| Студент: | Бардадым С.О. | Допуск: |  |
| --- | --- | --- | --- |
| **Отчет по работе №4**  Построение топологии предприятия с филиалом | | | |
| Дата выполнения | 17.05.25 | Дата защиты | 17.05.25 |
| Оценка |  | Подпись |  |

Цель работы: обобщить полученные знания по курсу “Основы телекоммуникационных технологий”, спроектировать и развернуть небольшую корпоративную сеть.

Задачи работы: разработать таблицу адресации для указанной сети. Построить локальную сеть (уровни access и distribution), разбить ее на VLAN, настроить HSRP. Разместить пограничные маршрутизаторы. Подключить их к маршрутизатору ISP, у которого организовать выход в интернет. Настроить между L3 коммутаторами и пограничными маршрутизаторами обмен маршрутами по протоколу динамической маршрутизации (например, OSPF). Настроить на пограничных маршрутизаторах правила nat, позволяющие получить пользователям доступ в интернет. Развернуть оборудование филиала. Настроить IPsec шифрование трафика, идущего по тоннелю между офисом и филиалом. Протестировать отказоустойчивость сети, отключая по очереди различные ее компоненты.

Краткий конспект теоретической части:

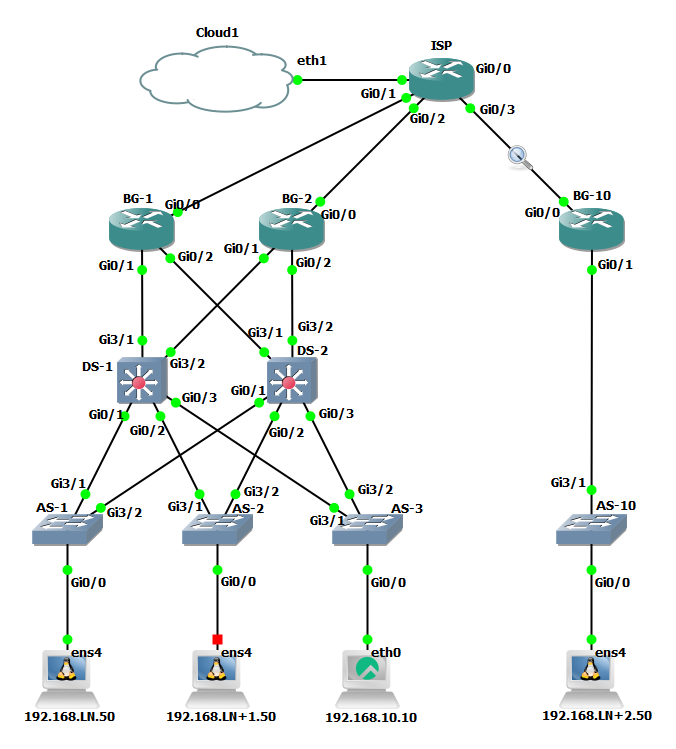
| Комплект документации сети  Комплект документации сети – совокупность технических и организационных документов, описывающих архитектуру, оборудование, схемы подключения, протоколы, правила эксплуатации, политику безопасности и процедуры администрирования компьютерной сети.  ISO 27001 – международный стандарт, определяющий требования к системе управления информационной безопасностью (СУИБ). Он помогает организациям защищать информацию системно и эффективно, основываясь на оценке рисков и мерах контроля.  Принцип пяти девяток  Принцип пяти девяток – концепция обеспечения доступности ИТ-сервисов на уровне 99.999% времени в году, что эквивалентно примерно 5 минутам простоя в год. Часто используется как ориентир при проектировании систем высокой доступности.  Отказоустойчивость и высокая доступность  Свойства ИТ-систем, обеспечивающие непрерывность работы при сбоях или отказах. Отказоустойчивость означает способность системы продолжать работу при выходе из строя её компонентов, а высокая доступность – минимизацию времени простоя благодаря резервированию и восстановлению.  Технологии туннелирования трафика – методы инкапсуляции сетевого трафика одного протокола внутри другого, позволяющие передавать данные через промежуточные сети. Используются, например, для создания VPN-соединений (Virtual Private Network), скрытия реального маршрута и обеспечения безопасности.  IPsec  IPsec (сокращение от IP Security) – набор стандартов для создания защищенных туннелей поверх незащищенных сетей, таких как интернет. Предоставляет возможность аутентификации участников и шифрование трафика. |
| --- |

В этой и следующих работах следует придерживаться простых правил:

- hostname устройств должен содержать фамилию и инициалы студента, если не указано иное,

- вместо LN должен быть подставлен персональный Lucky Number из таблички.

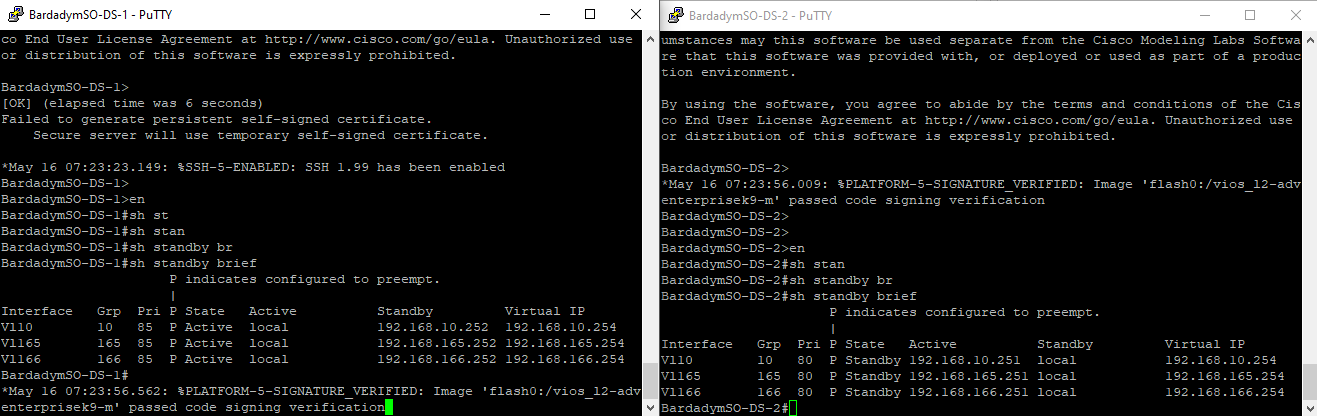
Все результаты следует подтверждать скриншотами, наглядно демонстрирующими описанный в задании функционал.

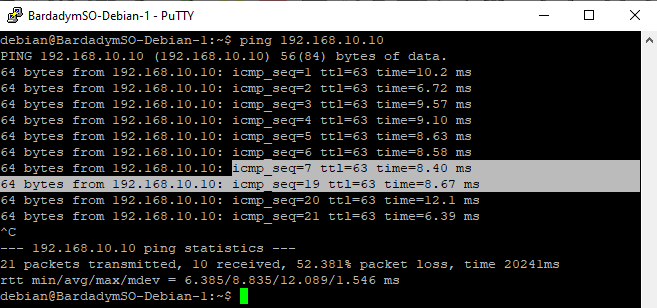


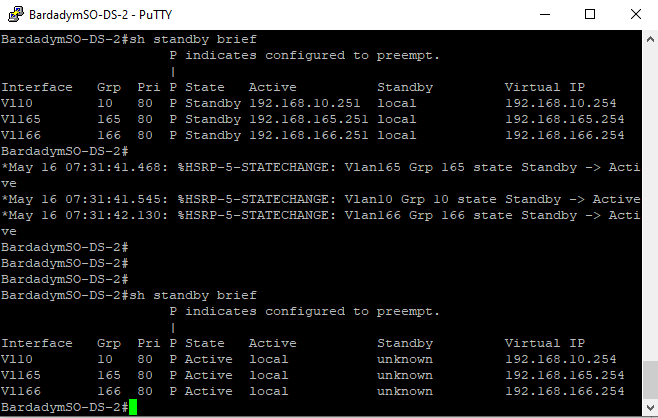
Задание 1. Разработать таблицу адресации для указанной сети. Для внутренних пользовательских сетей следует использовать адреса 192.168.LN.0/24 и 192.168.LN+1.0/24, для адресации пользовательских устройств филиала - 192.168.LN+2.0/24. Для служебных каналов точка-точка между коммутаторами и маршрутизаторами следует 172.18.LN.0/24 разбить на подсети с префиксом /30. Для адресации внутри тоннеля следует 172.19.LN.0/24 разбить на подсети с префиксом /30.

