

МГТУ им. Н. Э. Баумана
Кафедра «Системы обработки информации и управления»

**Методические указания к лабораторным работам по
дисциплине Сетевые технологии в АСОиУ.**

Лабораторная работа №2.

Настройка DSL.

Для студентов 3-го курса кафедры ИУ5

Разработал: ст. преподаватель

Антонов А. И.

Москва 2024 г.

Содержание

<i>Содержание</i>	2
<i>Цель работы</i>	3
<i>Необходимое оборудования</i>	3
<i>Задание</i>	3
<i>Требования</i>	3
<i>Порядок выполнения лабораторной работы</i>	4
<i>Схема</i>	4
<i>Порядок выполнения лабораторной работы</i>	4
<i>Контрольные вопросы</i>	9

Цель работы

Закрепление теоретических знаний и развитие практических навыков проектирования сетей FrameRelay. Приобретение практических навыков настройки сетей DSL, VPNтуннелей.

Необходимое оборудования

Персональный компьютер, система CiscoPacketTracerверсии не ниже 5.0. (Примеры выполнения работы приведены для версии CiscoPacketTracer8.0.1)

Задание

Три маршрутизатора соединены последовательно по интерфейсу DTE. К маршрутизаторам R1 и R3, не связанным между собой напрямую, подключены локальные сети с количеством компьютеров равным А и В. К третьей сети через облако подключен один локальный компьютер через DSLмодем. Настроить VPNканал между маршрутизаторами R1 и R3. Добиться пересылки пакетов между всеми локальными рабочими станциями. Настроить IPSectуннель между R1 и R3.

Требования

1. IPадреса всех сетей должны содержать номер группы (к примеру: для группы ИУ5-61 ipадрес локальной сети должен выглядеть как 192.161.1.1)
2. IPадреса всех сетей должны содержать номер студента по списку (к примеру: студент группы ИУ5-61 с номером по списку 7 может использовать ipадреса 192.161.7.1, 192.161.57.1, 192.161.107.1 и т.д.)

Порядок выполнения лабораторной работы

Схема

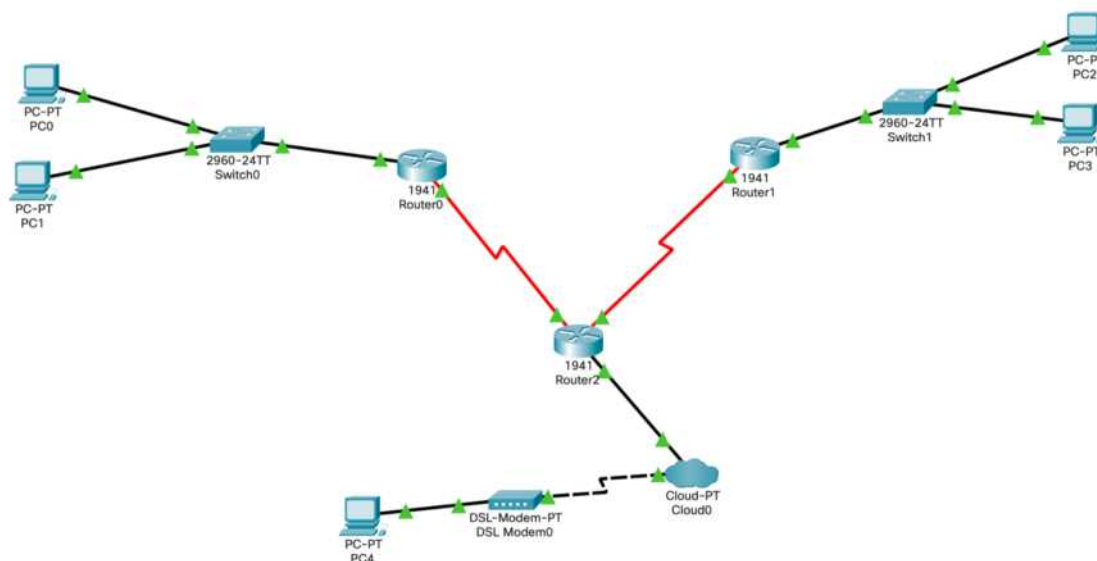


Рисунок 1. Общая схема сети

Порядок выполнения лабораторной работы

1. Собрать схему сети. Обратите внимание, что маршрутизаторы между собой соединены по интерфейсу SerialDTE. Для этого на маршрутизаторах должен быть хотя бы один serialпорт. В случае использования маршрутизаторов, схожих с изображённым на рисунке 1, требуется добавить модуль, содержащий данные порты. Для настройки IPsec рекомендуется использовать маршрутизаторы 4331 (ISR4331).

