**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»

**Лабораторная работа № 3**

на тему «Настройка VPN по средствам IPsec протокола»

|  |
| --- |
| Выполнил: студент группы ВКБ43 |
| Ковалев Данил Петрович |
| (Фамилия, имя, отчество) |
| Проверил: доцент |
| Решетникова Ирина Витальевна |
| (Фамилия, имя, отчество) |

# **Цель:** Изучение технологии IPSec и практическая её реализация в организации VPN на имитации реальной сети.

# **Ход работы:**

## **Задание 1.** Построить схему сети, как показано на рисунке 1. Предварительно в оба роутера необходимо добавить модуль NM-4A/S.

Для начала построим схему, как указывается в лабораторной работе. В оба роутера – Router0, Router1 были добавлены NM-4A/S. Схема представлена на рисунке 1.

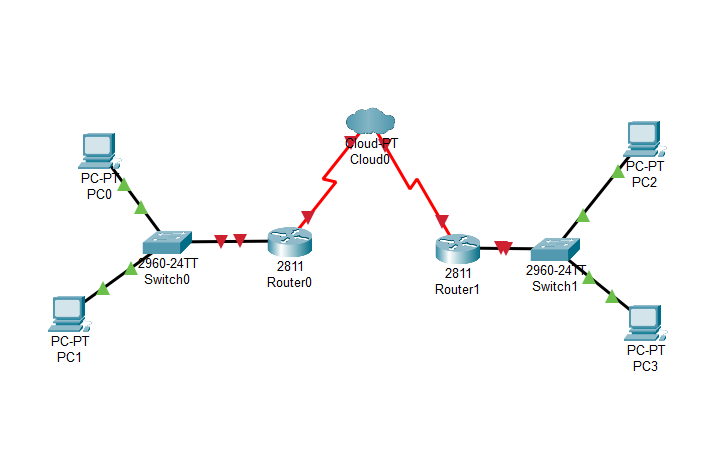


Рисунок 1 - схема сети

**Задание 2.** Настроить IP адреса, маски и шлюз по умолчанию для конечных устройств (лкм по PC, вкладка Desktop -> IP Configuration).

Произведем теперь настройку конечных устройств. Для PC были заданы параметры, как указано было в условии лабораторной работы. Произведем уточнение, что 192.168.1.254 и 192.168.2.154 – это соответственно IP адреса роутера R0 и R1. Результат представлен на рисунке 2.