| **Устройство** | **Интерфейс** | **IP-адрес** | **Маска** | **Шлюз по умолчанию** |
| --- | --- | --- | --- | --- |
| **ISP** | Gi0/0 | DHCP | 24 | — |
| Gi0/1 | 1.1.165.2 | 30 | — |
| Gi0/2 | 1.1.165.6 | 30 | — |
| Gi0/3 | 1.1.165.10 | 30 | — |
| **BG1** | Gi0/0 | 1.1.165.1 | 30 | 1.1.165.2 |
| Gi0/1 | 172.18.165.2 | 30 | — |
| Gi0/2 | 172.18.165.6 | 30 | — |
| Tunnel1 | 172.19.165.1 | 30 | — |
| **BG2** | Gi0/0 | 1.1.165.5 | 30 | 1.1.165.6 |
| Gi0/1 | 172.18.165.10 | 30 | — |
| Gig0/2 | 172.18.165.14 | 30 | — |
| Tunnel2 | 172.19.165.5 | 30 | — |
| **BG10** | Gi0/0 | 1.1.165.9 | 30 | 1.1.165.10 |
| Gi0/1.167 | 192.168.167.254 | 24 | — |
| Tunnel1 | 172.19.165.2 | 30 | — |
| Tunnel2 | 172.19.165.6 | 30 | — |
| **DS1** | VLAN 165 | 192.168.165.251 | 24 | — |
| VLAN 166 | 192.168.166.251 | 24 | — |
| VLAN 10 | 192.168.10.251 | 24 | — |
| Gi3/1 | 172.18.165.1 | 30 | — |
| Gi3/2 | 172.18.165.9 | 30 | — |
| **DS2** | VLAN 165 | 192.168.165.252 | 24 | — |
| VLAN 166 | 192.168.166.252 | 24 |  |
| VLAN 10 | 192.168.10.252 | 24 | — |
| Gi3/1 | 172.18.165.5 | 30 | — |
| Gi3/2 | 172.18.165.13 | 30 | — |
| **PC1** | ens4 | 192.168.165.50 | 24 | 192.168.165.254 |
| **PC2** | ens4 | 192.168.166.50 | 24 | 192.168.166.254 |
| **PC3** | eth0 | 192.168.10.10 | 24 | 192.168.10.254 |
| **PC11** | ens4 | 192.168.167.50 | 24 | 192.168.167.254 |

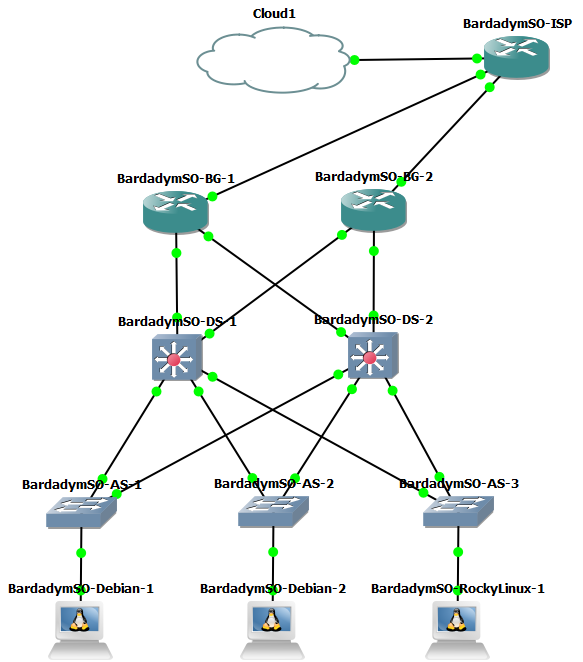
Задание 2. Построить локальную сеть (уровни access и distribution), разбить ее на VLAN, настроить HSRP и проверить отказоустойчивость топологии в случае выхода из строя одного из L3 коммутаторов.

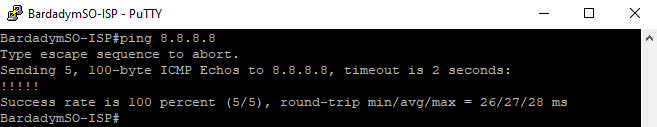


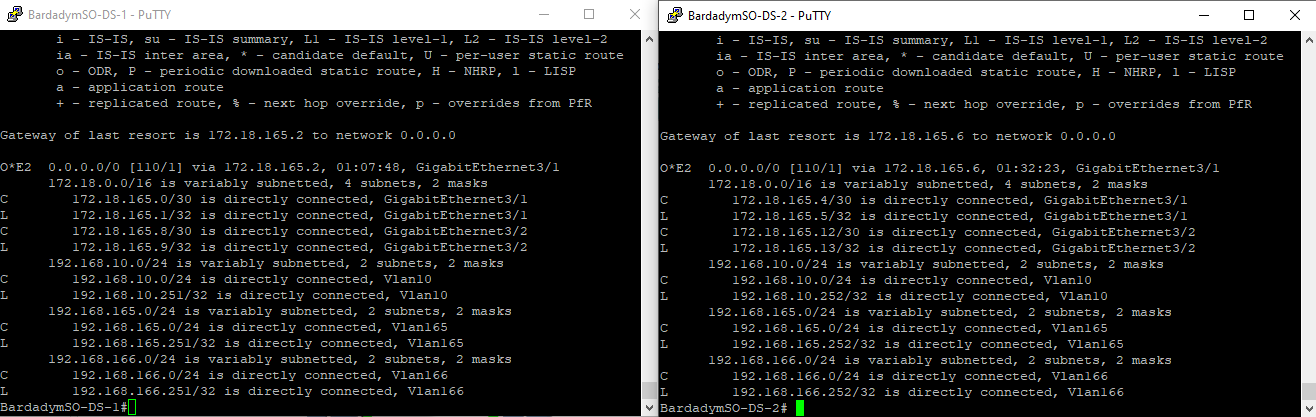


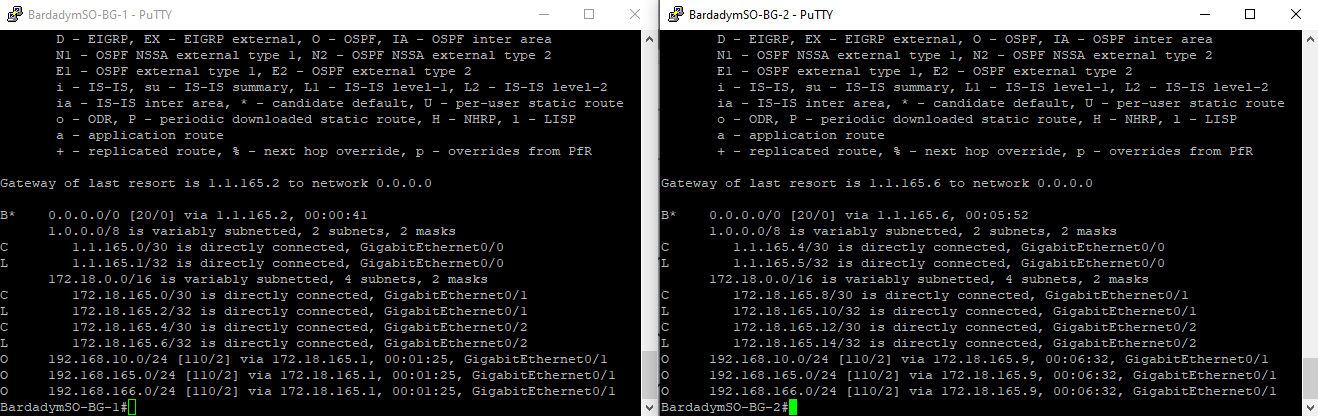


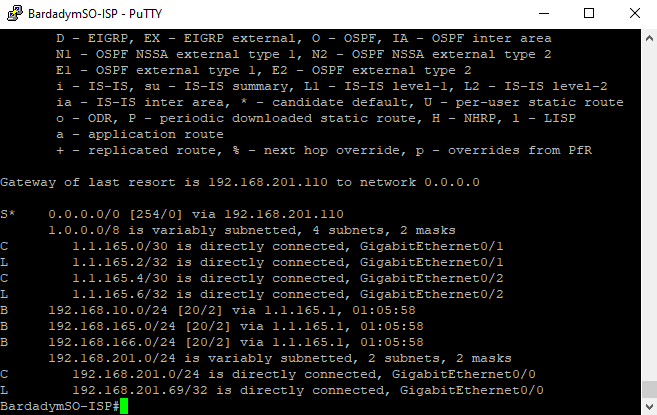
Задание 3. Разместить пограничные маршрутизаторы. Подключить их к маршрутизатору ISP, у которого организовать выход в интернет. Настроить между L3 коммутаторами и пограничными маршрутизаторами обмен маршрутами по протоколу динамической маршрутизации (например, OSPF). Исключить дублирующиеся маршруты в один момент времени, не потеряв при этом возможности резервирования.



