнаружено, что устройства имеют одинаковые параметры в конкретной политике, то поиск прекращается.

2-я фаза - установление IPSec туннеля:

На данном этапе создается сам IPSec туннель для передачи пользовательских данных. Поэтому маршрутизаторы снова договариваются какие протоколы шифрования и хэширования будут использоваться между ними.

Он остается активным во время работы IPSec туннеля. У каждого туннеля есть свое время “жизни”. Поэтому, если необходимо продлить сеанс связи, то мини-туннель ISAKMP обновит таймер туннеля, а также секретные ключи безопасности.

Давайте теперь приступим к выполнению заказа. В начале нам нужно построить схему сети. Предварительно в оба роутера необходимо добавить модуль NM-4A/S. Как добавить модуль, показываю на рисунке 1.

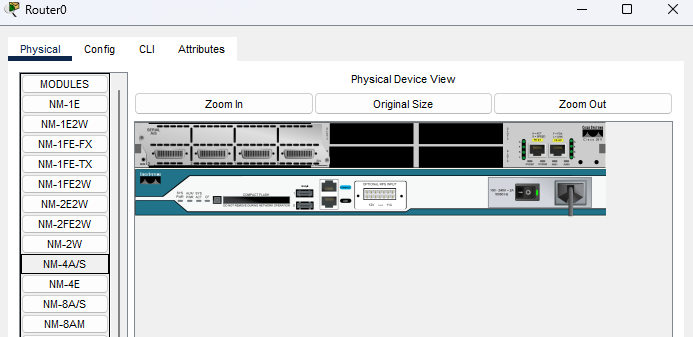


Рисунок 1 – настройка роутера с точки зрения физ. модулей

Теперь перейдем к настройке, IP адресов, масок и шлюзов. Все настройки были скопированы с методического материала, поэтому их прилагать не буду.

Прилагаю ниже фото по настройке R0, R1. Все представлено на рисунке 2.

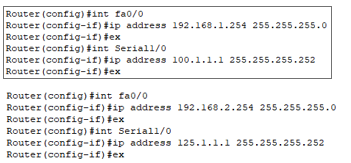


Рисунок 2 – настройки роутеров

Теперь настроим политику ISAKMP на R0, последовательно указав метод шифрования, аутентификации и обмена секретными ключами, а также время жизни сессии. В конце указываем IP адрес конечной точки туннеля, то есть маршрутизатора R1:

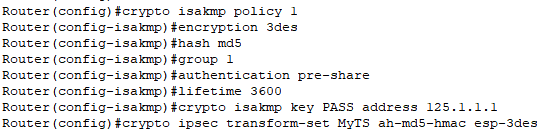


Рисунок 3 – настройка политики ISAKMP на R0

Аналогично сделаем то же самое и на R1, здесь мы выставим все параметры, как представлено в методическом материале.

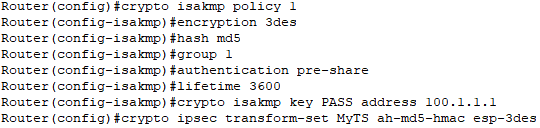


Рисунок 4 – настройка политик ISAKMP на R1

Теперь настроим параметры туннеля IPSec и создать карту шифрования для R0, привязав её к интерфейсу Serial1/0:

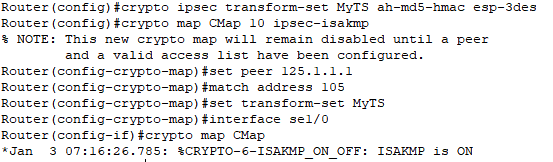


Рисунок 5 – настройка параметров туннеля IPSec для R0

Теперь проведем также настройку и для R1, результат представлен на рисунке 6.

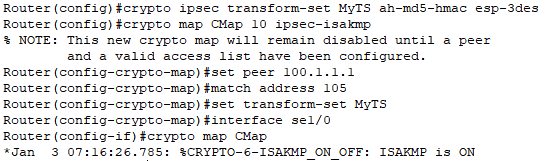


Рисунок 6 – настройка параметров туннеля для R1

Теперь настроим ACL, где указывается шифруемый траффик, для R0, а также разрешаем протоколы. Результат представлен на рисунке 7.

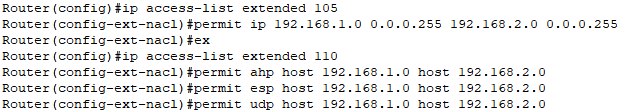


Рисунок 7 – настройка ACL для R0.

Аналогично сделаем то же самое и для R1, результат представлено на рисунке R1.

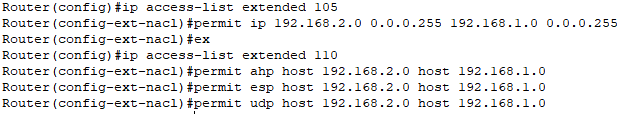


Рисунок 8 – настройка ACL для R1

Настроим теперь маршрутизацию сети и frame-relay для R0. Результат представлен на рисунке 9.

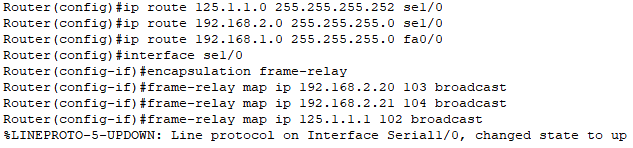


Рисунок 9 – настройка маршрутизации сети и frame-relay для R0

Повторим те же самые действия теперь и для R1. Результат представлен на рисунке 10.

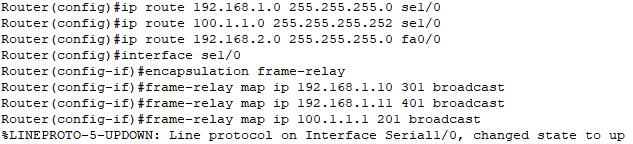


Рисунок 10 – настройка маршрутизации на R1

Теперь настроим различные параметры, связанные с Frame Relay. Результат представлен на рисунке 11.



Рисунок 11 – настройка frame relay

Проверим теперь конфигурацию системы путем отправки Simple PDU. Для этого нужно нажать сверху на конвертик, фото данной кнопки прикрепляю на рисунке 12.

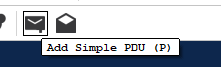


Рисунок 12 – кнопка для тестирования системы

В результате все заработало идеально, результат представлен на рисунке 13.

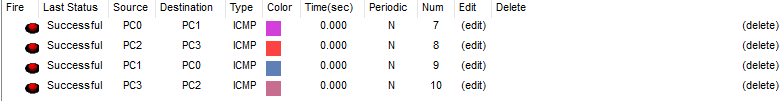


Рисунок 13 – параметры ответа в сети

# **Лабораторная работа №3**

**Тема:** «Знакомство с командами Cisco IOS»

**Цель:** научиться использовать командную строку Cisco Packet Tracer

**Задание 1.** Изучить работу CLI.

Столкнулся с проблемой, что нельзя выйти из настройки интерфейсов, используя команду Interface. Помогает только закрытие файла или простое ожидание. Все представлено на рисунке 1.



Рисунок 1 – попытка настроить интерфейсы

Установку пароля делал, как представлено на рисунке 2. Здесь главное в начале войти в config через команду `conf t`, а потом уже вводить настройки для установки.