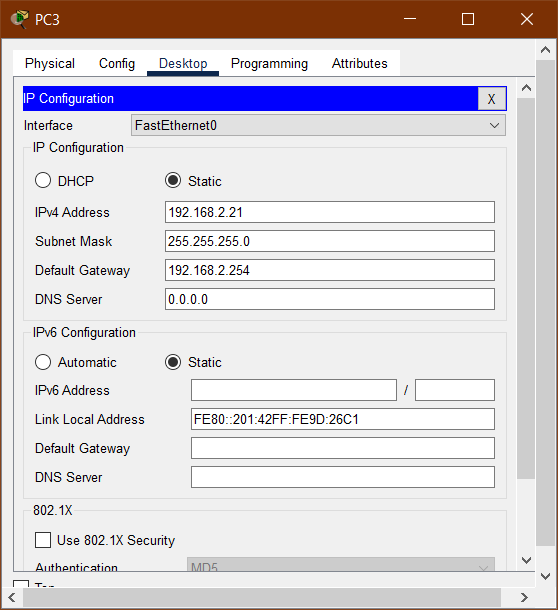
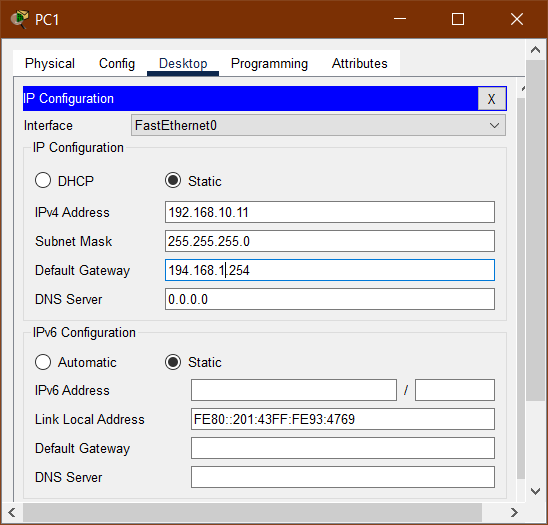
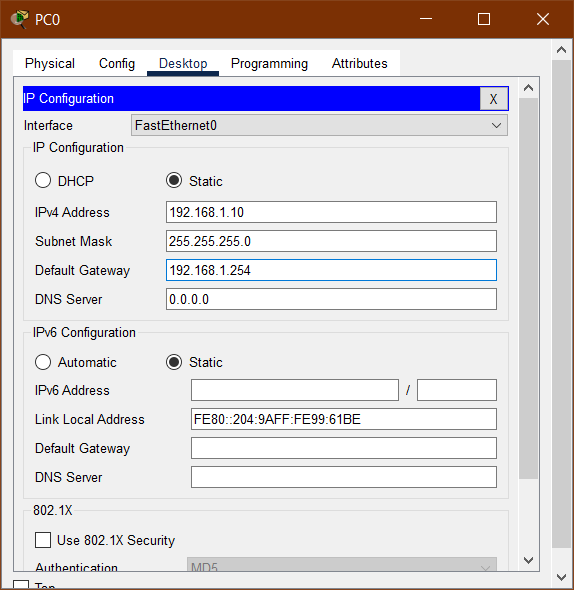
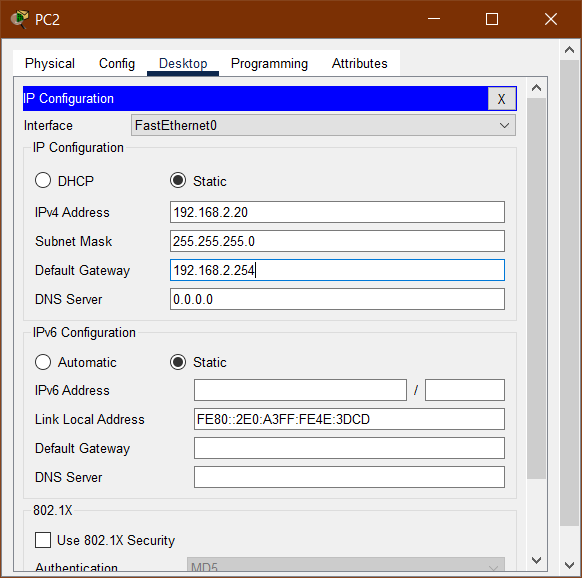


Рисунок 2 - настройка IP конечных узлов

**Задание 3.** Настроить интерфейсы маршрутизатора R0 и R1 соответственно:

Перейдем теперь к настройке интерфейсы маршрутизатора R0 и R1 соответственно. На рисунке 3 представлена настройка R0.

Напомним, что команда “en” нужна, чтобы перейти из пользовательского режима в привилегированный, данный режим нужен для доступа к командам для просмотра состояния системы и, что самое главное, входа в режим конфигурации.

“conf t” – это сокращение от “configure termial”. Данная команда переводит из привилегированного режима EXEC в режим глобальной конфигурации. Это нужно, потому что в режиме глобальной конфигурации можно вносить изменения в общую конфигурацию устройства (имя, пароли, маршруты) и переходить в режимы конфигурации конкретных интерфейсов.

“int fa0/0” – это сокращение от “interface fastethernet 0/0”. Данная команда переводит роутер в режим конфигурации интерфейса для “fastethernet 0/0”.

“ip address 192.168.1.254 255.255.255.0” – данная команда назначает интерфейсу “fastethernet 0/0” IP-адрес “192.168.1.254” и маску подсети “255.255.255.0” (эквивалентно нотации /24 в нотации CIDR). Напомним, что IP-адрес – это уникальный идентификатор интерфейса в сети. Маска подсети определяет какая часть IP-адреса идентифицирует сеть “192.168.1.”, а какая – конкретное устройство – (.254).

“int Seriall/0” – это команда глобального режима конфигурации, которая переводит роутер в режим конфигурации для последовательного интерфейса “Serial 1/0”. Данная команда в нашем случае используется, чтобы настроить интерфейс для WAN-соединения.