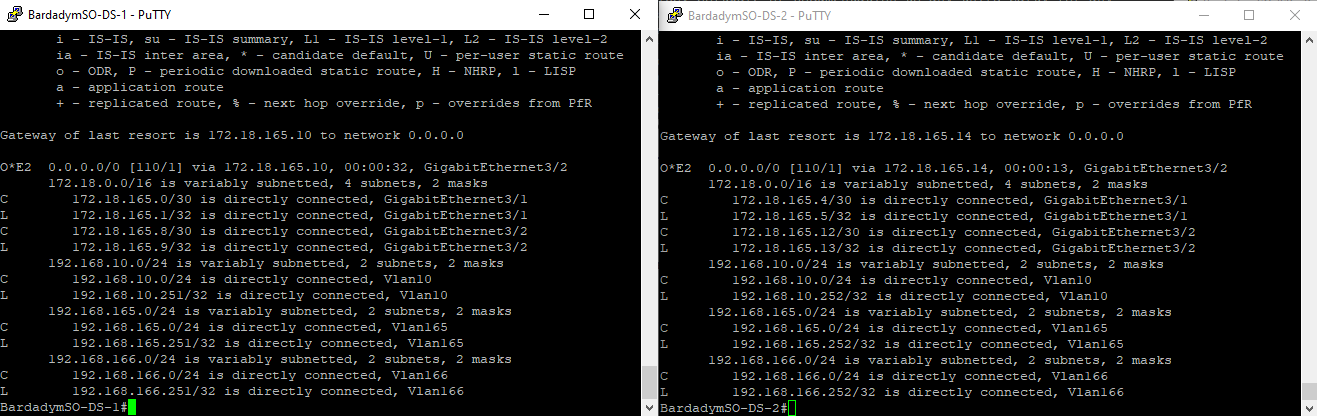


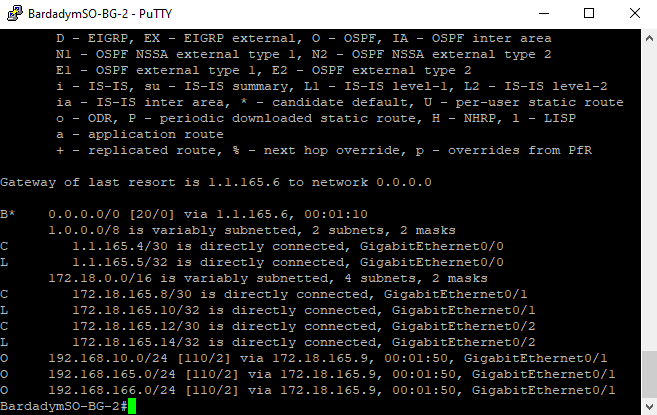


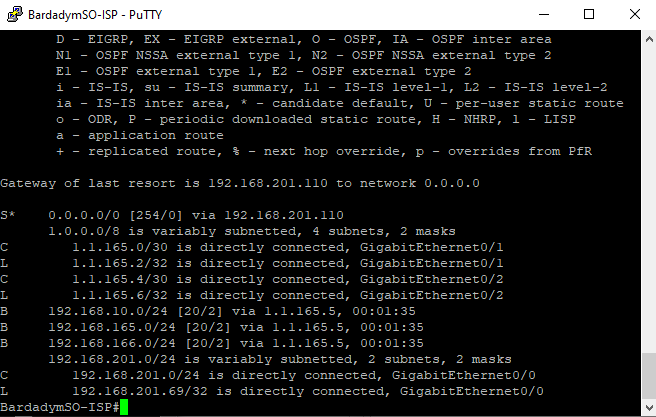




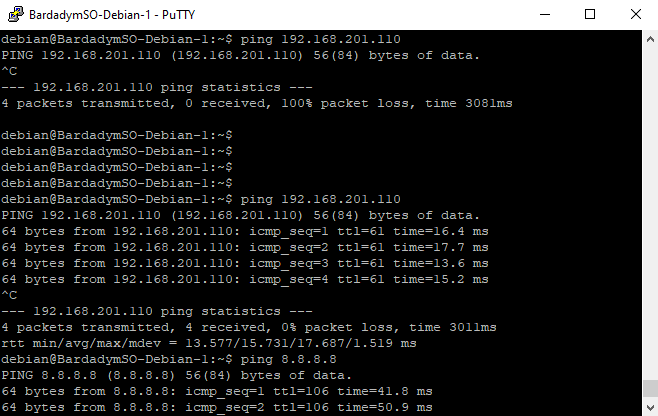
После выключения BG1

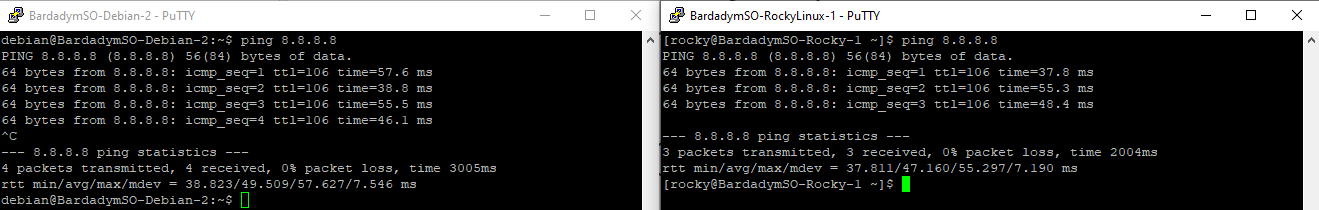




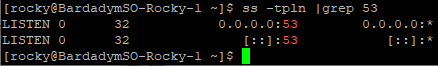


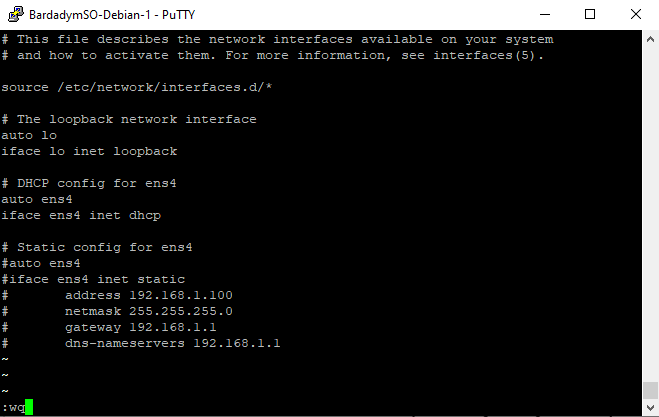
Задание 4. Настроить на пограничных маршрутизаторах правила nat, позволяющие получить пользователям доступ в интернет.

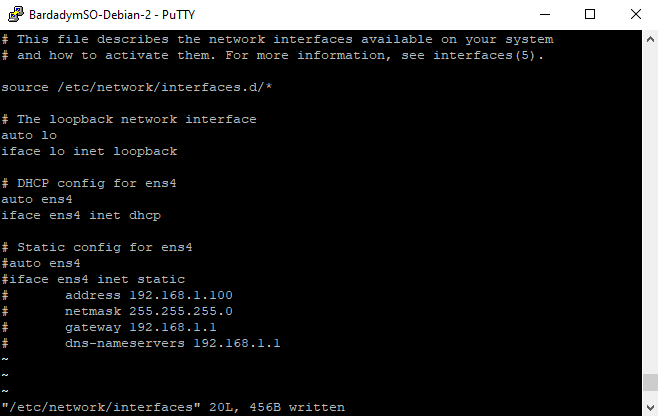


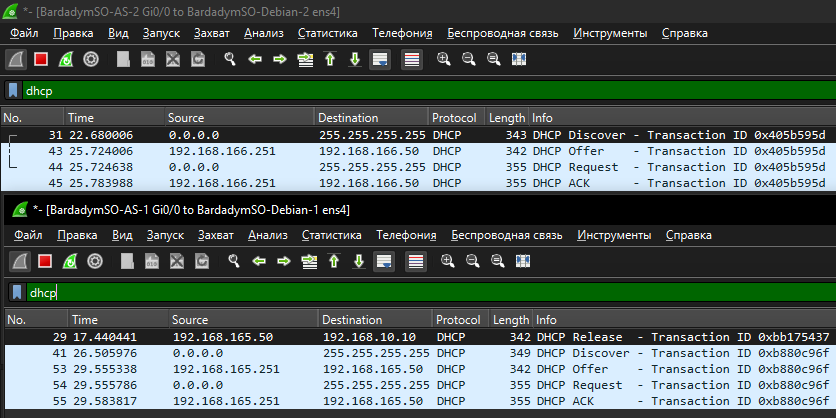


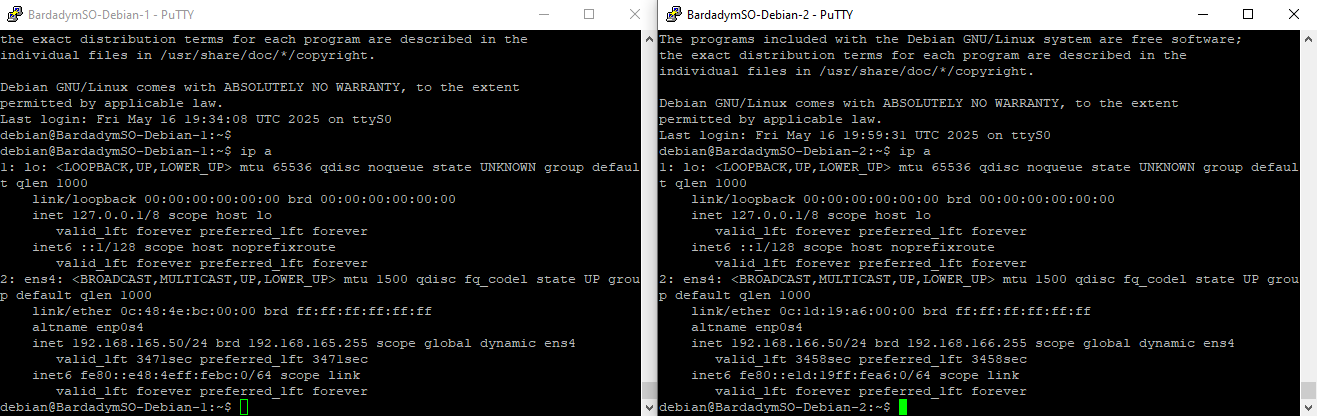
Задание 5. Выделить VLAN 10 под серверную сеть, разместить в нем сервер, на котором настроить сервисы DNS, DHCP, веб-сервер. Настроить пользовательские компьютеры на получение настроек по DHCP.