Изображение выглядит как текст, снимок экрана, линия, Шрифт

Автоматически созданное описание

Рисунок 2 – установка пароля на роутер

Теперь я проверил, что для входа в привилегированный режим нужно использовать пароль, все работает. Для выхода из данного режима нужно ввести `logout`. Результат проверки находится на рисунке 3.

Изображение выглядит как текст, Шрифт, снимок экрана, дизайн

Автоматически созданное описание

Рисунок 3 – проверка входа в привилегированный режим

C помощью secret поменяли пароль для входа пользователя в привилегированный режим. Для сохранения всех наших операций можем воспользоваться сохранением пароля в память, используя `write memory`.

# **Лабораторная работа №4**

**Тема:** «Работа с сервером в Cisco Packet Tracer»

**Цель:** научиться строить Web серверы

**Задание 1**. Настраиваем WEB сервер.

Для начала проведем настройку сети, строение сети показано на рисунке 1. Здесь все было сделано по методичке. У сервера обязательно нужно включить HTTP во вкладке Services для работы.

Изображение выглядит как снимок экрана, диаграмма, линия

Автоматически созданное описание

Рисунок 1 – строение сети

Теперь напишем нашу HTML страницу для отображения, назвав обязательно “index.html”, теперь с ноутбука запустим Web Browser, чтобы проверить работоспособность. На рисунке 2 представлен результат отображения index.html.

Изображение выглядит как текст, программное обеспечение, Шрифт, веб-страница

Автоматически созданное описание

Рисунок 2 – результат отображения html cтраницы

**Задание 2.** Настройка сетевых сервисов DNS, DHCP и Web

Для начала построить схему, которая представлена на рисунке 3. Здесь мы изначально подключили ПК, выставив параметр DHCP у каждого ПК.

Изображение выглядит как текст, диаграмма, снимок экрана, линия

Автоматически созданное описание

Рисунок 3 – сеть для 2 задания

Зададим статический адрес для серверов, приложу фото как я это сделал. Для всех PC мы зададим DHCP, чтобы был автоматический IP адрес. Теперь начнем работать с DNS в Server1. Результат представлен на рисунке 4.

Изображение выглядит как текст, снимок экрана, дисплей, программное обеспечение

Автоматически созданное описание

Рисунок 4 – связь доменного имени с IP адресом

В начале мы задаем имя домена - `www.yandex.ru`, а также задаем имя хоста, на который мы будем ссылаться `server1.yandex.ru`. А на хост мы должны дать ссылку на адрес `10.0.0.1` (физический адрес cервера).

На Server0 открываем консоль для проверки запроса к нашему домену. Результат представлен на рисунке 5. Команда nslookup служит для определения IP-адреса по доменному имени (и наоборот).

Изображение выглядит как текст, электроника, снимок экрана, программное обеспечение

Автоматически созданное описание

Рисунок 5 – результат обращения к домену

На Server0 мы выставили DHCP, как показано на рисунке 6. Напоминаю, что DHCP нужен для внутреннего распределения IP адресов, чтобы было понятно как с домена идти на хост.

Изображение выглядит как текст, Шрифт, число, линия

Автоматически созданное описание

Рисунок 6 – включение протокола DHCP для Server0

Теперь для PC0 и PC1 сбросим параметры сети, и попросим выдать от сервера данные, чтобы могли взаимодействовать по локальной сети. Теперь через веб браузер мы можем попробовать обратиться к домену, чтобы получить HTML страницу.

Изображение выглядит как текст, снимок экрана, программное обеспечение, дисплей

Автоматически созданное описание

Рисунок 7 – результат запроса к серверу

**Задание 3.** Конфигурирование DHCP сервера на маршрутизаторе.

Построим сеть, как сказано в условии. Результат построения представлен на рисунке 8.

Изображение выглядит как снимок экрана, диаграмма

Автоматически созданное описание

Рисунок 8 – сеть для 2 задания

Зайдем в командную консоль роутера, где мы будет работать по заданию. Для начала создадим пул IP адресов для DHCP cервера с именем TST. Команда, которую я использовал, выглядит так: `ip dhcp pool TST`, далее я оставляю ссылку – IP адрес роутера. Теперь укажем адрес основного шлюза, который будет рассылать в сообщениях DHCP. Теперь мне нужно указать адрес DNS сервера, который находится `dns-server 5.5.5.5`. В конце нам нужно исключить из пула.

Изображение выглядит как текст, снимок экрана, Шрифт, документ

Автоматически созданное описание

Рисунок 9 – команды для настройки роутера

Проверим DHCP с помощью команды `ipconfig /all`.

**Задание 4**. Пример настройки интерфейса маршрутизатора в качестве DHCP клиента.

Для начала построим сеть, как представлено на рисунке 10. После этого мы должны перейти в режим продвинутого пользователя через `enable`, теперь перейдем в настройку в `int fa0/0`, `ip address dhcp`. После этого на PC1 не будет работать DHCP, как представлено на рисунке 11.

После настройки интерфейса роутера на получение настроек по DHCP, DHCP клиент на PC1 перестал получать IP-адрес – IP из диапазона 169.254.x.x/16 назначается автоматически самим ПК при проблемах с

получением адреса по DHCP. Интерфейс роутера IP-адрес так же не получит т.к. в данной подсети нет DHCP серверов.

Изображение выглядит как снимок экрана, дизайн

Автоматически созданное описание

Рисунок 10 – сеть для задания

Видим, что тут на рисунке 11 не пустые поля, что свидетельствует о запасном IP в случае того, если DHCP не заработает.

Изображение выглядит как текст, снимок экрана, дисплей, программное обеспечение

Автоматически созданное описание

Рисунок 12 – настройка PC1

**Задание 5**. DHCP сервис на маршрутизаторе 2811.

Для начала создадим нашу сеть, используя маршрутизатор 2811, сама сеть представлена на рисунке 13. Наша задача настроить так, чтобы ПК подключались с помощью DHCP, для этого в Config мы должны задать настройки для подключения.

Изображение выглядит как линия

Автоматически созданное описание

Рисунок 13 – сеть для задания 5

Далее мы зайдем в роутер, чтобы выставить все возможные IP адреса для настроек. Для начала зайдем в консоль, перейдем в режим продвинутого, вбив команду `enable`. После этого мы можем перейти в настройки, вбив команду `conf t`. Теперь у нас есть возможность зарезервировать адреса, используя команду `ip dhcp excluded-address 192.168.1.1 192.168.1.10`. Таким образом, данные адреса будут только для хостов, DHCP их выдавать устройствам не будет.

Теперь наша задача – создать пул адресов, которые будут выдаваться из нашей сети для подключение внешних устройств по типу ПК.

Изображение выглядит как текст, снимок экрана, Шрифт, линия

Автоматически созданное описание

Рисунок 14 – настройки для сети

Теперь настроим интерфейс для маршрутизатора, как сказано в задании. Все представлено на рисунке 15.

Изображение выглядит как текст, снимок экрана, Шрифт, алгебра

Автоматически созданное описание

Рисунок 15 – настройка роутера

Теперь может получить список выданных роутером адресов. Надо посмотреть на список выданных роутером адресов. Данный список представлен на рисунке 16.

Изображение выглядит как текст, снимок экрана, Шрифт, линия

Автоматически созданное описание

Рисунок 16 – IP адресы, выданные роутером

Итак, мы видим, что протокол DHCP позволяет производить автоматическую настройку сети на всех компьютерах.