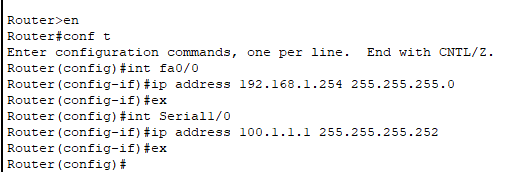


Рисунок 3 - настройка маршрутизатора R0

На рисунке 4 приведена аналогичная настройка, как на R0, но только для R1. Из изменений – это только другие адреса.

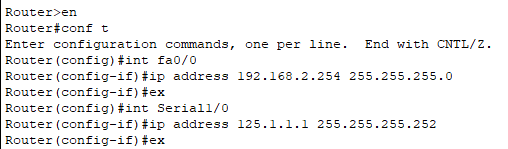


Рисунок 4 - настройка маршрутизатора R1

**Задание 4.** Настроить политику ISAKMP на R0, последовательно указав метод шифрования, аутентификации и обмена секретными ключами, а также время жизни сессии. В конце указать IP адрес конечной точки туннеля, то есть маршрутизатора R1.

Теперь перейдем к настройке политики ISAKMP на R0, последовательно указав метод шифрования, аутентификации и обмена секретными ключами, а также время жизни сессии. В конце нам нужно указать IP адрес конечной точки туннеля, то есть маршрутизатора R1. На рисунке 5 показано выполнение задания.

Напомним, что ISAKP(Internet Security Association and Key Management Protocol) — это протокол уровня приложений, используемый для установления защищённых соединений и управления криптографическими ключами в сетях IP. Он является фундаментальной частью IPSec (набора протоколов для защиты IP-трафика), но не ограничивается только им. Главная задача — безопасно договориться между двумя устройствами (например, роутерами или серверами) о параметрах защищённого соединения и обменяться ключами шифрования. Это включает:

Аутентификацию сторон (проверка "кто есть кто").

Согласование алгоритмов шифрования и хеширования (AES, SHA и т. д.).

Генерацию и обмен сессионными ключами.

Посмотрим теперь за что отвечают разные команды.

“crypto isakmp policy 1” – это создание политики ISAKMP/IKE (Фаза 1) с номером 1. policy 1 – это уникальный номер политики (1-10000). Чем меньше номер, тем выше приоритет при согласовании с удалённым пиром.

“Router(config-isakmp)# encryption 3des” - задание алгоритма шифрования*.* Это нужно для шифрования переговоров фазы 1.

“Router(config-isakmp)# hash md5” – это нужно для обеспечения целостности сообщений фазы 1.

“Router(config-isakmp)# group 1” – это выбор группы Диффи-Хеллмана. Данная операция нужна для безопасного обмена криптографическими ключами.

“Router(config-isakmp)# authentication pre-share” **–** это аутентификация с помощью предварительного общего ключа (PSK). Это нужно, чтобы устройства использовали общий пароль для взаимной проверки.

“Router(config-isakmp)# lifetime 3600” – это время жизни SA. SA – это виртуальное соглашение между двумя устройствами, описывающее какие алгоритмы использовать, ключи для этих алгоритмов.

“Router(config-isakmp)# crypto isakmp key PASS address 125.1.1.1” – это настройка PSK-ключа для удаленного пира. “PASS” – это предварительный общий ключ, а “address 125.1.1.1” – это IP-адрес удаленного роутера, с которым будет устанавливаться VPN. Этот ключ должен совпадать с ключом на роутере “125.1.1.1”.

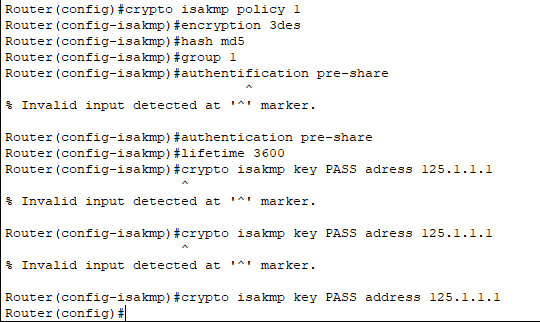


Рисунок 5 - настройка политики ISAKMP на маршрутизаторе R0

**Задание 5.** Аналогично настроить политику ISAKMP на R1.

Теперь произведем аналогичную настройку для R1. Все команды были описаны на шаге 4. Единственная разница, что здесь отличается IP-адрес. Результат представлен на рисунке 6.