Добавить модуль можно сделать по следующему алгоритму:

- a. Откройте окно настройки маршрутизатора. Выберите вкладку «Physical»
- b. Выключите маршрутизатор, нажав кнопку питания (см. рисунок 2, выделено красным)
- c. Перетащите модуль, содержащий serialпорты (см. рисунок 2, выделено синим), в свободную ячейку маршрутизатора
- d. Включите маршрутизатор

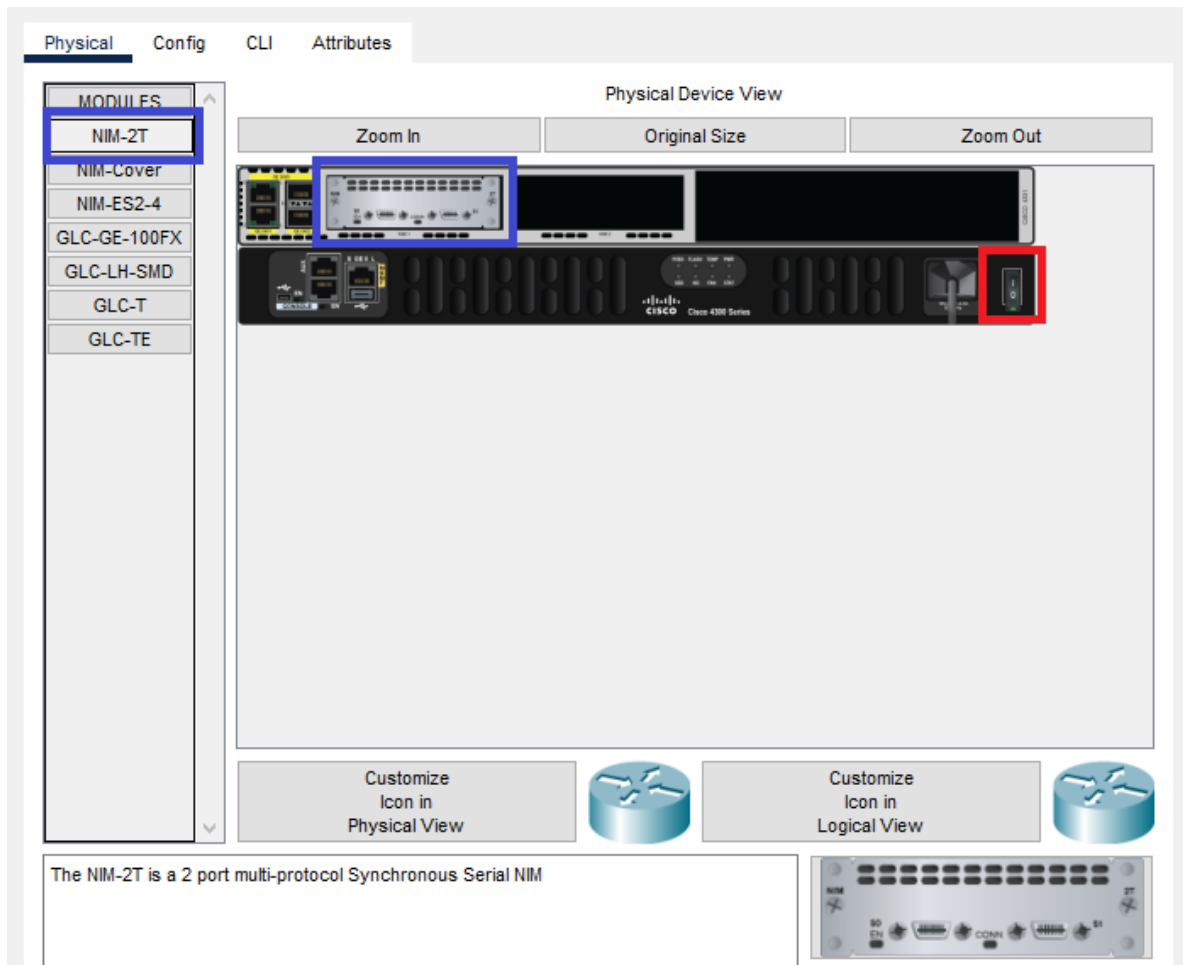


Рисунок 2. Настройка портов маршрутизатора

2. Настройте IP-адреса сети в соответствии с требованиями. Добейтесь пересылки пакетов от рабочих станций до внутренних интерфейсов роутеров.
3. Настройка DSL. Откройте настройки Cloud. Во вкладке «Config», подразделе «Interface», выберите пункт «Modem...». Введите любой номер телефона в поле формы. В подразделе «Connections» выберите пункт меню «DSL». В открывшейся форме добавьте запись Modem <-> Ethernet.
4. Настройте IP-адреса роутера и рабочих станций в сети DSL. Обратите внимание, что они находятся в одной сети, при этом внутренний интерфейс роутера является шлюзом по умолчанию.