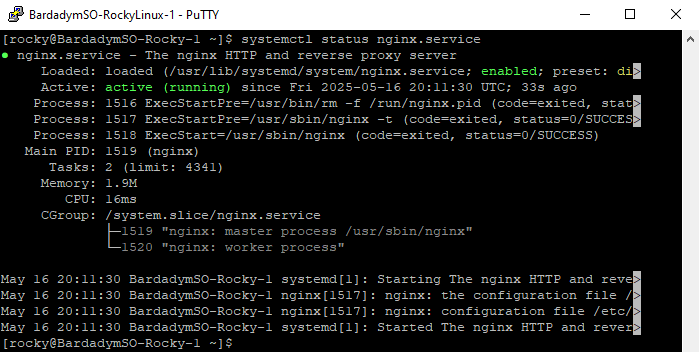






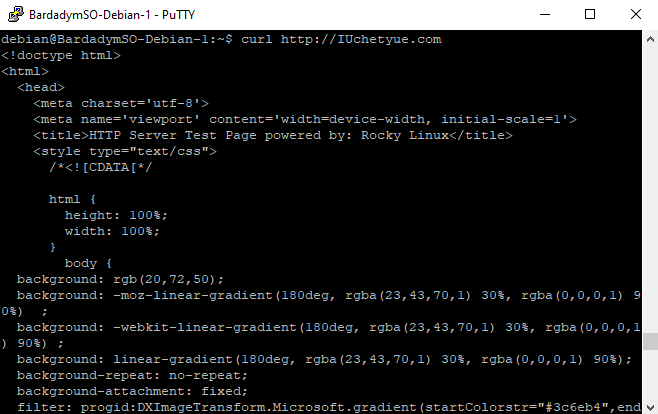




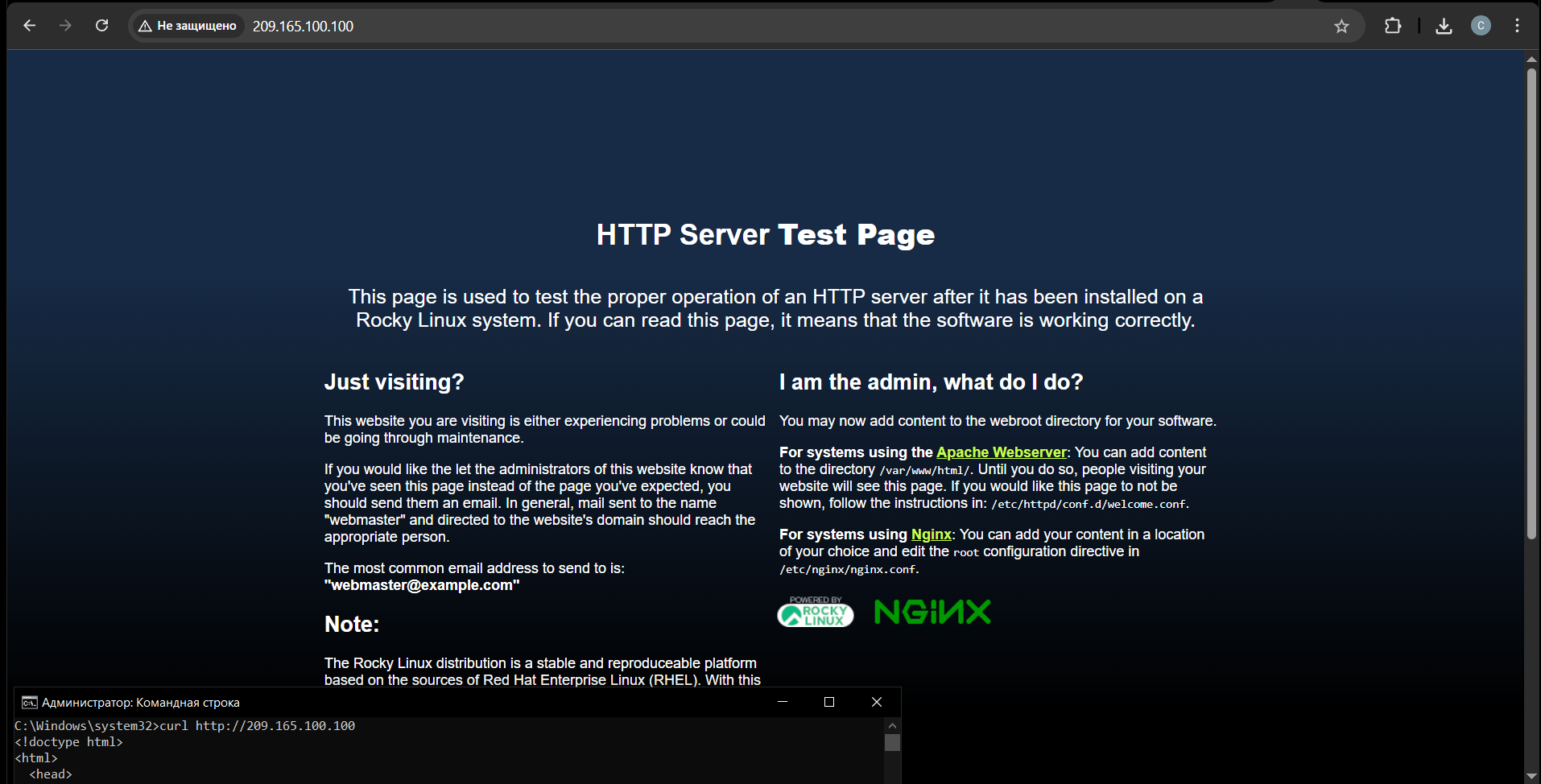


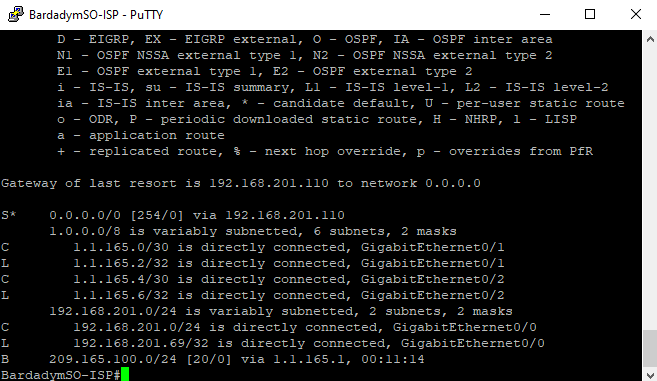


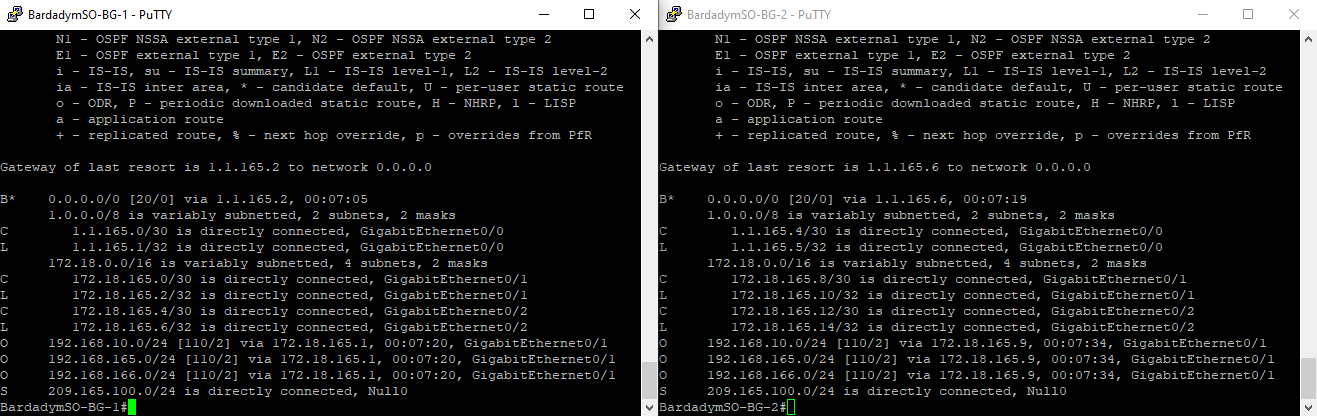




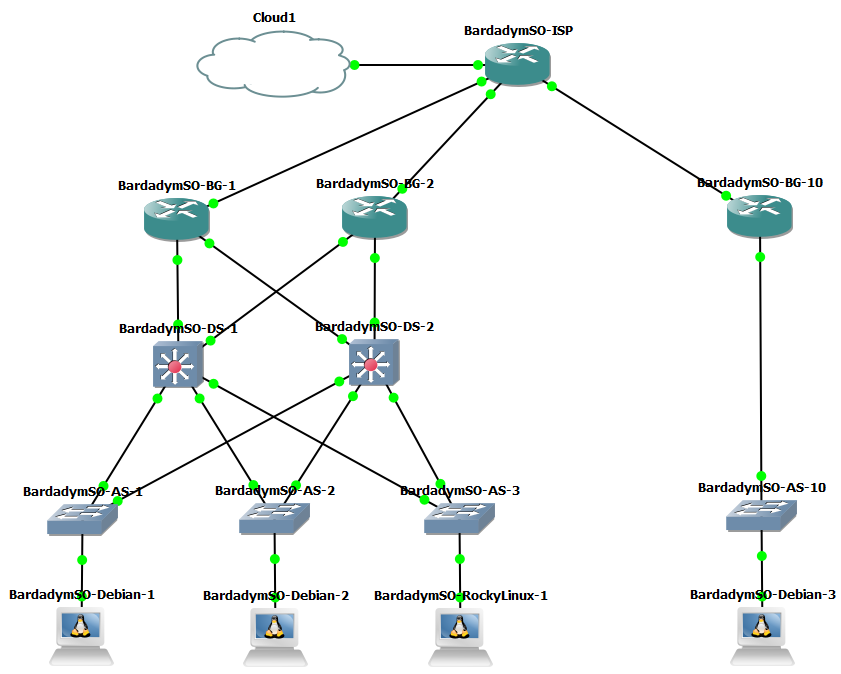
Задание 6. Настроить на пограничных маршрутизаторах правила nat, позволяющие получить с хоста через ISP доступ к развёрнутому сайту.