# **Лабораторная работа №5**

**Тема:** «Статическая маршрутизация»

**Цель:** научиться работать со статической и динамической маршрутизацией внутри сети

**Задание 1**. Настраиваем связь двух сетей через маршрутизатор

Наша цель – настроить связь двух сетей через маршрутизатор (роутер). Тандем сетей представлен на рисунке 1. Для начала мы должны настроить ПК, связанные свитчем, чтобы они находились в одной подсети.

Изображение выглядит как диаграмма, линия, снимок экрана, График

Автоматически созданное описание

Рисунок 1 – сеть для 1 задания

Наша задача также настроить роутер так, чтобы он выступал в роли шлюза для первой сети на интерфейсе Fa0/0. Настройка роутера представлена на рисунке 2.

Изображение выглядит как текст, чек, Шрифт, алгебра

Автоматически созданное описание

Рисунок 2 – настройка роутера

Теперь настраиваем роутер так, чтобы он со второго порта принимал запросы от второй подсети, настройка в принципе ничем не отличается за исключением того, что нужно прописать адрес другой для шлюза.

Остается проверить только результат настройки, использовав команду `show ip route`. Результат команды представлен на рисунке 3.

Изображение выглядит как текст, снимок экрана, Шрифт, число

Автоматически созданное описание

Рисунок 3 – результат запроса по IP

Проверим теперь, что проходит сигнал на разные подсети, использовав команду ping, результат представлен на рисунке 4.

Изображение выглядит как текст, снимок экрана, документ, Шрифт

Автоматически созданное описание

Рисунок 4 – пинг для двух сетей

Теперь проверим работоспособность сети, сделав запрос к каждому отдельному ПК.

Изображение выглядит как текст, снимок экрана, Шрифт, линия

Автоматически созданное описание

Рисунок 5 – проверка работы первой подсети

Аналогичные действия сделаем и со второй подсетью.

**Задание 2.** Настройка трех сетей с WEB сервером. Понятие маршрута по умолчанию.

Схема у нас будет следующая: два коммутатора 2950–25, два ПК в сети 192.168.10.0 с маской 255.255.255.0. Сервер и компьютер в сети 192.168.20.0 с маской 255.255.255.0. Сеть между маршрутизаторами (марки 1851) 192.168.1.0 с маской 255.255.255.252. Компьютеры из сети 192.168.10.0 должны достучаться к DNS серверу в сети 192.168.20.0. Сеть представлена на рисунке 6.

Изображение выглядит как текст, диаграмма, снимок экрана, линия

Автоматически созданное описание

Рисунок 6 – сеть для 2 задания

Мы будем делать статическую маршрутизацию, поэтому в начале мы настроим роутеры для корректной работы. Зайдем в терминал у Router0, теперь пишем команды, которые представлены на рисунке 7.

Изображение выглядит как текст, Шрифт, снимок экрана, белый

Автоматически созданное описание

Рисунок 7 – настройка первого роутера

То же самое проделаем и для Router1, правда мы воспользуемся в этот раз уже GUI для разнообразия. Результат представлен на рисунке 8.

Изображение выглядит как текст, снимок экрана, дисплей, число

Автоматически созданное описание

Рисунок 8 – настройка Router 1

Теперь настроим fa0/0 у Router 0, чтобы наш роутер стал шлюзом. Настройка представлена на рисунке 9.

Изображение выглядит как текст, снимок экрана, дисплей, число

Автоматически созданное описание

Рисунок 9 – настройка порта Router0 в качестве шлюза

Аналогично настроим порт fa0/1 у Router 1, чтобы он стал шлюзом. Результат представлен на рисунке 10.

Изображение выглядит как текст, снимок экрана, число, дисплей

Автоматически созданное описание

Рисунок 10 – настройка порта Router1 в качестве шлюза

Теперь перейдем к настройке всех ПК в сети, нужно задать им IP адреса, маску подсети и основной шлюз. Настройка шлюза представлена на рисунке 11, все параметры можно выставить в Config с разделом Settings.

Изображение выглядит как текст, снимок экрана, Шрифт, линия

Автоматически созданное описание

Рисунок 11 – настройка шлюза для PC1

Представлю ниже на рисунке 12 параметры – IP Adress, Subnet Mask.

Изображение выглядит как текст, линия, Шрифт, число

Автоматически созданное описание

Рисунок 12 – настройка IP и маски подсети у PC1

Теперь перейдем к настройке сервера и PC3 для дальнейшей работы. Настройки сервера прилагаю ниже на рисунках 13, 14.

Изображение выглядит как текст, Шрифт, линия, снимок экрана

Автоматически созданное описание

Рисунок 13 – настройки fa0/0 для сервера

Изображение выглядит как текст, снимок экрана, дисплей, Шрифт

Автоматически созданное описание

Рисунок 14 – настройки DNS и Default Gateway

Теперь перейдем к настройке маршрутизации на маршрутизаторах. У нас подсеть не возвращает обратно пакеты, поэтому мы должны настроить роутеры. Для этого зайдем в CLI для настройки роутеров. По умолчанию маршрут для Router0 представлена на рисунке 15.

Изображение выглядит как текст, Шрифт, снимок экрана, алгебра

Автоматически созданное описание

Рисунок 15 – настройка Router0

Настройка для Router1 делается аналогичным образом за исключением того, что IP должен быть 192.168.1.1. Запись означает, что все запросы, для которых не прописаны маршруты, R2 отправляет на 192.168.1.1, то есть,

на R1. Теперь если мы пропингуем, то увидим результат, что не все пакеты возвращаются обратно. Результат команды ping представлен на рисунке 16.

Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание

Рисунок 16 – запросы с помощью ping от PC1 к PC2

Чтобы убедиться наверняка, давайте посмотрим, как идут пакеты по узлам сети и для этого воспользуемся командой tracert 192.168.20.20.

**Задание 3**. Сеть на двух маршрутизаторах.

Теперь наша задача настроить сеть так, чтобы она поддерживала статическую маршрутизацию. Сеть для задания представлена на рисунке 17.

Изображение выглядит как текст, диаграмма, снимок экрана, линия

Автоматически созданное описание

Рисунок 17 – сеть для задания 3

Теперь для каждого роутера покажем, что можно пересылать данные в нужные подсети. Для Router 1 покажем, что он может попасть в подсеть “192.168.10.0” с маской “255.255.255.0” c помощью интерфейса “192.168.200.1”. Аналогичным образом сделаем и для Router0. Результат настройки для Router1 представлен на рисунке 18.



Рисунок 18 – настройка подключения для Router1

Теперь таблица для маршрутизации для Router1 выглядит следующим образом, как на рисунке 19.

Изображение выглядит как текст, снимок экрана, Шрифт, линия

Автоматически созданное описание

Рисунок 19 – таблица маршрутизации для Router1

Обязательно нужно добавить шлюз для сети – это IP адрес, на который отсылаются пакеты в случае того, если нужное устройство не найдено было в подсети.

**Задание 4.** Статическая маршрутизация для пяти сетей и роутеров с тремя портами.

Для начала создадим сеть для нашего задания. Она представлена на рисунке 20. На данной схеме имеется пять сетей: 192.168.1.0, 152.20.20.0, 192.168.100.0, 10.10.10.0 и 192.168.2.0. В качестве шлюза по умолчанию у каждого компьютера указан интерфейс маршрутизатора, к которому он подключен. Маска у всех ПК одна – 255.255.255.0. Маска маршрутизаторов для каждого порта своя: Fa0/0 – 255.255.255.0, Fa0/1 – 255.255.0.0, Fa1/0 – 255.255.255.252.