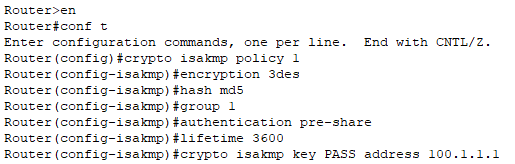


Рисунок 6 - настройка политики ISAKMP на маршрутизаторе R1

**Задание 6.** Настроить параметры туннеля IPSec и создать карту шифрования для R0, привязав её к интерфейсу Serial1/0.

Теперь перейдем к настройке параметров туннеля IPSec и создадим карту шифрования для R0, привязав её к интерфейсу Serial1/0. Рассмотрим команды, представленные на рисунке 7.

“Router(config)#crypto ipsec transform-set MyTS ah-md5-hmac esp-3des” **–** данная команда создаёт набор преобразований (transform-set) для IPSec с именем MyTS. ah-md5-hmac – аутентификация заголовка (AH) c использованием MD5-HMAC. Esp-3des – шифрование esp с использованием 3des. Получается, что данная команда определяет комбинацию протоколов безопасности для защиты данных, где заголовок AH обеспечивает аутентификацию и целостность пакетов, а ESP обеспечивает конфиденциальность (шифрование).

“Router(config)#crypto map CMap10 ipsec-isakmp” – это создание криптографической карты CMap с последовательным номером 10. Ipsec-isakmp указывает, что для установки туннеля будет использоваться “IKE”.

“Router(config-crypto-map)#set peer 125.1.1.1” – это указание адреса удаленного роутера (пира). Роутер будет использовать данный адрес для установки IPSec-туннеля.

“Router(config-crypto-map)#match address 105” – связывание криптографической карты с access-list 105. Данный access-list определяет трафик, который будет защищен “IPSec”. Данный access-list мы настроим в шаге 8.

“Router(config-crypto-map)#set transform-set MyTS” - применяет созданный ранее набор преобразований MyTS к этой криптографической карте.

“Router(config-crypto-map)#interface sel/0” – переходит в режим конфигурации интерфейса Serial1/0. Данная команда нужна, чтобы применить криптографическую карту к этому интерфейсу.

“Router (config-if)#crypto map CMap” – это применение cryptomap для данного интерфейса.

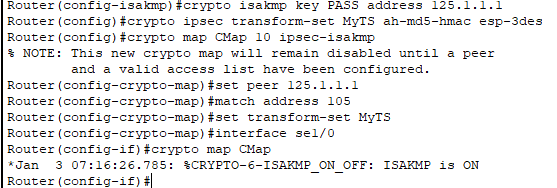


Рисунок 7 - настройка протокола IPSec на маршрутизаторе R0

**Задание 7.** Повторить предыдущий шаг для R1.

Произведем аналогичную настройку для R1, в принципе никакой разницы нет в отличие от R0. Результат представлен на рисунке 8.

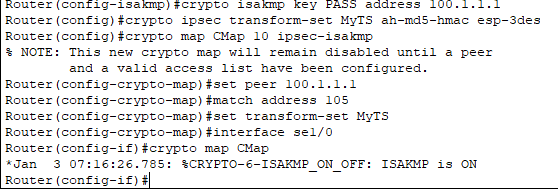


Рисунок 8 - настройка протокола IPSec на маршрутизаторе R1

**Задание 8.** Настроить ACL, где указывается шифруемый траффик, для R0, а также разрешаем протоколы.

Теперь перейдем к настройке ACL, где указывается шифруемый траффик, для R0. На рисунке 9 представлена настройка access-list. Перейдем к объяснению команд.