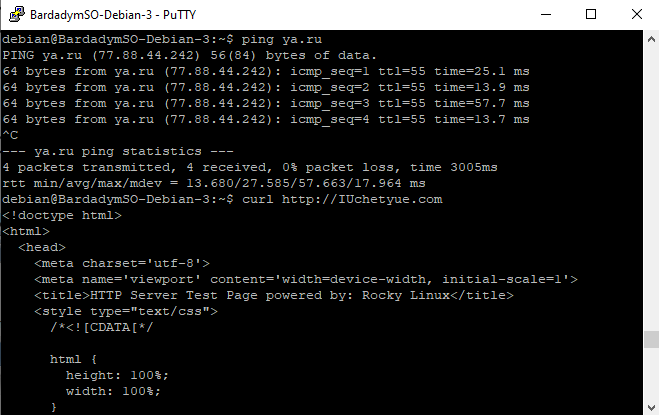


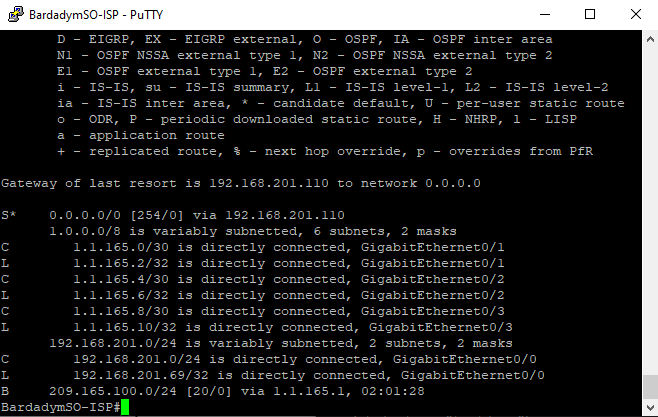


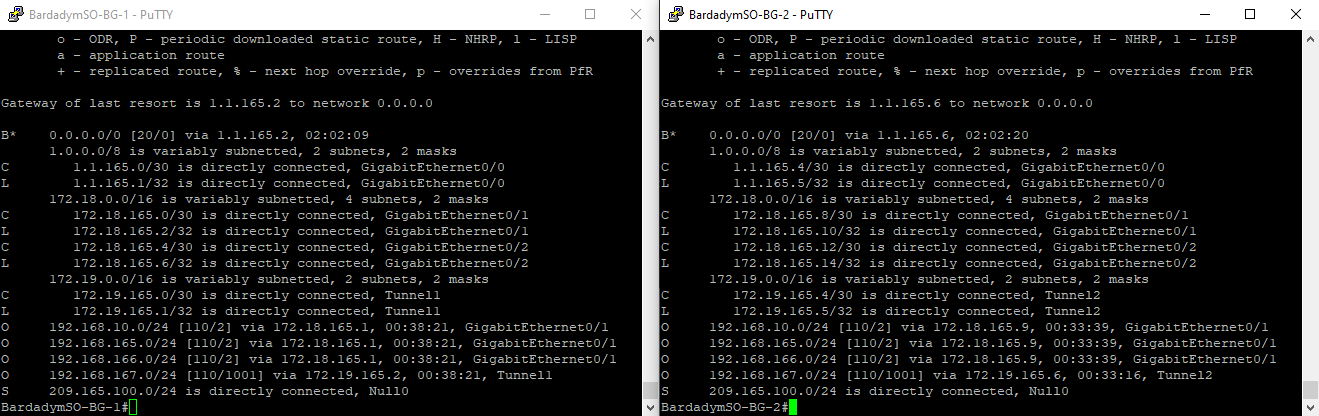


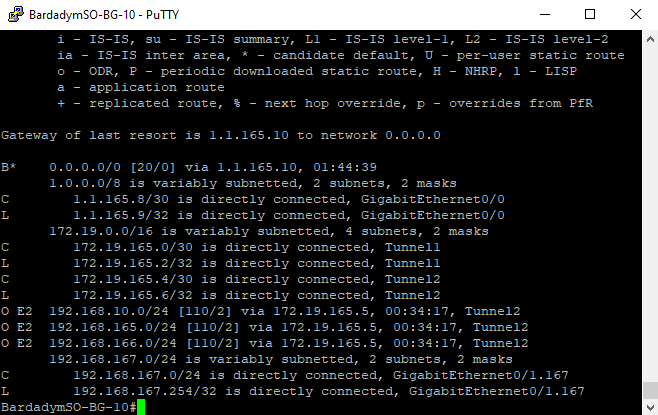
Задание 7. Развернуть оборудование филиала. Настроить доступ в интернет из филиала. Настроить тоннель между филиалом и пограничными маршрутизаторами офиса, поверх которого настроить динамическую маршрутизацию. Добиться доступности ресурсов офиса из филиала.