Изображение выглядит как текст, снимок экрана, диаграмма, линия

Автоматически созданное описание

Рисунок 20 – сеть для 4 задания

Теперь мы должны соединить маршрутизаторы между собой, нужно добавить интерфейсную плату NM-1FE-TX. Результат представлен на рисунке 21.

Изображение выглядит как машина, электроника, панель управления, Электронная техника

Автоматически созданное описание

Рисунок 21 – конфигурация Router0

Не все пакеты будут возвращаться обратно, поэтому мы должны настроить путь по умолчанию для возврата, для этого мы пропишем в конфигурации R0 следующие команды, которые представлены на рисунке 21.

Изображение выглядит как текст, Шрифт, снимок экрана, алгебра

Автоматически созданное описание

Рисунок 21 – путь по умолчанию для R0

# **Лабораторная работа №6**

**Тема:** «Динамическая маршрутизация на протоколах RIP и EIGRP»

**Цель:** научится строить сети с динамической маршрутизацией.

**Задание 1**. Настройка протокола RIP версии 2 для сети из шести устройств.

Построим сеть, которую попросят по заданию. Результат представлен на рисунке 1.

Изображение выглядит как текст, снимок экрана, диаграмма, линия

Автоматически созданное описание

Рисунок 1 – настройка сети для задания 1

Перейдем в настройки Router0, чтобы настроить протокол RIP. Последовательность шагов представлена на рисунке 2.

Изображение выглядит как текст, Шрифт, снимок экрана, алгебра

Автоматически созданное описание

Рисунок 2 – параметры для Router0

То же самое мы должны сделать и c Router1. Теперь нужно перейти в Config Router0 и Router1 для проверки наличия параметров. Результат для Router0 представлен на рисунке 3.

Изображение выглядит как текст, снимок экрана, дисплей, число

Автоматически созданное описание

Рисунок 3 – RIP для Router0

**Задание 2.** Конфигурирование протокола RIP версии 2 для сети из четырех устройств.

Для начала построим нашу сеть, которую просят сделать по заданию. Все представлено на рисунке 4.

Изображение выглядит как линия, снимок экрана, График

Автоматически созданное описание

Рисунок 4 – сеть для 2 задания

По условию задания даны IPv4 для 4 устройств и 2 шлюза. Сначала сконфигурируем R0, как требуется в задании. Настройки представлены на рисунке 5.

Изображение выглядит как текст, Шрифт, снимок экрана, алгебра

Автоматически созданное описание

Рисунок 5 – настройки R0

В Config, где находится RIP, добавились следующие поля, которые представлены на рисунке 6.

Изображение выглядит как текст, Шрифт, снимок экрана, белый

Автоматически созданное описание

Рисунок 6 – Config R0

Теперь перейдем к настройке R1, все команды представлены на рисунке 7.

Изображение выглядит как текст, Шрифт, снимок экрана, алгебра

Автоматически созданное описание

Рисунок 7 – настройки R1

Наблюдаем результат, представленный на рисунке 8.

Изображение выглядит как текст, Шрифт, снимок экрана, белый

Автоматически созданное описание

Рисунок 8 – Config R1

Теперь проверим доступность от одного ПК к другому, использовав команду ping. Результат отправки пакетов представлен на рисунке 9.

Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание

Рисунок 9 – результат команды ping

**Задание 3**. Конфигурирование протокола EIGRP.

Протокол EIGRP более прост в реализации и менее требователен к вычислительным ресурсам маршрутизатора, чем протокол OSPF. Также EIGRP имеет более продвинутый алгоритм вычисления метрики. В формуле вычисления метрики есть возможность учитывать загруженность и надежность интерфейсов на пути пакета. Недостатком протокола EIGRP является его ограниченность в его использовании только на

оборудовании компании Cisco.

Построим теперь сеть для 3 задания. Она представлена на рисунке 10.

Изображение выглядит как текст, снимок экрана, диаграмма

Автоматически созданное описание

Рисунок 10 – сеть для 3 задания

Теперь нам нужно настроить параметры протокола для двух роутеров. На рисунке 11 представлена настройка для Router0.

Изображение выглядит как текст, снимок экрана, Шрифт, число

Автоматически созданное описание

Рисунок 11 – настройки для Router0

Для проверки работоспособности сделаем ping c одного ПК на другой. Результат представлен на рисунке 12.

Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание

Рисунок 12 – результат ping

**Задание 4**. Пример конфигурирования протокола OSPF для 4-х устройств. Дана прямая маска 266.266.266.246. Выполните расчет и докажите, что обратная равна 0.0.0.7.

Чтобы рассчитать обратную маску (wildcard mask) из данной прямой маски, нужно использовать следующее правило: каждый байт обратной маски равен 255 минус соответствующий байт прямой маски.

Однако, 266 — это недопустимое значение для байта (максимум — 255).

Получается у нас есть прямая маска 255.255.255.248 (или /29). Вычисляем обратную маску:

- 255 - 255 = 0

- 255 - 255 = 0

- 255 - 255 = 0

- 255 - 248 = 7

Таким образом, обратная маска будет 0.0.0.7. Теперь построим сеть, которую попросили в задании 4. Все представлено на рисунке 13.

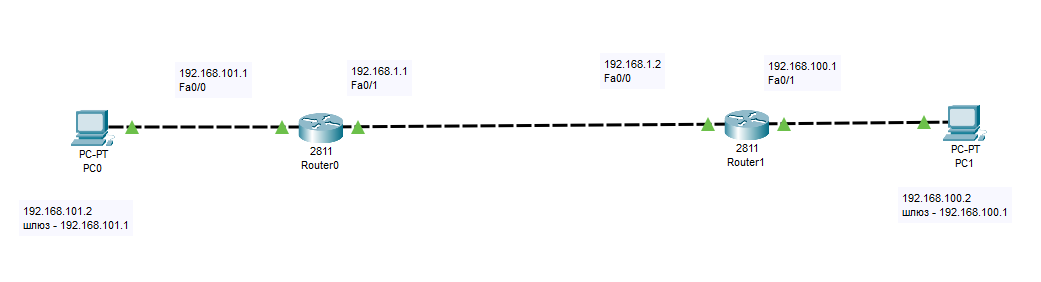


Рисунок 13 – сеть для задания 4

Теперь перейдем к настройке роутеров, чтобы все работало по протоколу OSPF. Для этого нужно выполнить операции, которые представлены ниже на рисунках 14 и 15. Рисунок 14 – это настройка Router0, а рисунок 15 – настройка Router1.

Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание

Рисунок 14 – настройка Router0

Изображение выглядит как текст, снимок экрана, Шрифт, линия

Автоматически созданное описание

Рисунок 15 – настройка для Router1

Теперь остается сделать проверку, что пакеты с одного ПК идут на другой ПК. Результат пинга представлен на рисунке 16.

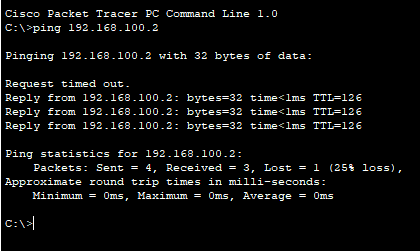


Рисунок 16 – отправка пакетов с PC0 на PC1

**Задание 5**. Настройка маршрутизации по протоколу OSPF для 6 устройств.

Построим для начала сеть для задания 5. Она представлена на рисунке 17.