“ip access-list extended 105” - создаёт расширенный ACL с номером 105. Разница между обычным acl и extended представлена на таблице 1. Этот ACL определяет "интересный трафик", который должен защищаться IPSec. Он привязывается к crypto map (как было в предыдущем фрагменте через match address 105).

|  |  |  |
| --- | --- | --- |
| **Критерий** | **Стандартный ACL** | **Расширенный ACL** |
| **Номера** | 1–99, 1300–1999 | 100–199, 2000–2699 |
| **Фильтрация** | Только исходный IP | Протокол, IP/порты источника и назначения |
| **Гранулярность** | Низкая (“весть трафик с сети X”) | Высокая (“HTTP с ПК1 к серверу 2”) |
| **Место применения** | Ближе к получателю (out) | Ближе к отправителю (in) |

Таблица 1 – сравнение стандартного и расширенного ACL

“permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255” - разрешает IP-трафик между сетями.

“ip access-list extended 110” - создаёт другой расширенный ACL с номером 110. Данный ACL разрешает служебный трафик IPSec (AH/ESP/IKE) через межсетевой экран. В то время, как 105 нужен, чтобы определять какой пользовательский трафик должен шифроваться в VPN.

“permit ahp host 192.168.1.0 host 192.168.2.0” - разрешает трафик протокола AHP (Authentication Header Protocol, IP протокол 51) между адресами 192.168.1.0 и 192.168.2.0.

“permit esp host 192.168.1.0 host 192.168.2.0” – разрешает трафик протокола ESP (Encapsulating Security Payload, IP протокол 50) между адресами 192.168.1.0 и 192.168.2.0.

“permit udp host 192.168.1.0 host 192.168.2.0” – разрешает UDP-траффик.

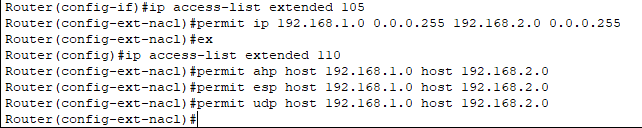


Рисунок 9 - настройка ACL на маршрутизаторе R0

**Задание 9.** Аналогично настроить ACL для R1.

Произведем теперь аналогичную настройку ACL и для R1. Все описанные шаги на рисунке 10 совпадают с описанием на шаге 8.

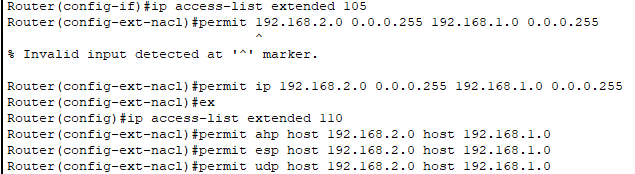


Рисунок 10 - настройка ACL для маршрутизатора R1

**Задание 10.** Настроить маршрутизацию сети и frame-relay для R0.

Теперь перейдем к настройке маршрутизации сети и frame-relay на маршрутизаторе R0. Результат настройки представлен на рисунке 11. Ниже рассмотрим за что отвечает каждая команда.

“Router(config)#ip route 125.1.1.0 255.255.255.252 sel/0” – добавляет статический маршрут к сети 125.1.1.0 через интерфейс Serial1/0. Это мы указываем роутеру, что сеть 125.1.1.0 доступна через этот интерфейс. Здесь ниже система предупреждает, что для многоточечных изменений (multipoint) интерфейсов лучше указать next-hop IP вместо интерфейса.

“Router(config)#ip route 192.168.2.0 255.255.255.0 sel/0” – то же самое, что и в прошлой команде, но только IP другой.

“Router(config)#ip route 192.168.1.0 255.255.255.0 fa0/0” - добавляет маршрут к локальной сети 192.168.1.0/24 через FastEthernet0/0.

“Router(config)#interface sel/0; Router(config-if)#encapsulation frame-relay” – включает инкапсуляцию Frame Relay на интерфейсе. Frame Relay — это протокол WAN, используемый для соединений "точка-точка" или "точка-многоточка".

“Router(config-if)#frame-relay map ip 192.168.2.20 103 broadcast; Router(config-if)#frame-relay map ip 192.168.2.21 104 broadcast; Router(config-if)#frame-relay map ip 125.1.1.1 102 broadcast” – настройка Frame Relay Mapping. Сопоставляет IP-адреса с DLCI (Data Link Connection Identifiers).