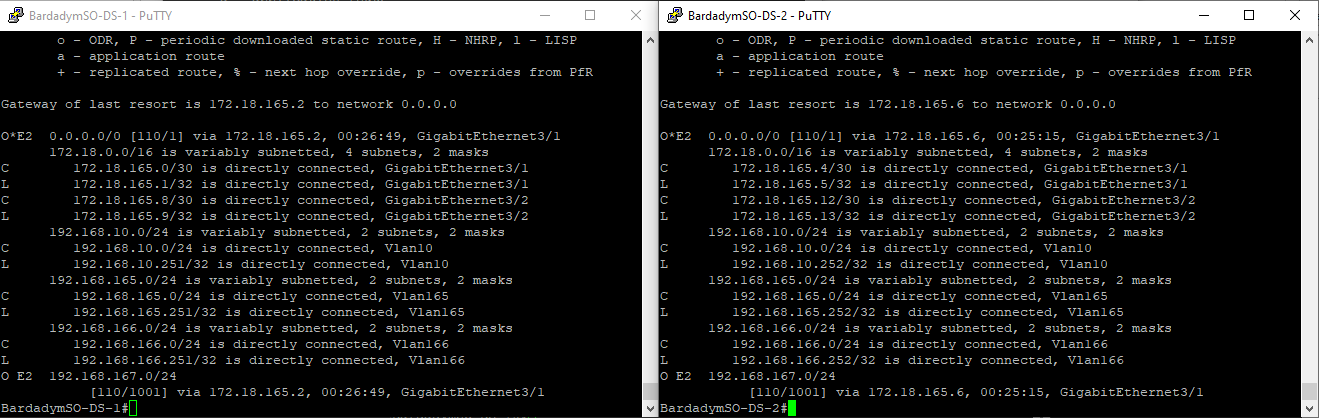




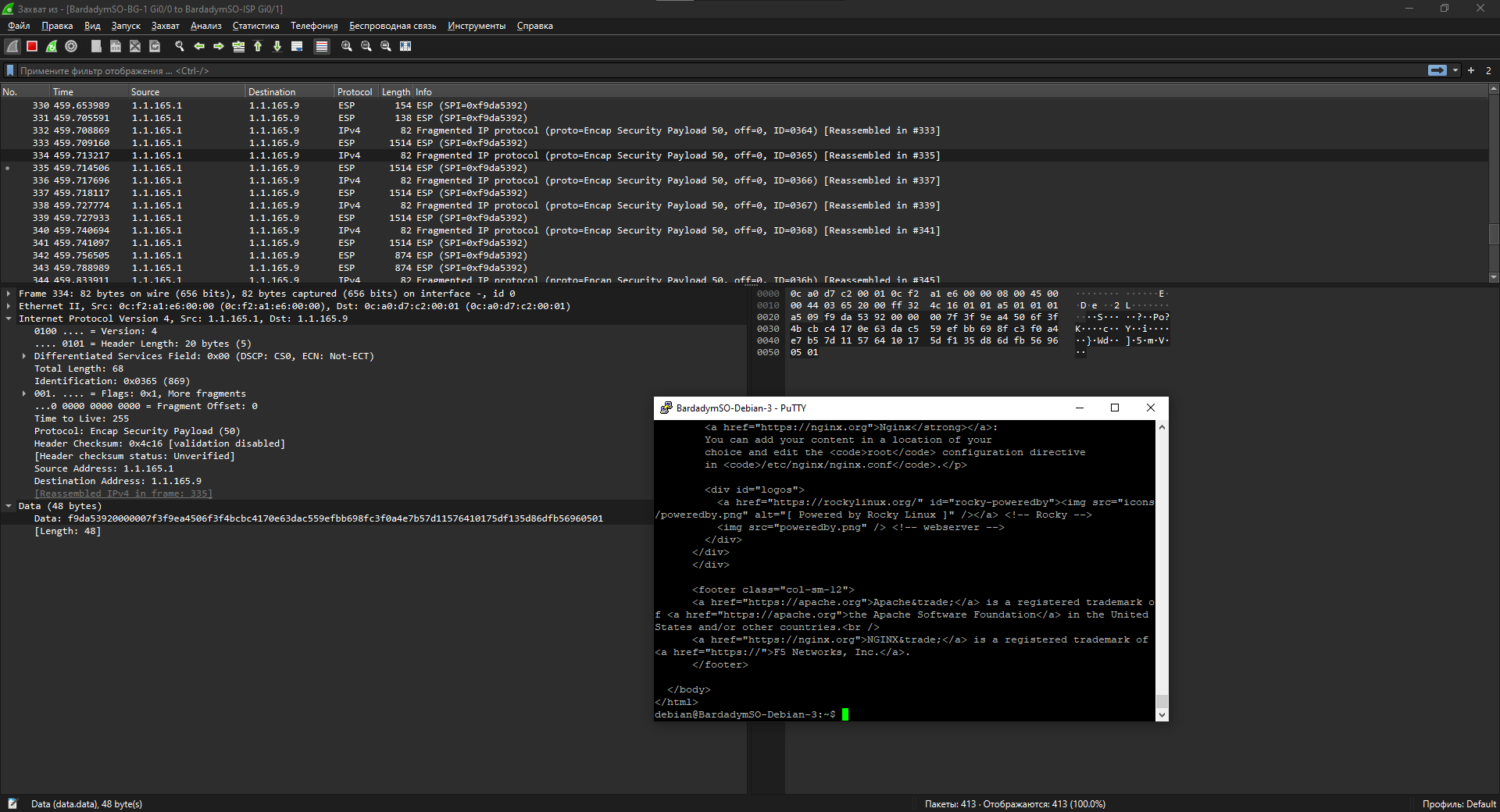


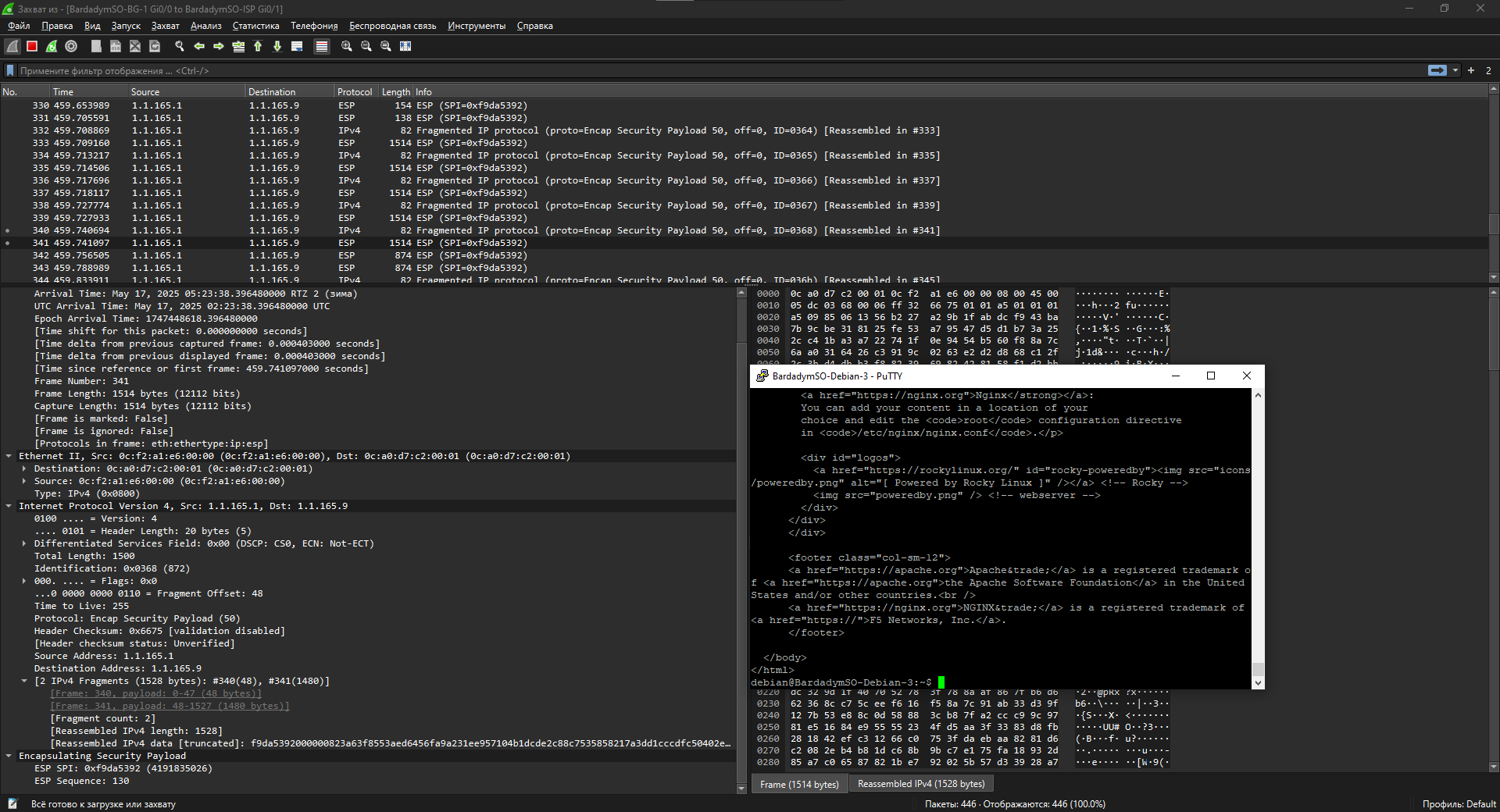


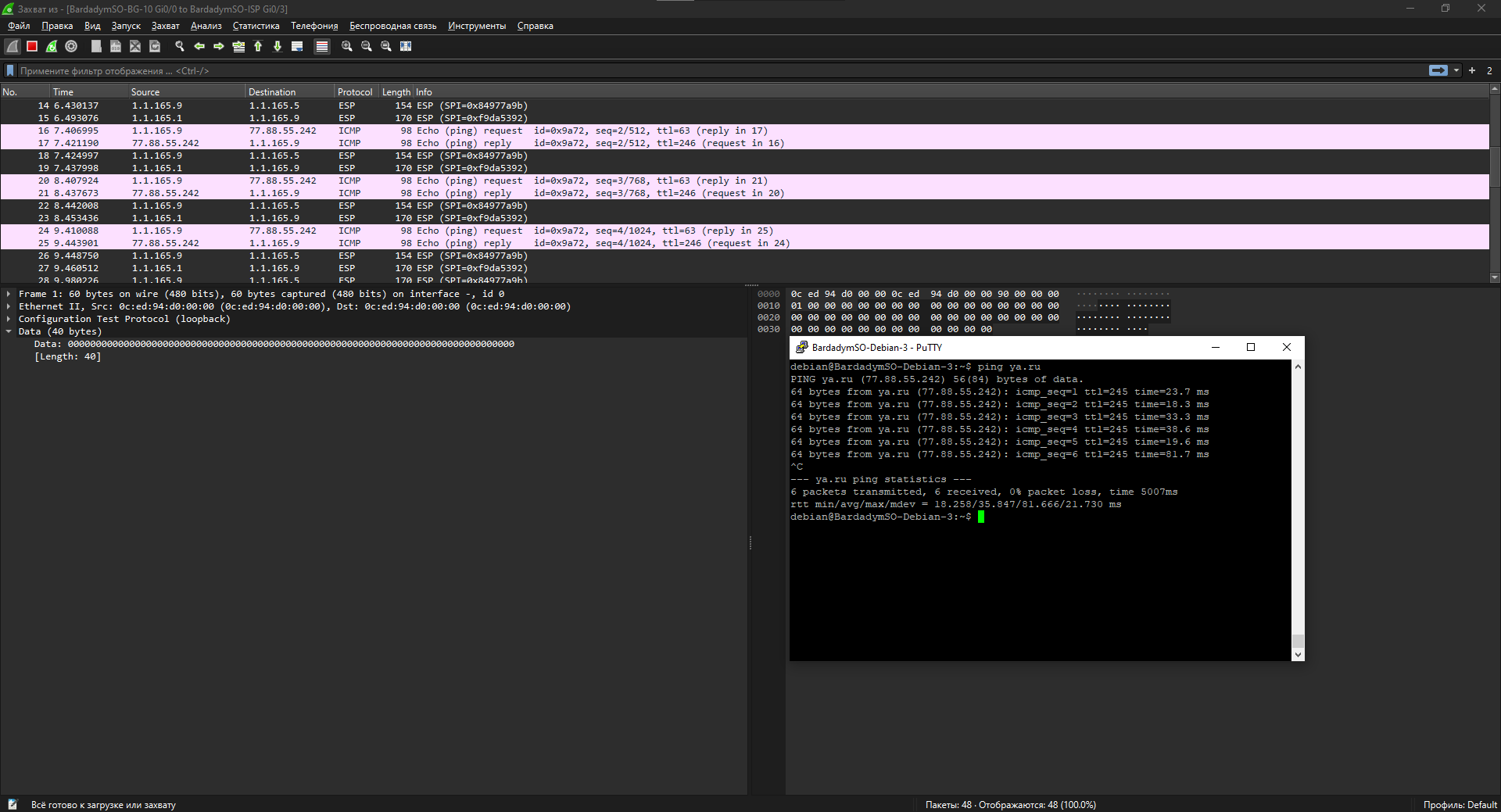




Задание 8. Настроить IPsec шифрование трафика, идущего по тоннелю между офисом и филиалом.