5. Настройте статическую маршрутизацию. Добейтесь пересылки пакетов между всеми участниками сети. Выполните операцию `tracert` посмотрите на результат пересылки из сети 1 в сеть 3. Пример результата приведен на рисунке 3. Обратите внимание, что в шагах прохода регистрируется как один из адресов центрального роутера (синяя стрелка), так и внешний адрес роутера сети 3 (оранжевая стрелка).

```
C:\>tracert 192.168.3.2

Tracing route to 192.168.3.2 over a maximum of 30 hops:
  0  0 ms  0 ms  0 ms  192.168.1.1
  1  15 ms  25 ms  20 ms  192.168.10.1
  2  1 ms  28 ms  1 ms  192.168.11.2
  3  38 ms  0 ms  28 ms  192.168.3.2
```

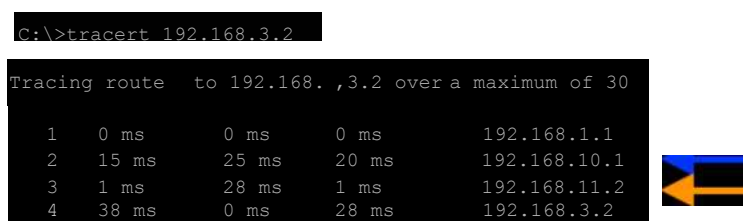


Рисунок 3. Пример вывода команды `tracert`

6. Сохраните схему сети. Далее будет настроен GRE туннель.
7. Настройка туннеля. Откройте настройки роутера R1, перейдите во вкладку «Config», откройте настройки любого интерфейса, а затем перейдите во вкладку «CLI». Здесь введите последовательно команды:
- “exit” - выход из настройки текущего интерфейса
 - “interface tunnel1” - создание нового интерфейса Tunnel1. После выполнения данной команды вы перейдете в режим настройки интерфейса Tunnel1.
 - “ip address <new IPR1>” - установка IP адреса устройства в интерфейсе Tunnel1
 - “tunnel source serial0/1/0” - подключение входного потока к интерфейсу. В данной команде следует подставить свой номер выходного интерфейса
 - “tunnel destination <IPR3>” - установка конечной точки туннеля. Под <IPR3> понимается IP адрес внешнего интерфейса роутера R3.
 - “end” - сохранение и выход из настроек интерфейса
8. Для проверки правильности ввода команд следует навести на роутер мышкой. В описании будут указаны параметры нового интерфейса. Пример приведен на рисунке 4.

