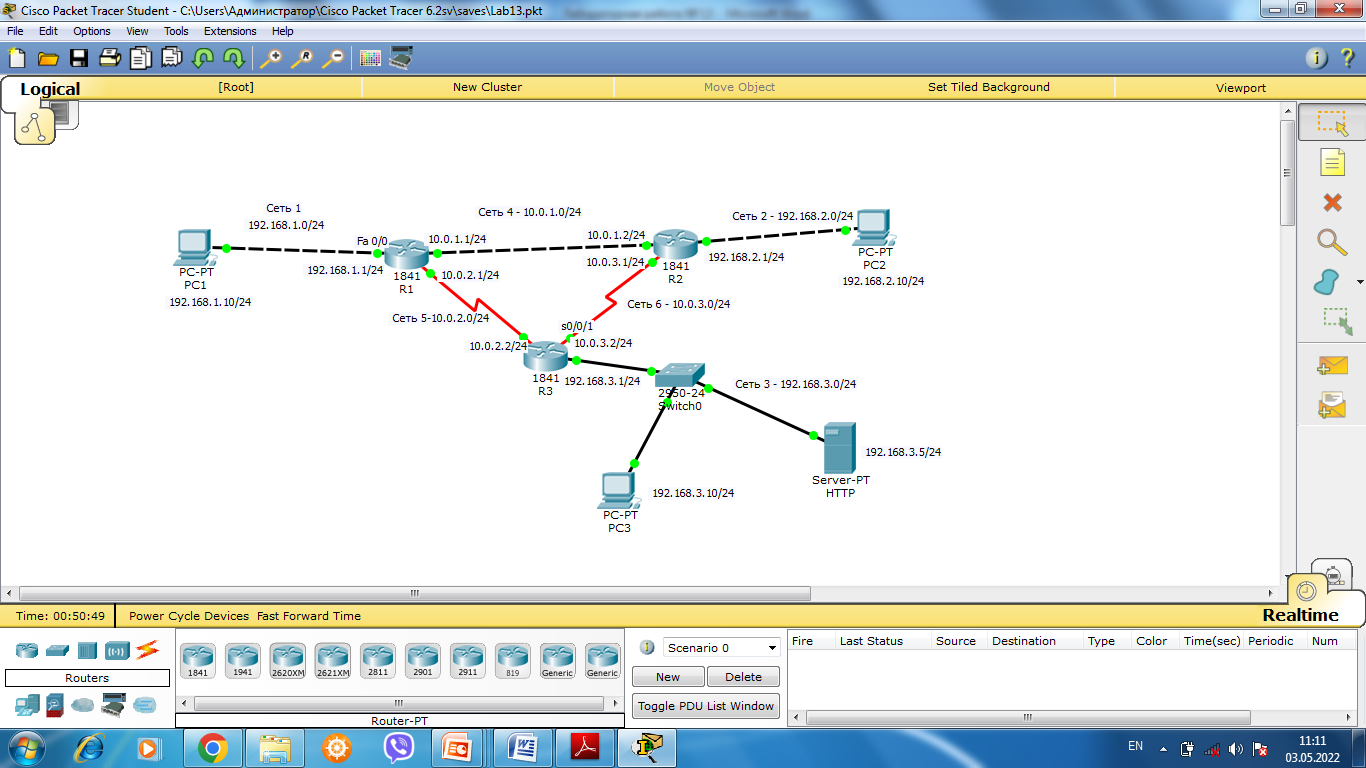
**Лабораторная работа № 12.**

**Настройка списков контроля доступа**

**на устройствах Cisco.**

Топология сети:



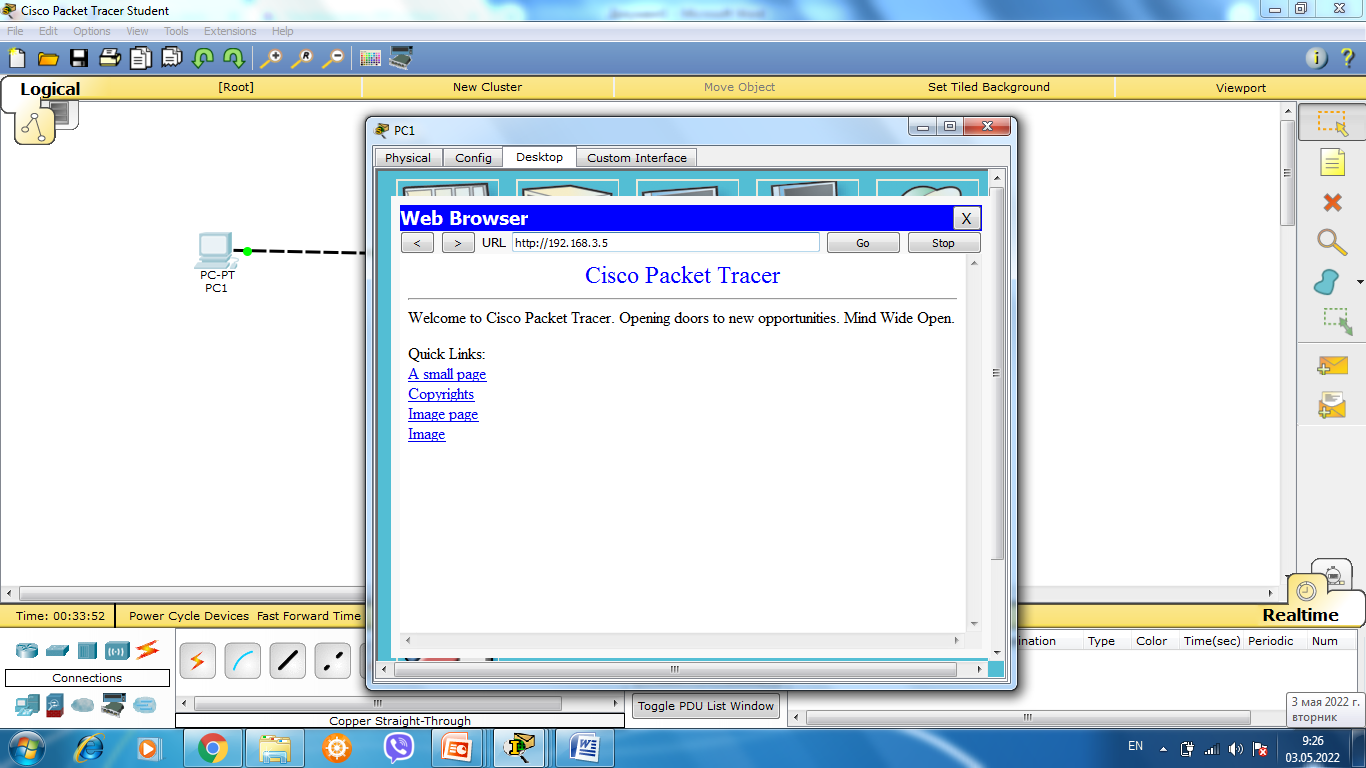
**Цель работы.**

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

**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. (***В отчет включить результаты пингов***)
2. Через эмулятор браузера на узлах проверьте доступность HTTP-

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



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

3.1. Зайдите в режим глобальной конфигурации маршрутизатора.

R1>**enable**

R1#**configure terminal**

3.2. Создайте стандартный ACL.

R1(config)#**access-list 1 deny 192.168.1.10 0.0.0.0**

|  |  |
| --- | --- |
| access-list | Команда создания ACL |
| 1 | Номер ACL |
| deny | Команда «запретить» |
| 192.168.1.10 | Адрес, к которому надо применить команду |
| 0.0.0.0 | Wildcard маска |

R1(config)#**access-list 1 permit any**

3.3. Установите ACL на интерфейсе fa0/0 маршрутизатора R1.

R1(config)#**interface fa 0/0**

R1(config-if)#**ip access-group 1 in**

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.

