**МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ**

**БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ**

**Факультет прикладной математики и информатики**

**СЕРГИЕНКО ЛЕВ ЭДУАРДОВИЧ**

Отчет по лабораторной работе № 12,

вариант 21

(“Компьютерные сети”)

студента 3-го курса 12-ой группы

|  |  |  |
| --- | --- | --- |
|  |  | **Преподаватель** |
|  | **Горячкин В.В.** |
|  | | |
| **2024 г.** | | |

**Цель работы.**

С помощью стандартного и расширенного ACL-листов запретить доступ к некоторым ресурсам сети.

|  |  |
| --- | --- |
| **Вариант** | Сеть 1 - 6 |
| **21** | 137.42.0.0/24  137.43.0.0/24  137.44.0.0/24  137.45.0.0/24  137.46.0.0/24  137.47.0.0/24 |

**Этапы выполнения работы.**

1. Соберите схему сети, приведенную на скриншоте. Согласно Вашему варианту, настройте маршрутизацию между узлами, задав маршруты по умолчанию. Проверьте взаимодействие с узлами сети с помощью команды ping.

A diagram of a network

Description automatically generated

A screenshot of a computer

Description automatically generated

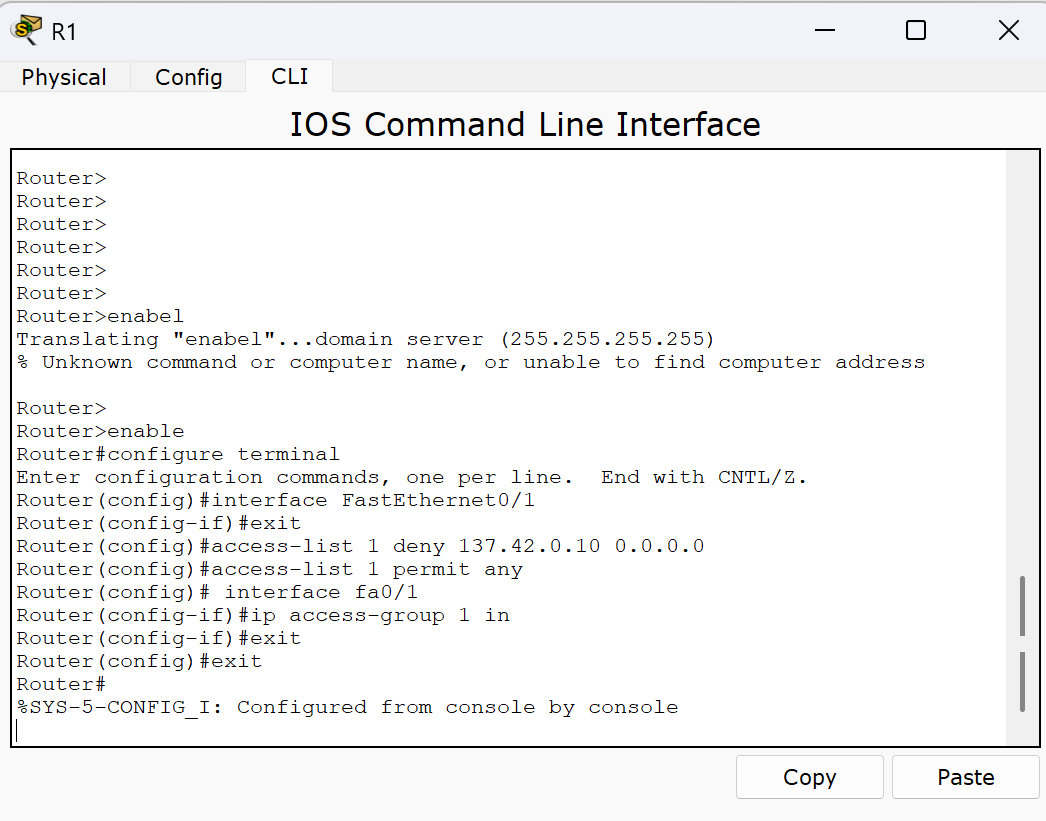
1. Через эмулятор браузера на узлах проверьте доступность HTTP-

сервера. В строке браузера введите ip-адрес HTTP-сервера.

A computer screen shot of a computer

Description automatically generated

1. Настройте на маршрутизаторе R1 стандартный ACL, запрещающий устройству PC1 взаимодействовать с устройствами из других сетей



4. Проверьте правильность настройки стандартного ACL.

4.1. Зайдите в эмулятор командной строки на устройстве PC1.

4.2. С помощью утилиты ping проверьте возможность взаимодействия устройства PC1 c любым конечным устройством сети. Если PC1 не получает эхо ответы от другого устройства, ACL настроен правильно.