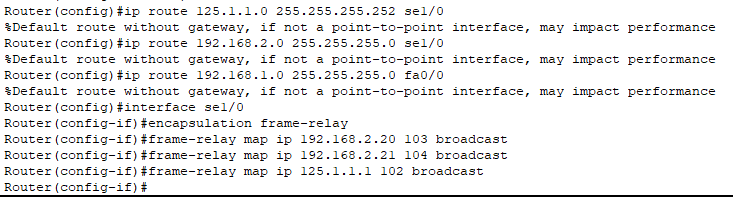


Рисунок 11 - настройка маршрутизации сети и frame-relay на маршрутизаторе R0

**Задание 11.** Повторить предыдущий шаг для R1:

Теперь проделаем те же самые действия, но для роутера R0. Команды ничем не меняются относительно прошлого шага, за исключением того, что другие IP адреса надо указать. Результат выполнения задания представлен на рисунке 12.

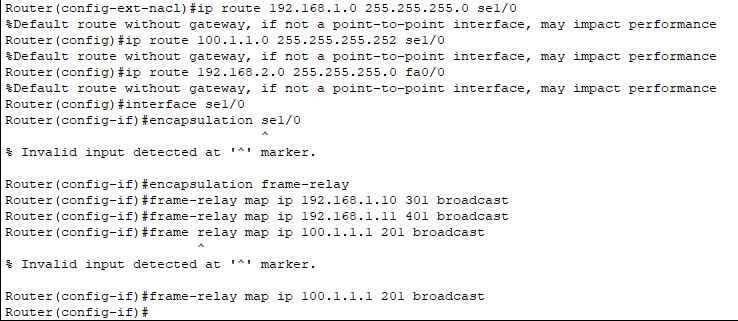


Рисунок 12 - настройка маршрутизации и frame-relay для маршрутизатора R1

**Задание 12.** Для облака настроить интерфейсы Serial0 и Serial1, а также Frame Relay.

Для облака настроить интерфейсы Serial0 и Serial1, а также Frame Relay. DLCI мы создали в прошлых пунктах, остается только задать просто здесь в описании облака. Напомню, что DLCI – это идентификатор соединения канального уровня. Результаты настройки представлены на рисунках 13 и 14.

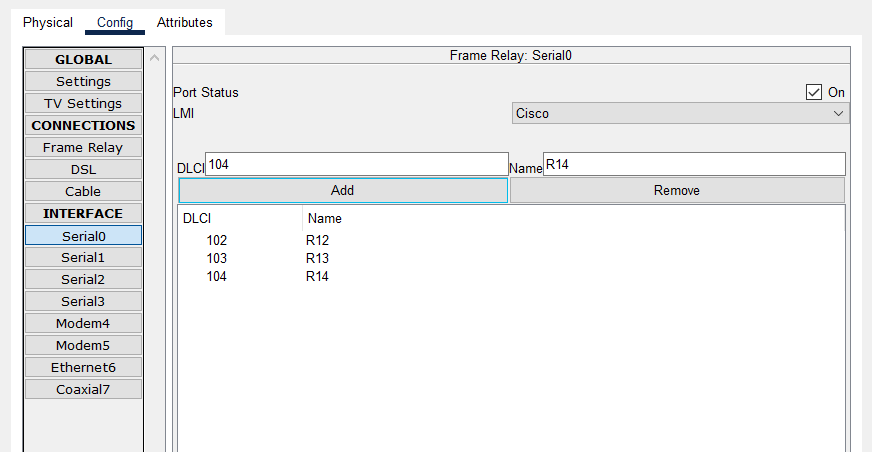


Рисунок 13 – настройка Serial 0

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

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 14 - настройка Serial1

Теперь произведем настройку Frame relay, конфигурация представлена на рисунке 15.