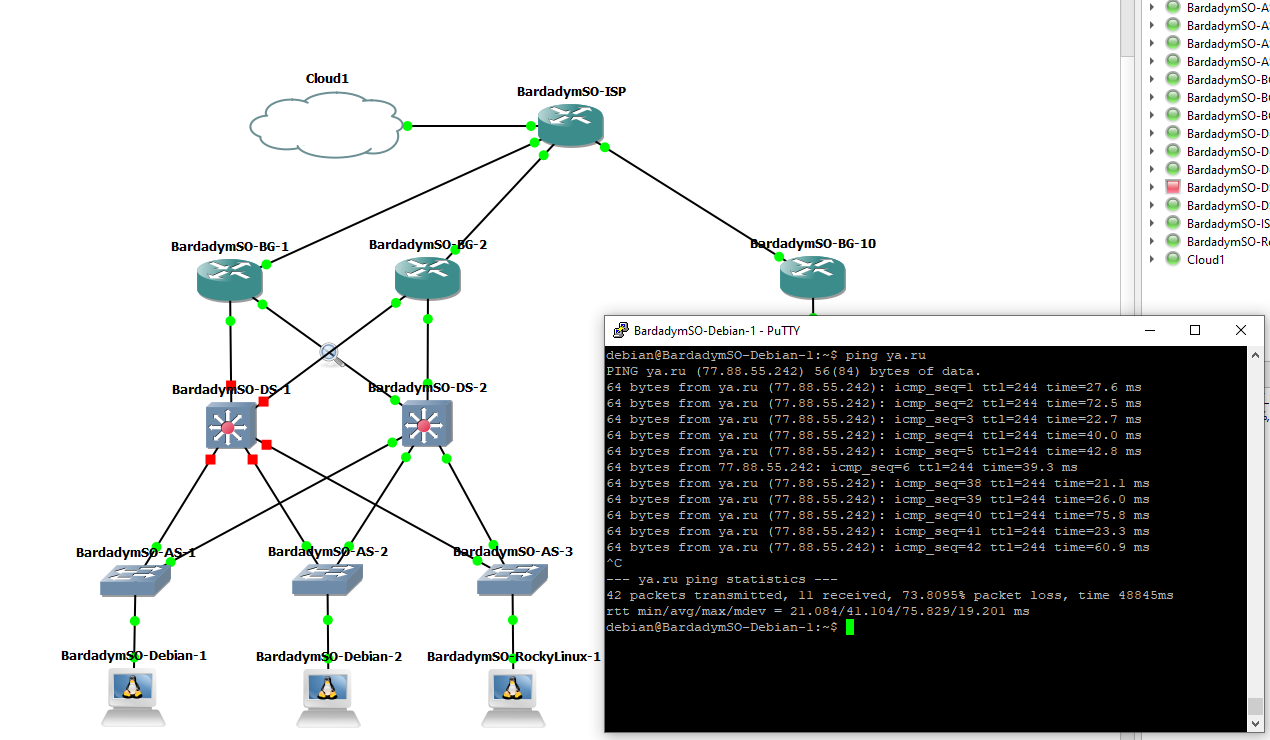


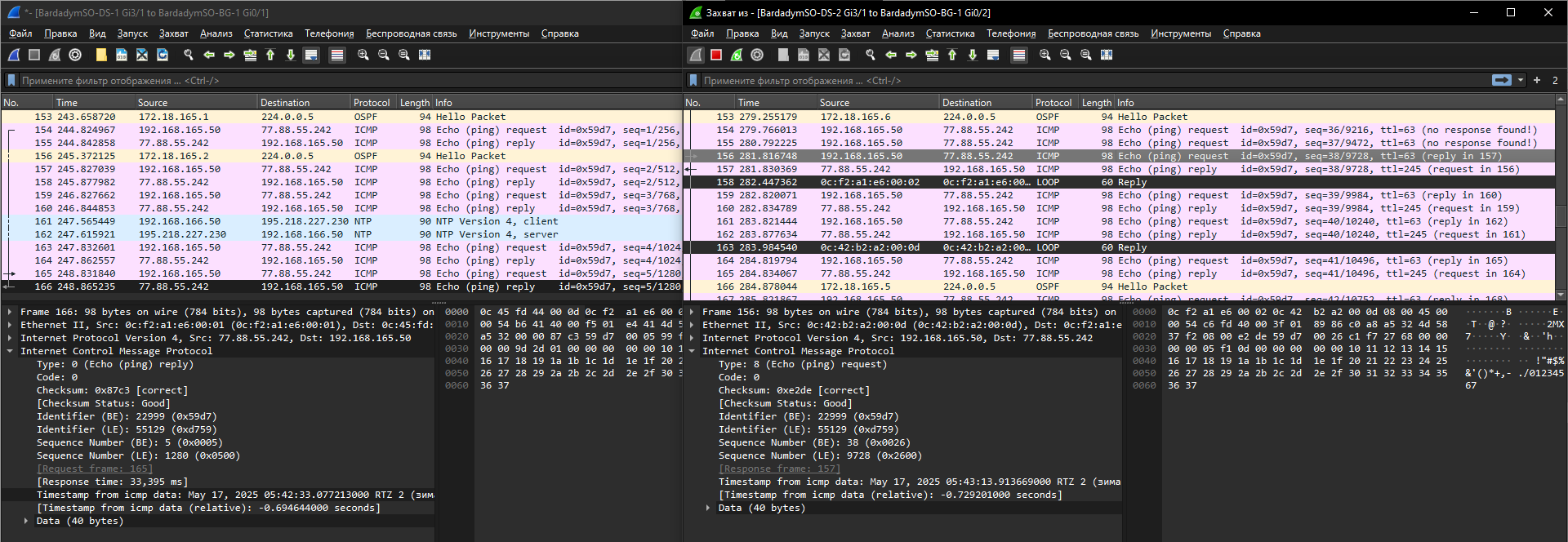




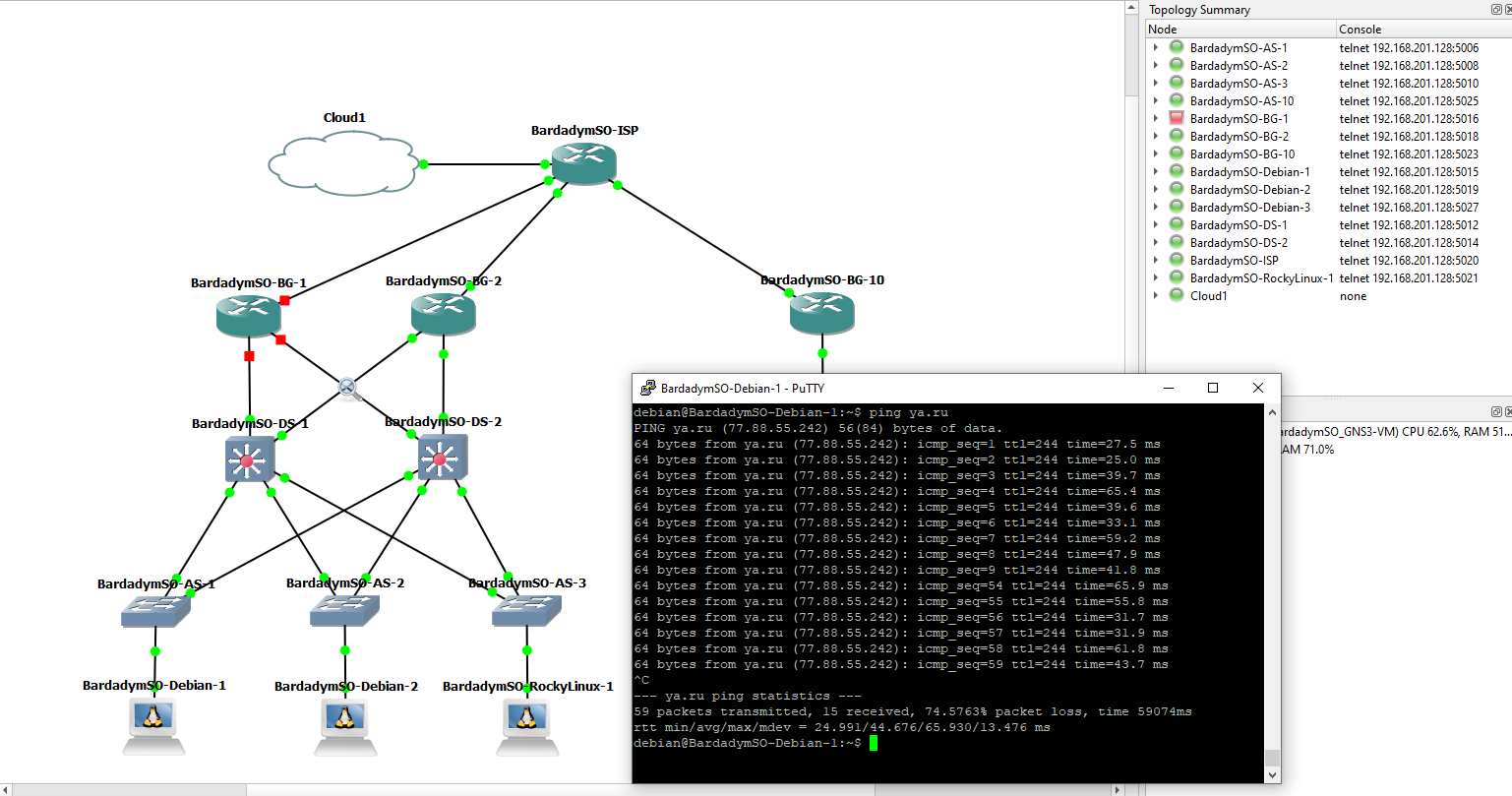
Задание 9. Протестировать отказоустойчивость сети, отключая по очереди различные ее компоненты. Предложить изменения настроек, способствующие ускорению сходимости сети после отказов ее компонентов.