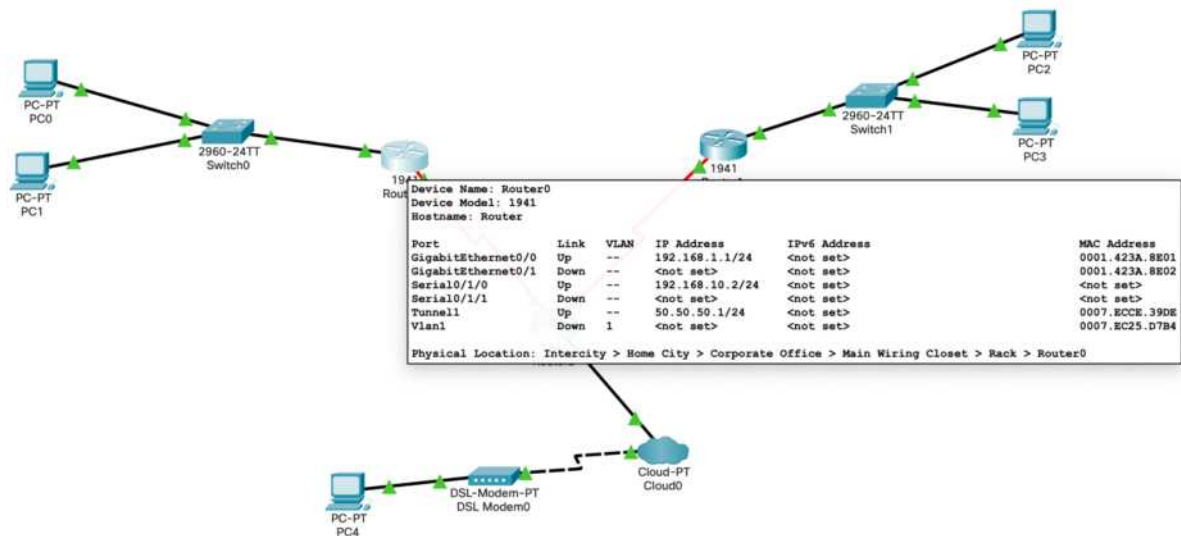


Рисунок 4. Пример описания туннеля

9. Произведите аналогичные п.7 действия для роутера R3.
10. Замените записи в настройках статической маршрутизации роутеров R1 и R3, связанные с пересылкой пакетов между маршрутизаторами R1 и R3. Следует направить пакеты в установленный туннель. Также следует добавить записи для доступа к внешним интерфейсам роутеров R1 и R3. Пример приведен на рисунке 5.

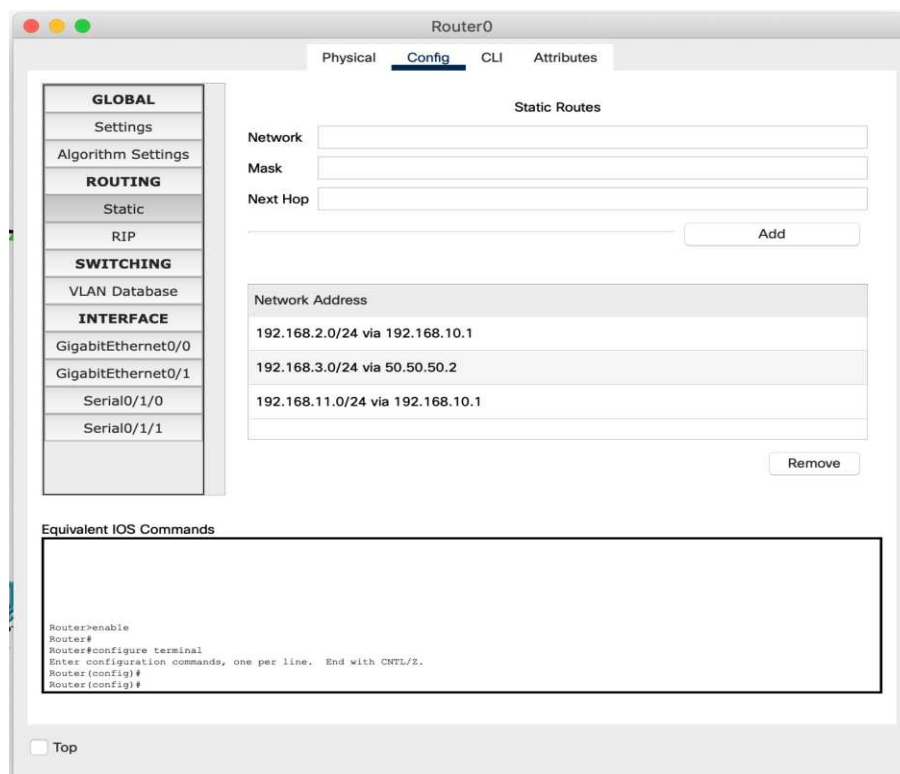


Рисунок 5. Пример итоговой настройки статической маршрутизации роутера R1

11. Проверьте пересылку пакетов между всеми участниками сети. Продемонстрируйте работу туннеля через команду `tracert`. Пример приведен на рис. 6.

```
C:\>tracert 192.168.102.2

Tracing route to 192.168.102.2 over a maximum of 30 hops:

  0  0 ms    0 ms    0 ms    192.168.101.1
  1  19 ms   2 ms    12 ms   10.10.10.2
  2  11 ms   2 ms    2 ms    192.168.102.2
```

Рисунок 6. Пример итогового вывода команды `tracert`

12. Сохраните схему, чтобы вернуться к ней при сдаче ЛР. Откройте схему, где ещё не был настроен туннель GRE.

13. Настроим между 2 сетями туннель IPsec. IPsec позволяет осуществлять аутентификацию, проверку целостности и шифрование IP-пакетов. IPsec также включает в себя протоколы для защищённого обмена ключами в сети Интернет. В основном применяется для организации VPN-соединений. IPsec реализован на сетевом (3-м) уровне модели OSI.