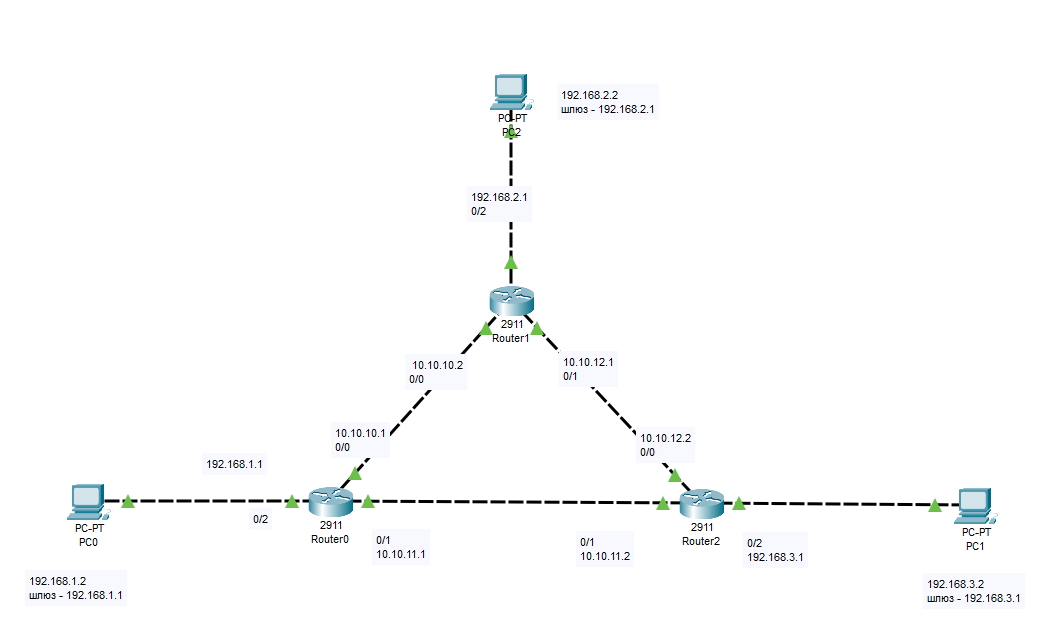


Рисунок 17 – сеть для задания 5

Теперь настроим на R0 настроим программный loopback интерфейс — алгоритм, который направляет полученный сигнал (или данные) обратно отправителю. Все команды представлены ниже на рисунке 18.

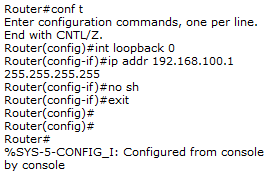


Рисунок 18 – настройка loopback на R0

Можем перейти к настройке OSPF на R0. Включаем OSPF на R0, все маршрутизаторы должны быть в одной зоне area 0. Настройка данного протокола представлена на рисунке 19.

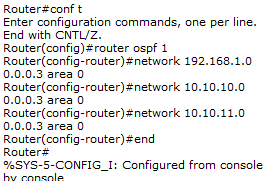


Рисунок 19 – настройка OSPF на Router0

Теперь можем перейти к настройке Router1. Все настройки представлены на рисунке 20.

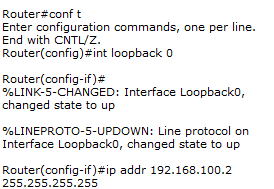


Рисунок 20 – настройка loopback на R1

Настраиваем OSPF на R1: включаем протокол OSPF на R1, все маршрутизаторы должны быть в одной зоне area 0.

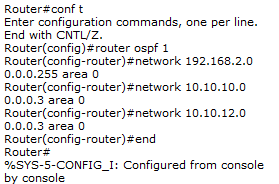


Рисунок 21 – настройка OSPF на R1

Настраиваем loopback интерфейс на R2. Аналогично все делаем, как у прошлых роутеров. Команды представлены на рисунке 22.

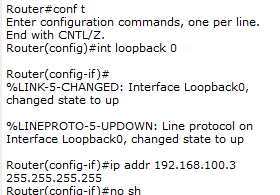


Рисунок 22 – настройка loopback на R2

Убедимся, что Router2 видит Router1 и Router0. Заходим в CLI у Router2. Переходим в режим администратора с помощью команды “en”, а дальше набираем “sh ip ospf neighbor”. Результат представлен на рисунке 23.



Рисунок 23 – результат команды

Теперь выведу таблицу маршрутизации, её можно получить, использовав команду “sh ip route”. Результат представлен на рисунке 24.

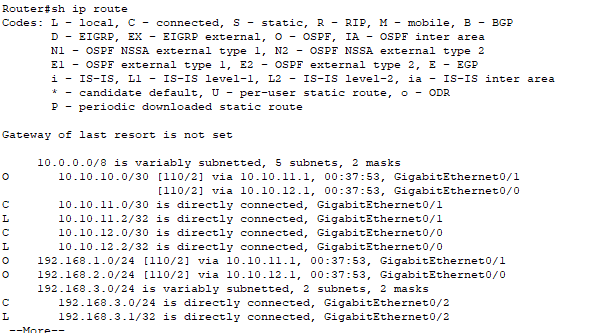


Рисунок 24 – таблица маршрутизации

В этой таблице запись с буквой "О" говорит о том, что данный маршрут прописан протоколом OSPF. Мы видим, что сеть 192.166.1.0 доступна для R2 через адрес 10.10.11.1 (это порт gig0/1 маршрутизатора R0). Аналогично, сеть 192.166.2.0 доступна для R2 через адрес 10.10.12.1 (это порт gig0/1 маршрутизатора R1).

Теперь проверим доступность разных сетей. Для этого зайдем в CLI у Router2 и выполним ping 192.168.1.2, а ещё ping 192.168.2.2. Результат представлен на рисунке 25.

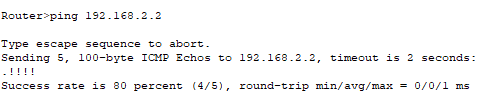


Рисунок 25 – результат запроса на IP 192.168.2.2

# **Лабораторная работа №7**

**Тема:** «Списки доступа ACL. Настройка статического и динамического NAT»

**Цель:** разобраться со списками доступа, научиться динамически и статически настраивать NAT.

**Задание 1.** Создание стандартного списка доступа

Списки доступа бывают нескольких видов: стандартные, расширенные, динамические и другие. В стандартных ACL есть возможность задать только

IP адрес источника пакетов для их запретов или разрешений.

Построим схему, которая требуется в задании. Она представлена на рисунке 1.

Изображение выглядит как текст, снимок экрана, диаграмма, линия

Автоматически созданное описание

Рисунок 1 – схема для 1 задания

Требуется разрешить доступ на сервер PC0 с адресом 172.178.0.12, а PC1 c адресом 172.178.0.11 – запретить. С этой целью для начала настроим роутер R0, все представлено на рисунке 2.

Изображение выглядит как текст, снимок экрана, Шрифт, число

Автоматически созданное описание

Рисунок 2 – настройки роуетра для блокировки IP

Теперь надо настроить сервер, его конфигурация представлена на рисунке 3.

Изображение выглядит как текст, снимок экрана, линия, дисплей

Автоматически созданное описание

Рисунок 3 – настройки сервера

Можно теперь проверить связь ПК из разных сетей. Результат пинга представлен на рисунке 4.

Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание

Рисунок 4 – пинг с разных подсетей

Правило запрета и разрешения доступа будем составлять с использованием стандартных списков доступа (ACL). Пока не задан список доступа на интерфейсе всё разрешено (permit). Но, стоит создать список, сразу действует механизм "Всё, что не разрешено, то запрещено". Поэтому нет необходимости что-то запрещать (deny) – указываем что разрешено, а "остальным – запретить" подразумевается автоматически. По условиям задачи нам нужно на R0 пропустить пакеты с узла 172.178.0.12 на сервер. Сделаем это следующим образом, как представлено на рисунке 5.

Изображение выглядит как текст, снимок экрана, дисплей, Шрифт

Автоматически созданное описание

Рисунок 5 - Создаем на роутере разрешающий ACL

Применяется данное правило на интерфейс в зависимости от направления (PC0 расположен со стороны порта Fa0/0) Эта настройка означает, что список доступа (правило с номером 1) будет действовать на интерфейсе fa0/0 на входящем (in) от PC0 направлении. Применим правило, все представлено на рисунке 6.

Изображение выглядит как текст, снимок экрана, Шрифт, линия

Автоматически созданное описание

Рисунок 6 - Применяем правилу к порту fa0/0

Проверим связь ПК с сервером, а также узел 192.168.0.12, все представлено на рисунке 7.

Изображение выглядит как текст, снимок экрана, программное обеспечение, компьютер

Автоматически созданное описание

Рисунок 7 - Проверка сети

**Задание 2.** Расширенные списки доступа ACL

Соберем схему, которую просят по заданию, она представлена на рисунке 8.

Изображение выглядит как текст, снимок экрана, диаграмма, линия

Автоматически созданное описание

Рисунок 8 – схема сети

Нам необходимо разрешить доступ к FTP серверу 10.0.1.3 для узла 172.178.1.2 и запретить для узла 172.178.1.3, все представлено на рисунке 9.

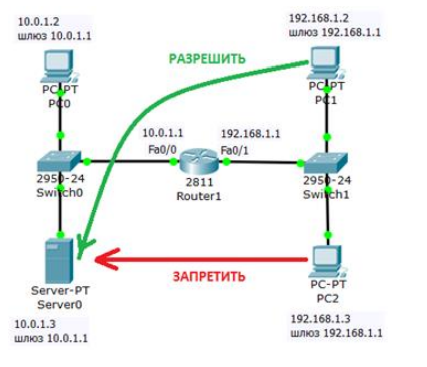


Рисунок 9 - Задание из методички

Изначально на сервере 10.0.1.3 FTP сервис поднят по умолчанию со значениями имя пользователя Cisco, пароль Cisco. Убедимся, что узел S0 доступен и FTP работает, для этого заходим на PC0 и связываемся с сервером. Выполняем какие-либо команды, например, DIR – чтение директории. Результат представлен на рисунке 10.

Изображение выглядит как текст, электроника, снимок экрана, программное обеспечение

Автоматически созданное описание

Рисунок 10 – FTP сервер доступен

Теперь создадим список правил с номером, 101 в котором укажем 2 разрешающих и по 2 запрещающих правила для портов сервера 21 и 20 (Эти порты служат для FTP - передачи команд и данных), все представлено на рисунке 11.

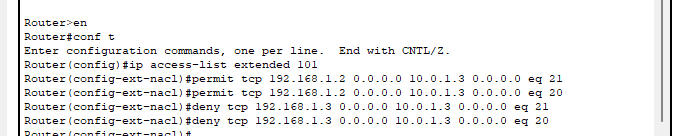


Рисунок 11 - Составляем расширенные списки доступа

А теперь применяем наш список с номером 101 на вход (in) Fa0/1 потому, что трафик входит на этот порт роутера со стороны сети 172.178.1.0, все находится на рисунке 12.

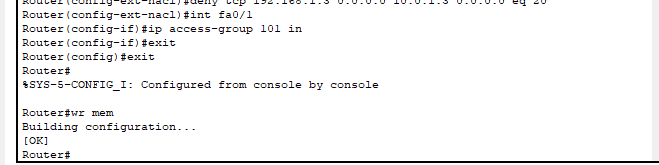


Рисунок 12 - Применяем правило с номером 101 к порту 0/1 роутера

Проверяем связь сервера с PC2, все представлено на рисунке 13.

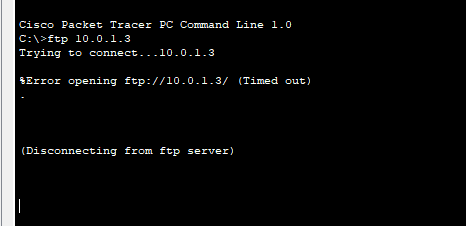


Рисунок 13 - для PC2 сервер не доступен

Проверим связь сервера с PC1, все представлено на рисунке 14.

**Задание 3.** Статическая трансляция адресов NAT.

Построим схему, которую просят по заданию, она представлена на рисунке 14.

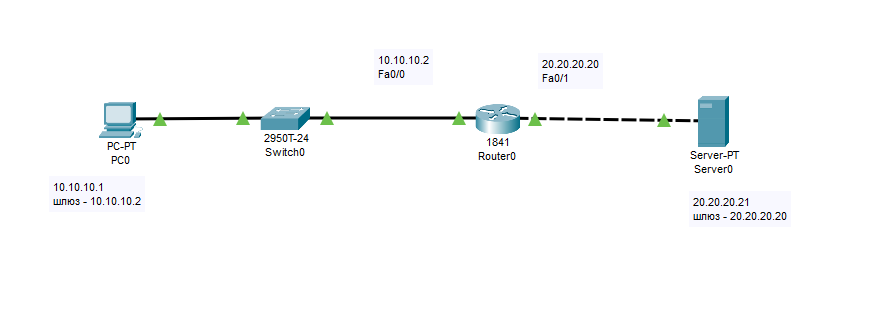


Рисунок 14 – схема сети для задания 3

На роутере добавляем access-list и разрешаем всё. Результат представлен на рисунке 15.

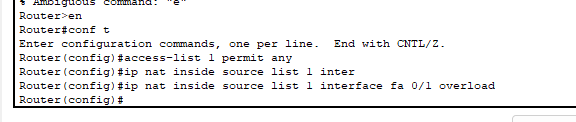


Рисунок 15 – Составляем лист допуска

Далее настроим трансляцию на интерфейсах, все представлено на рисунке 16.

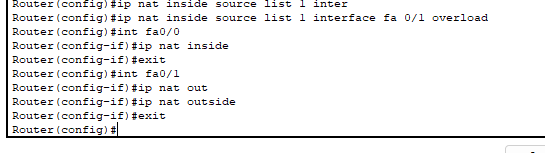


Рисунок 16 - Назначаем внутренний и внешние порты

Выходим из режима глобального конфигурирования и записываем настройки роутера в микросхему памяти (wr mem). Проверим работу сети, использовав команду ping. Результат представлен на рисунке 17.

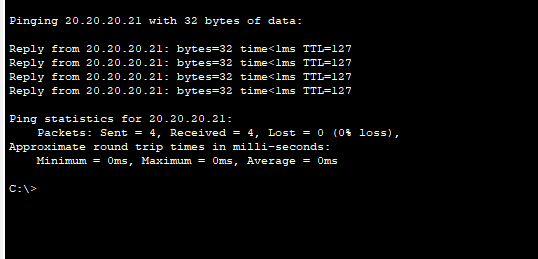


Рисунок 17 – пингуем 20.20.20.21

Для просмотра состояния таблицы NAT, одновременно с пингом нужно использовать команду, перейти заранее в режим конфигурации (“en”). “sh ip nat translations” (я запустил пинг с машины 10.10.10.1, т.е., с PC1 на адрес 20.20.20.21, т.е., на S0). Результат представлен на рисунке 18.