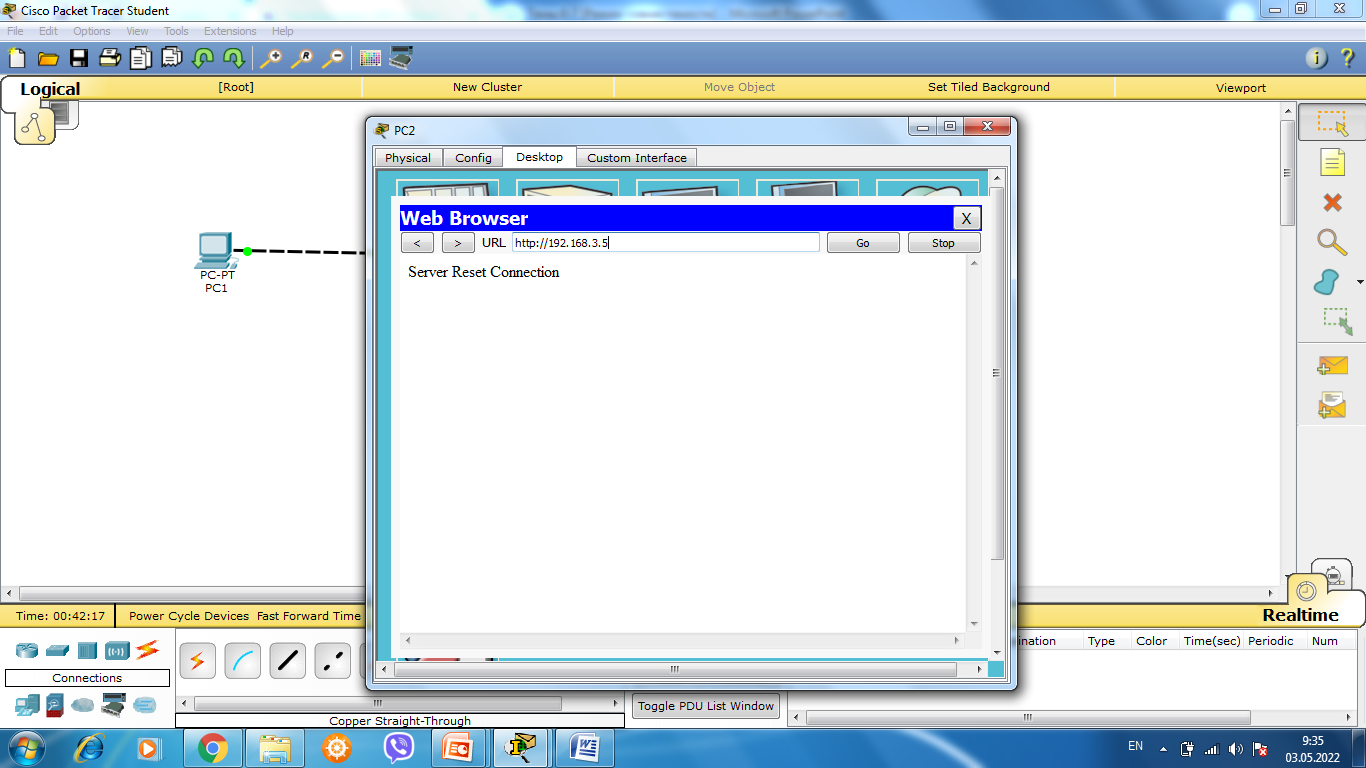
R3(config)#**interface serial 0/0/1**

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

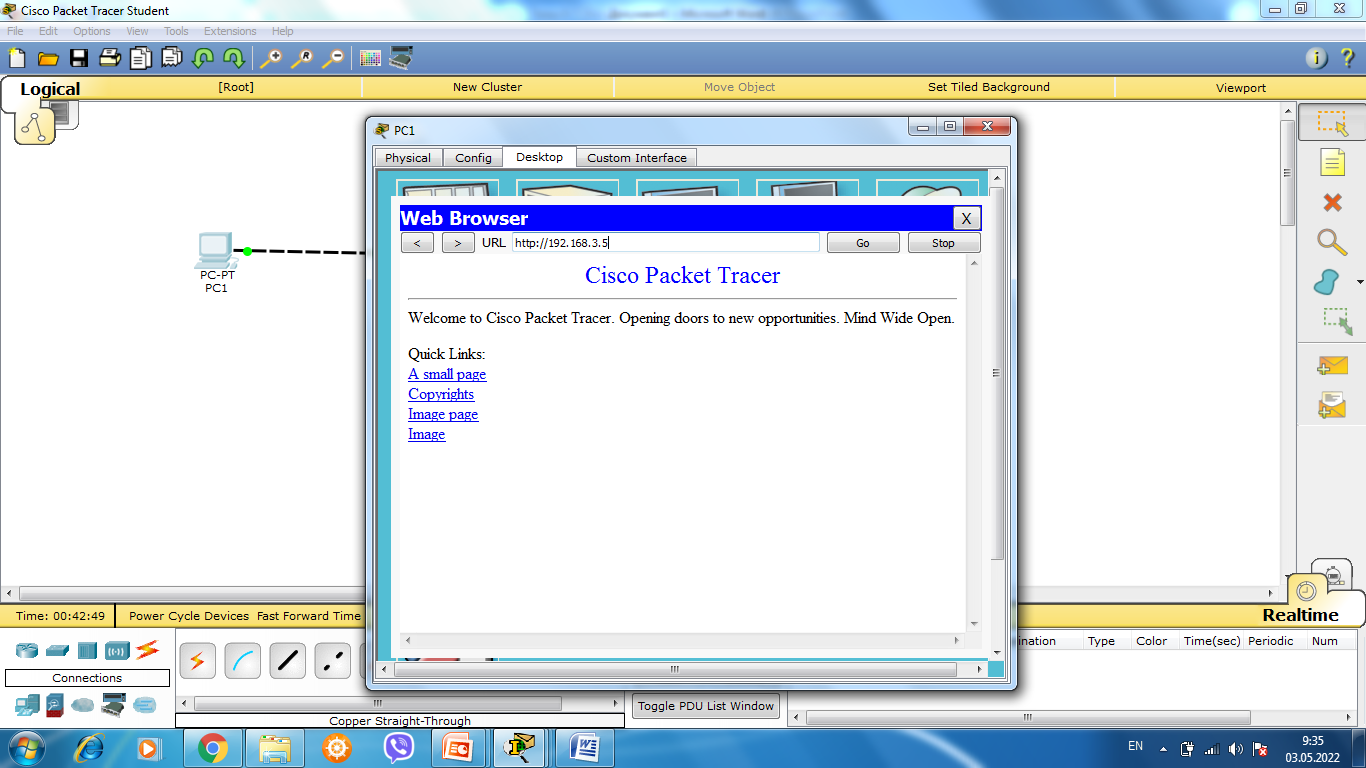
6. Проверьте правильность настройки расширенного ACL.

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.



С других узлов сервер должен быть доступен.



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

Варианты заданий

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Вариант** | ***Сеть 1 - 6*** | **Вариант** | ***Сеть 1 - 6*** | **Вариант** | ***Сеть 1 - 6*** |
| **1** | 111.0.0.0/24  112.0.0.0/24  113.0.0.0/24  114.0.0.0/24  115.0.0.0/24  116.0.0.0/24 | **2** | 131.0.0.0/24  132.0.0.0/24  133.0.0.0/24  134.0.0.0/24  135.0.0.0/24  136.0.0.0/24 | **3** | 196.5.1.0/24  196.5.2.0/24  196.5.3.0/24  196.5.4.0/24  196.5.5.0/24  196.5.6.0/24 |
| **Вариант** | ***Сеть 1 - 6*** | **Вариант** | ***Сеть 1 - 6*** | **Вариант** | ***Сеть 1 - 6*** |