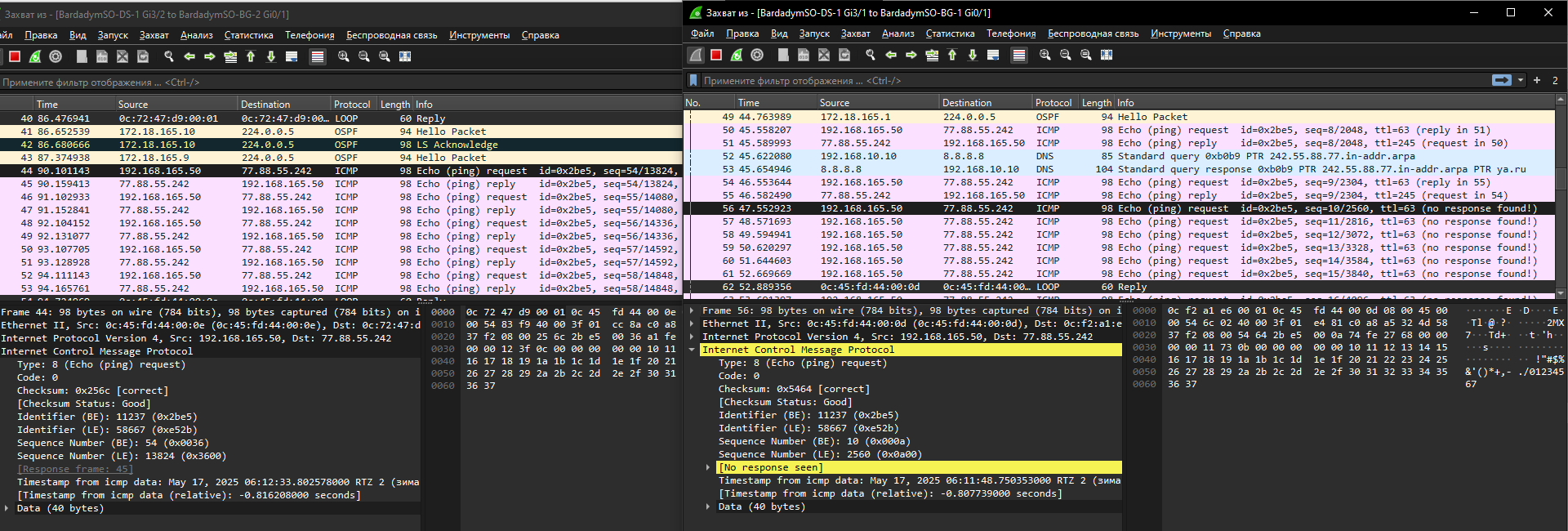
Отключение DS1:



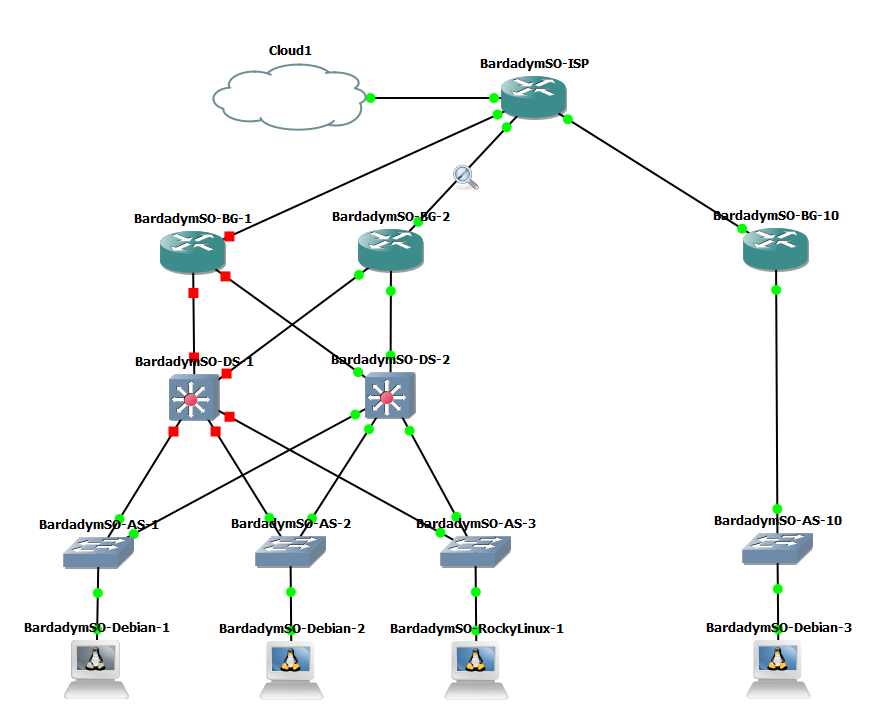


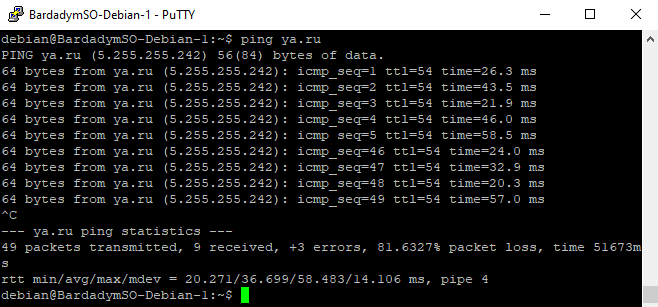
Отключение BG1:

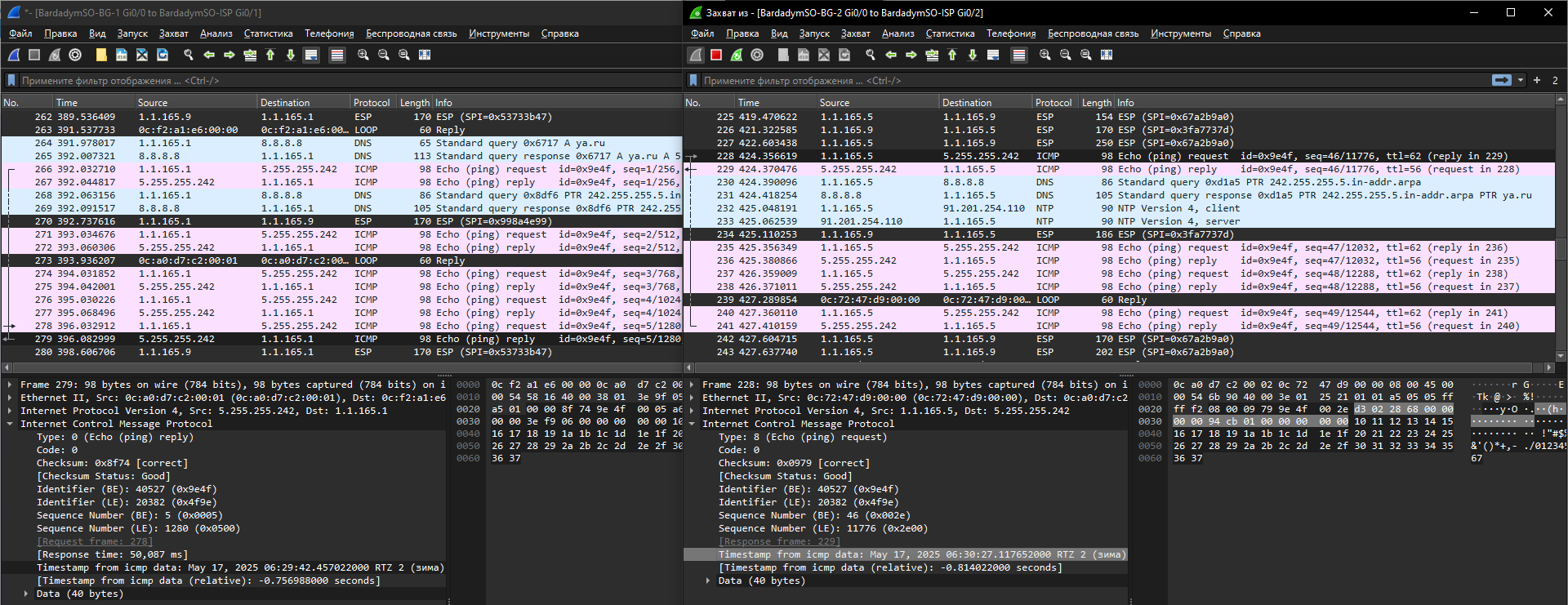




Отключение BG1 и DS1:







**Контрольные вопросы:**

1. Что необходимо учитывать при планировании адресного пространства?

2. Что такое PAT и PAT overload?

3. Что такое проброс портов?

4. Каковы принципы построения сетевых тоннелей?

5. Какова сходимость сети в случае применения различных версий протокола STP?

6. Перечислите фазы IPsec.