Изображение выглядит как текст, снимок экрана, Шрифт, линия

Автоматически созданное описание

Рисунок 18 – просмотр состояния таблицы NAT

**Задание 4.** Настройка статического NAT.

Построим схему, которая требуется для задания. Сеть представлена на рисунке 19.

**Изображение выглядит как текст, снимок экрана, диаграмма, линия

Автоматически созданное описание**

Рисунок 19 – схема сети для 4 задания

Настроим роутер R1, все команды представлены на рисунке 20.

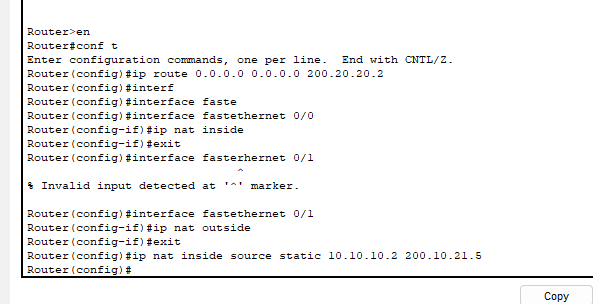


Рисунок 20 – настройка R1

Теперь проверим связь PC0 и R2, использовав команду ping. Результат представлен на рисунке 21.

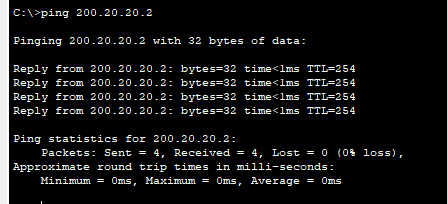


Рисунок 21 – результат пинга

Теперь мы можем проверить, что роутер R1 видит соседние сети, для этого пропингуем сеть “10.10.10.2” и сеть “200.20.20.2”. Результат представлен на рисунке 22.

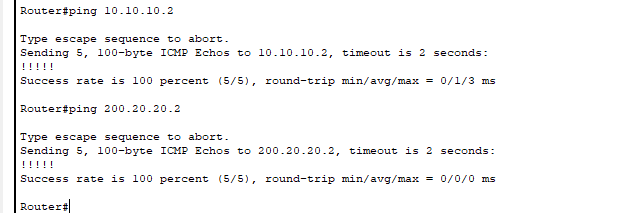


Рисунок 22 – результат пинга

Проверим механизм работы статического NAT. Мы можем воспользоваться командой “show ip nat translations”, которая выводит активные преобразования, а команда “show ip nat statistics” - выводит статистику по NAT преобразованиям. Результат представлен на рисунке 23.

Изображение выглядит как текст, снимок экрана, Шрифт, число

Автоматически созданное описание

Рисунок 23 – вывод активных преобразований и статистики

Из иллюстрации видим, что глобальному ip-адресу 200.10.21.5 соответствует локальный ip-адрес 10.10.10.2, а также, какой интерфейс является внешним, а какой -внутренним.

**Задание 5.** Настройка динамического NAT на маршрутизаторе R1 по шагам.

Динамический NAT – использует пул доступных глобальных (публичных) ip-адресов и назначает их внутренним локальным (частным) адресам. Построим схему, которую просят по заданию. Она представлена на рисунке 24.

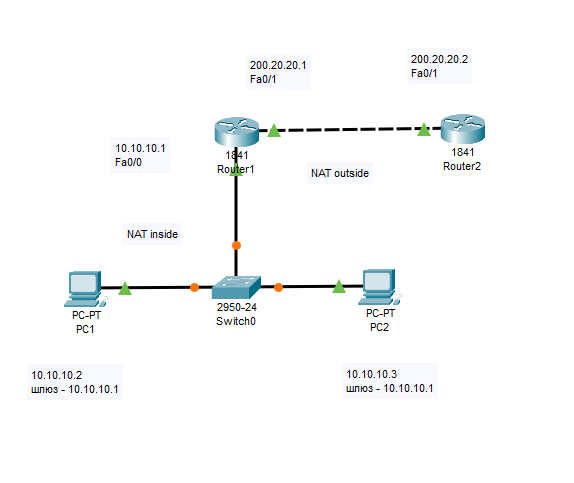


Рисунок 24 – схема сети для 5 задания

Для начала сделаем настройку на R1 списка доступа, соответствующего адресам LAN. Следующая команда – “ip nat pool white-address 200.20.20.1 200.20.20.30 netmask 255.255.255.0” – это настройка пула адресов. Следующая команда “ip nat inside source list 1 pool white-address” – это настройка трансляции. “interface fastethernet 0/0” и “ip nat inside” – это настройка внутреннего интерфейса в отношение NAT. “interface fastethernet 0/1” и “ip nat outside”. Листинг всех команд представлен на рисунке 25.

Изображение выглядит как текст, электроника, снимок экрана, дисплей

Автоматически созданное описание

Рисунок 25 – настройка роутера

Проверим связь между PC1 и R2. Результат пинга представлен на рисунке 26.

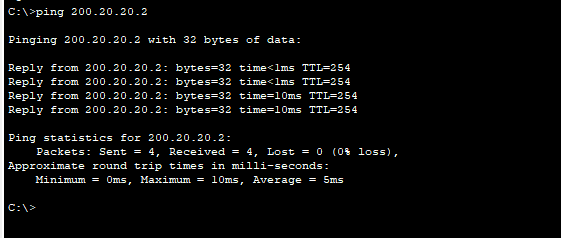


Рисунок 26 – результат пинга с PC1 на R2

Проверим, что R1 видит соседние сети. Результат пинга показан на рисунке 27.

Изображение выглядит как текст, снимок экрана, дисплей, Шрифт

Автоматически созданное описание

Рисунок 27 – проверка соединения R1

Проверим механизм работы динамического NAT: для этого выполним одновременно (параллельно). Для этого используем команды “ping” и “show ip nat translations”. Здесь будут представлены адреса - глобальный, внутренний, внешний. Результат можно увидеть на рисунке 28.

Изображение выглядит как текст, снимок экрана, Шрифт, линия

Автоматически созданное описание

Рисунок 28 – таблица NAT

Командой show ip nat statistics выведем статистику по NAT преобразованиям. Результат представлен на рисунке 29.

Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание

Рисунок 29 – статистика по NAT

**Задание 6.** Динамический NAT Overload: настройка PAT (маскарадинг).

PAT (Port Address Translation) - отображает несколько локальных (частных) ip-адресов в глобальный ip-адрес, используя различные порты. Для этого в начале построим схему, которую просят по заданию.

Изображение выглядит как текст, снимок экрана, диаграмма, линия

Автоматически созданное описание

Рисунок 30 – сеть для задания 6

Теперь нам нужно настроить роутер. Нам нужно перейти в режим конфигурации. Для этого нужно вписать команды “en” и “conf t”. Распишу команды поэтапно. Настроим списка доступа, соответствующие внутренним частным адресам. Для этого используем команду “access-list 1 permit 10.10.10.0 0.0.0.255”. Настроим все в роутере R1, все представлено на рисунке 31.