***В отчёте отразите результаты работы утилиты ping.***

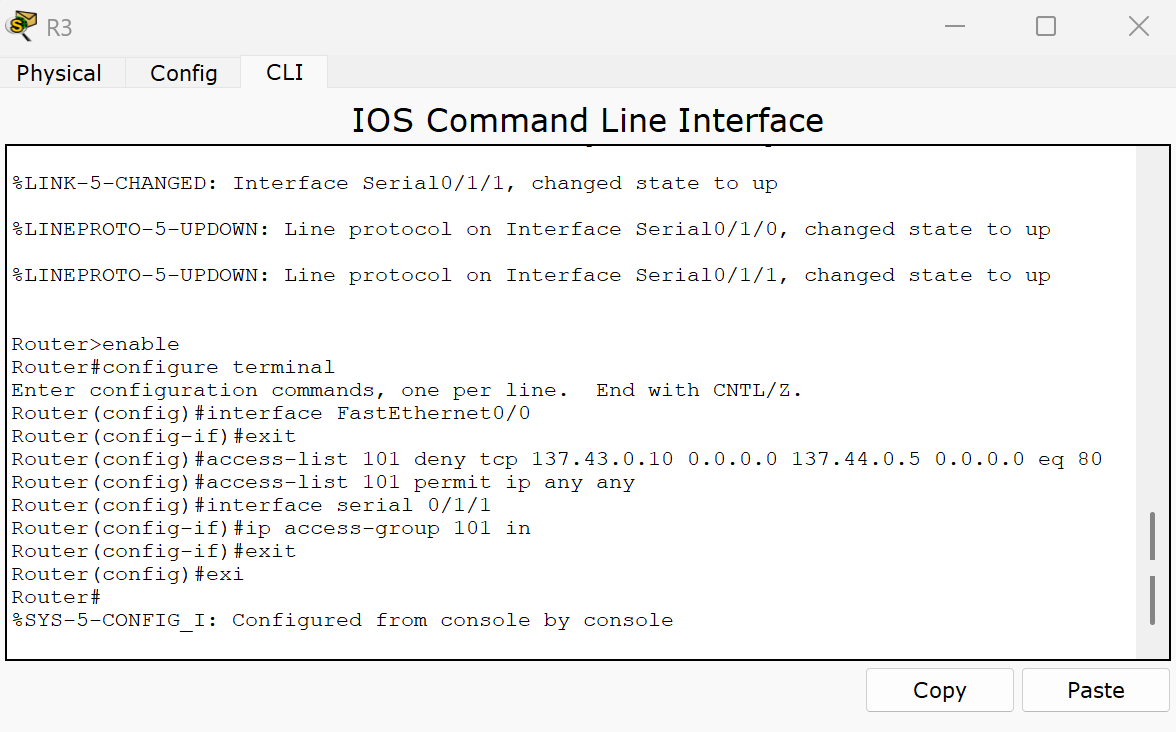
5. Настройте на маршрутизаторе R3 расширенный ACL, запрещающий устройству PC2 обращаться к веб-серверу по протоколу HTTP.

5.1. Зайдите в режим глобальной конфигурации маршрутизатора.

R3>**enable**

R3#**configure terminal**

5.2. Создайте расширенный ACL.



R3(config)#**access-list 101 deny tcp 192.168.2.10 0.0.0.0 192.168.3.5 0.0.0.0 eq 80**

|  |  |
| --- | --- |
| access-list | Команда создания ACL |
| 101 | Номер ACL |
| deny | Команда «запретить» |
| tcp | Протокол транспортного уровня |
| 192.168.2.10 | Адрес источника |
| 0.0.0.0 | Wildcard маска для адреса источника |
| 192.168.3.5 | Адрес получателя |
| 0.0.0.0 | Wildcard маска для адреса получателя |
| eq 80 | Порт назначения, по которому нужно запретить взаимодействие |

R3(config)#**access-list 101 permit ip any any**

R3(config)#**access-list 101 permit icmp any any**

5.3. Установите ACL на интерфейсе s0/0/1 маршрутизатора R3.

R3(config)#**interface serial 0/0/1**

R3(config-if)#**ip access-group 101 in**

6. Проверьте правильность настройки расширенного ACL.

6.1. Зайдите в эмулятор командной строки на устройстве PC2. С помощью утилиты ping проверьте возможность взаимодействия устройства PC2 c любым конечным устройством сети.

6.2. С помощью эмулятора браузера попробуйте загрузить страницу HTTP –сервера по его адресу. Если устройство PC2 получает эхо-ответы от сервера, но страницу загрузить не удаётся, значит ACL настроен правильно.

A computer screen with a white screen

Description automatically generated

С других узлов сервер должен быть доступен.

A computer screen with a white screen

Description automatically generated

***Отразите в отчёте результаты ping РС2 с HTTP-сервером, результаты загрузки на РС2 HTTP-страницы, взаимодействие остальных узлов сети с HTTP-сервером.***