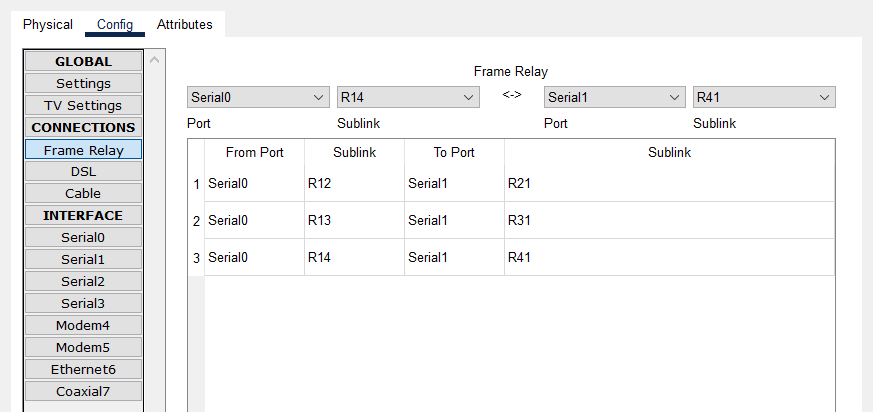


Рисунок 15 - настройка frame-relay

**Задание 13.** Проверить конфигурацию системы путем отправки Simple PDU. При корректной настройке каждое конечное устройство должно быть доступно для любого другого (из-за особенностей Cisco PT при отправке первых двух PDU система производит настройку, вследствие чего может выдавать ошибку передачи).

Теперь проверим, что ICMP пакеты с 1 устройства доходят на другое. На рисунке 16 представлена работоспособность нашей сети.

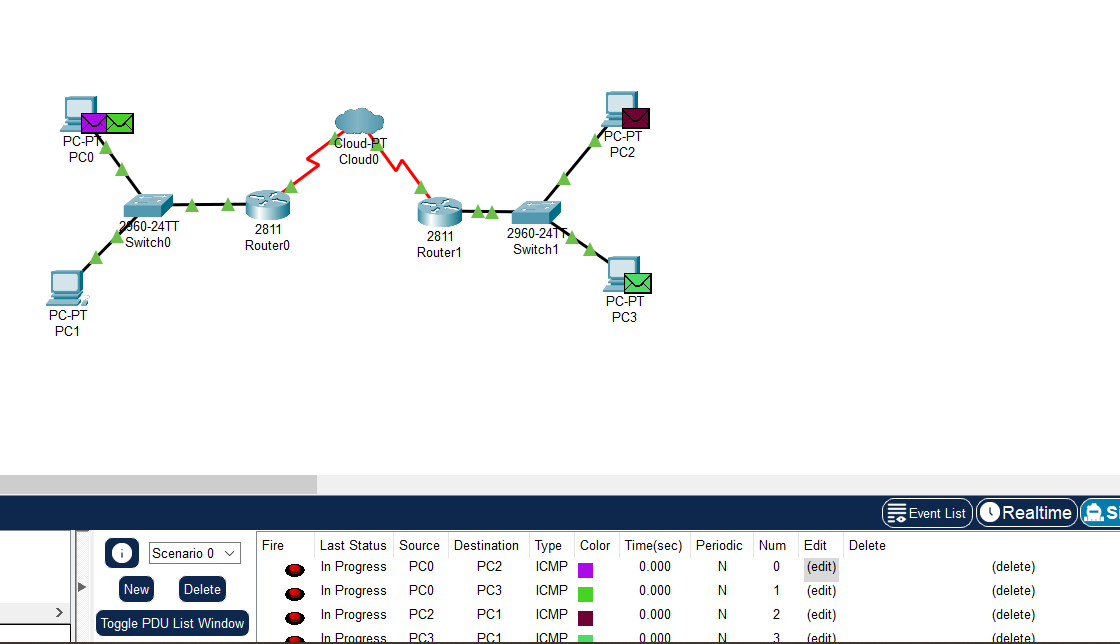


Рисунок 16 - успешная проверка конфигурации настроек

# **Вывод:** В ходе выполнения лабораторной работы были изучены технологии IPSec, а также была выполнена практическая её реализация в организации VPN на имитации реальной сети.

# **Контрольные вопросы**

## **Для чего применяется технология IPsec?**

IPsec (сокращение от 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.

## **Из каких фаз состоит процесс настройки VPN на основе IPsec? Назовите их.**

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.

## **Набор каких параметров определяет политику ISAKMP?**

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

Набор данных параметров определяет политику ISAKMP.

## **Что происходит на второй фазе настройки VPN на основе IPsec?**

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.

## **Каким образом указывается системе на траффик, который необходимо шифровать?**

В IPSec VPN на Cisco роутерах трафик, который необходимо шифровать, определяется с помощью **Access Control List (ACL)** и CryptoMap. ACL связывается с политикой IPSec через криптографическую карту.