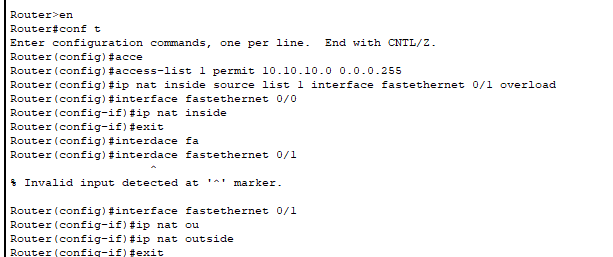


Рисунок 31 – настройка роутера R1

Проверим связь между ПК и роутером 2. Рисунок представлен на рисунке 32.

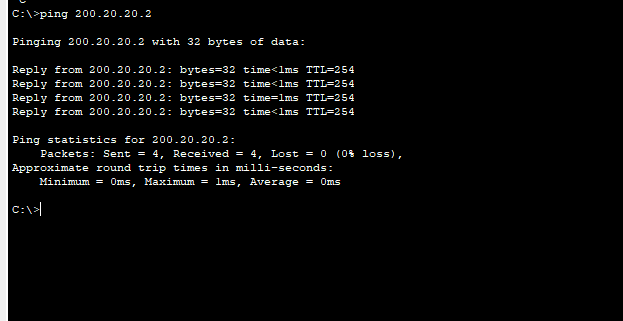


Рисунок 32 – пинг

Проверим, что роутер 1 видит соседние сети. Все представлено на рисунке 33.

Изображение выглядит как текст, снимок экрана, дисплей, Шрифт

Автоматически созданное описание

Рисунок 33 – проверка сети

Проверим механизм работы динамического NAT: для этого выполним одновременно (параллельно) команды “ping” и “show ip nat translations”. Все представлено на рисунке 34.

Изображение выглядит как текст, снимок экрана, Шрифт, дисплей

Автоматически созданное описание

Рисунок 34 – проверка работы NAT

# **Лабораторная работа №8**

**Тема:** “Беспроводная сеть WEP”

**Цель**: “Научиться работать с беспроводной сетью WEP”

**Задание 1.** Беспроводная сеть WEP

Построим схему, которую просят по заданию. Она представлена на рисунке 1.

Изображение выглядит как текст, снимок экрана, диаграмма, дизайн

Автоматически созданное описание

Рисунок 1 – схема сети

Проверим настройку точки доступа и убедимся, что там всё по умолчанию. Результат представлен на рисунке 2.

Изображение выглядит как текст, снимок экрана, программное обеспечение, Значок на компьютере

Автоматически созданное описание

Рисунок 2 – настройка точки доступа

Зададим статическую настройку первого ноутбука, результат представлен на рисунке 3.

Изображение выглядит как текст, снимок экрана, программное обеспечение, Значок на компьютере

Автоматически созданное описание

Рисунок 3 – Конфигурация ноутбука

Далее настраиваем сервера по умолчанию, т.е. оставляем как было. По желанию можно добавить еще устройства. На рисунке 4 видно, что всё настроено

Изображение выглядит как текст, снимок экрана, диаграмма, линия

Автоматически созданное описание

Рисунок 4 – Всё настроено

**Задание 2.** Беспроводная сеть между офисами

Составим схему, она представлена на рисунке 5.

Изображение выглядит как текст, диаграмма, снимок экрана, линия

Автоматически созданное описание

Рисунок 5 – Схема сети

Снабжаем все ноутбуки необходимым модулем для Wireless и настраиваем. Все представлено на рисунке 6.

Изображение выглядит как текст, снимок экрана, программное обеспечение, число

Автоматически созданное описание

Рисунок 6 – Настраиваем Wireless

Также настроим и IP. Настройка представлена на рисунке 7.

Изображение выглядит как текст, снимок экрана, программное обеспечение, Значок на компьютере

Автоматически созданное описание

Рисунок 7 – Настраиваем ноутбуки

Зададим SSID на точках доступа. Все представлено на рисунке 8.

Изображение выглядит как текст, программное обеспечение, Значок на компьютере, снимок экрана

Автоматически созданное описание

Рисунок 8 – Настраиваем точки доступа

Проверяем связь ПК. Связь представлена на рисунке 9.

Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание

Рисунок 9 – Всё настроено

**Задание 3.** Настройка коммутируемого WI-FI соединения

Построим следующую схему, она представлена на рисунке 10.

Изображение выглядит как текст, снимок экрана, диаграмма, дизайн

Автоматически созданное описание

Рисунок 10 – Схема сети

Сначала зададим имя сети (SSID) на точке доступа. Все представлено на рисунке 11.

Изображение выглядит как текст, снимок экрана, программное обеспечение, дисплей

Автоматически созданное описание

Рисунок 11 – Настройка точки доступа

В оба ПК вставляем беспроводной адаптер WPM-300N и устанавливаем связь точки доступа и PC0, для этого нажимаем на кнопку PC Wireless и настраиваем. Настройки роутера представлена на рисунке 12.

Изображение выглядит как текст, снимок экрана, программное обеспечение, веб-страница

Автоматически созданное описание

Рисунок 8.12 – Настройка подключения к точке доступа

На рисунке 13 видно, что всё подключено.

Изображение выглядит как текст, снимок экрана, диаграмма, дизайн

Автоматически созданное описание

Рисунок 13 – Всё подключено

Меняем динамический адрес на статический (рисунок 8.14)

Изображение выглядит как текст, снимок экрана, программное обеспечение, дисплей

Автоматически созданное описание

Рисунок 8.14

Проверяем связь между ПК. Обратите внимание на рисунок 15.

Изображение выглядит как текст, электроника, снимок экрана, программное обеспечение

Автоматически созданное описание

Рисунок 15 – Пинг

**Задание 4.** Беспроводная связь в Packet Tracer с беспроводным роутером

Построим следующую схему, она представлена на рисунке 16.

**Изображение выглядит как текст, снимок экрана, дизайн

Автоматически созданное описание**

Рисунок 8.16 – Схема сети

Снабдим ПК беспроводными модулями и у нас будет наблюдаться появление вай фай сети

Зайдем на роутер и посмотрим на его IP address. Как видим, включен DHCP service и роутер получает IP адрес автоматически. Все представлено на рисунке 17.

Изображение выглядит как текст, снимок экрана, программное обеспечение, дисплей

Автоматически созданное описание

Рисунок 17

Теперь на вкладке Config настроим аутентификацию роутера. Настройка представлена на рисунке 18.

Изображение выглядит как текст, снимок экрана, дисплей, программное обеспечение

Автоматически созданное описание

Рисунок 18 – Конфигурация роутера

Теперь в ПК 0 установим связь с точкой доступа. Все представлено на рисунке 19.

Изображение выглядит как текст, электроника, снимок экрана, программное обеспечение

Автоматически созданное описание

Рисунок 19 – GUI Wireless

Выберем и введем ключ аутентификации (1234567890). Аналогично делаем со вторым ПК. Теперь узнаем IP первого ПК, это представлено на рисунке 20. Теперь пропингуем его со второго. Результат пинга представлен на рисунке 21.

Изображение выглядит как текст, снимок экрана, дисплей, Шрифт

Автоматически созданное описание

Рисунок 20 – Узнаем IP ПК

Изображение выглядит как текст, электроника, снимок экрана, программное обеспечение

Автоматически созданное описание

Рисунок 21 – Пингуем ПК