14. Настройте ISAKMP – протокол аутентификации и обмена ключами на обоих роутерах, делается данная настройка с помощью команд:

```
Router(config-if)#crypto isakmp policy 1
Router(config-isakmp)#encr 3des
Router(config-isakmp)#hash md5
Router(config-isakmp)#authentication pre-share
Router(config-isakmp)#group 2
Router(config-isakmp)#lifetime 86400
```

Параметр `group n` в настройке ISAKMP отвечает за длину ключа шифрования.

15. Настройте ACL для криптографического протокола. ACL – Access Control List – позволяет создать список IP-адресов, которым разрешено подключаться к интерфейсу. ACL можно использовать как самостоятельно, например уайт-лист адресов для корпоративной сети – это будет обычный ACL. Для создания разрешений других протоколов создаётся extended ACL.

```
Router(config)#crypto isakmp key merionet address 192.168.202.2
Router(config)#ip access-list extended VPN-TRAFFIC
Router(config-ext-nacl)#permit ip <сеть 1><обратная маска 1><сеть 2><обратная маска 2>
Router(config-ext-nacl)#exit
```

16. Создайте набор трансформаций для протокола IPsec.

```
Router(config)#crypto ipsec transform-set TS esp-3des esp-md5-hmac
```

В данной команде:

TS – название набора

esp-3des – алгоритм шифрования (см. <https://crypt-online.ru/crypts/des/>)

esp-md5-hmac – алгоритм хеширования сообщения

Данные параметры должны совпадать с заданными в настройке ISAKMP.

17. Настройте криптографическую карту для IPsec. Здесь мы соединяем наш набор трансформаций сообщения со списком IP, к которому он применим.

```
Router(config)# crypto map CMAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
and a valid access list have been configured.
Router(config-crypto-map)#set peer <внешнийIP R3>
Router(config-crypto-map)#set transform-set TS
Router(config-crypto-map)#match address VPN-TRAFFIC
Router(config-crypto-map)#end
```

18. Включите криптокарту на интерфейсе:

```
Router(config)#interface Serial0/1/0
Router(config-if)#crypto map CMAP
*Jan 3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
```

19. Проверьте доступность из роутера R1:

```
Router#ping 192.168.102.2
```

Type escape sequence to abort.

```
Sending 5, 100-byte ICMP Echos to 192.168.102.2, timeout is 2 seconds:
.!!!!
```

```
Success rate is 80 percent (4/5), round-trip min/avg/max = 2/11/22 ms
```

Обратите внимание, что первый пинг не прошёл – в это время устанавливался защищённый канал. Обязательно проверьте, что в роутере произошла инкапсуляция IPsec, как на рисунке 7.

PDU Information at Device: Router11

OSI Model | Inbound PDU Details | Outbound PDU Details

At Device: Router11
Source: PC0
Destination: 192.168.102.2

In Layers	Out Layers
Layer7	Layer7
Layer6	Layer6
Layer5	Layer5
Layer4	Layer4
Layer 3: IP Header Src. IP: 192.168.102.2, Dest. IP: 192.168.101.2 ICMP Message Type: 0	Layer 3: IP Header Src. IP: 192.168.202.2, Dest. IP: 192.168.203.2
Layer 2: Ethernet II Header 00E0.F970.4A4C >> 00E0.B01C.9A01	Layer 2: HDLC Frame HDLC
Layer 1: Port GigabitEthernet0/0/0	Layer 1: Port(s): Serial0/1/0

1. The routing table finds a routing entry to the destination IP address.
2. The device decrements the TTL on the packet.
3. The traffic is interesting traffic and needs to be encrypted and encapsulated in IPsec PDUs.
4. The packet is getting encrypted and encapsulated in IPsec PDUs.
5. ESP encrypts the received packet.
6. The device encapsulates the data into an IP packet.
7. The device looks up the destination IP address in the routing table.
8. The routing table finds a routing entry to the destination IP address.
9. An IPSEC (ESP/AH) message is sending out of Serial0/1/0.

Рисунок 7. Инкапсуляция IPsec.

Контрольные вопросы

1. Что такое DSL?
2. Отличие DSLи ADSL.
3. Назначение VPNтуннеля.
4. GRE – способ инкапсулирования и принцип работы.
5. IPSec – способ инкапсулирования и принцип работы.
6. Обеспечит ли безопасность GREтуннель?
7. Обеспечит ли безопасность IPSecтуннель?
8. Настройте туннель GRE между R1 и R3 с включённым IPSec.