| **4** | 180.101.0.0/24  180.102.0.0/24  180.103.0.0/24  180.104.0.0/24  180.105.0.0/24  180.106.0.0/24 | **5** | 203.21.140.0/24  203.21.141.0/24  203.21.142.0/24  203.21.143.0/24  203.21.144.0/24  203.21.145.0/24 | **6** | 179.11.0.0/24  179.12.0.0/24  179.13.0.0/24  179.14.0.0/24  179.15.0.0/24  179.16.0.0/24 |
| **Вариант** | Сеть 1 - 6 | **Вариант** | Сеть 1 - 6 | **Вариант** | Сеть 1 - 6 |
| **7** | 205.100.1.0/24  205.100.2.0/24  205.100.3.0/24  205.100.4.0/24  205.100.5.0/24  205.100.6.0/24 | **8** | 155.10.0.0/24  155.11.0.0/24  155.12.0.0/24  155.13.0.0/24  155.14.0.0/24  155.15.0.0/24 | **9** | 200.192.210.0/24  200.192.211.0/24  200.192.212.0/24  200.192.213.0/24  200.192.214.0/24  200.192.215.0/24 |
| **Вариант** | Сеть 1 - 6 | **Вариант** | Сеть 1 - 6 | **Вариант** | Сеть 1 - 6 |
| **10** | 187.16.0.0/24  187.17.0.0/24  187.18.0.0/24  187.19.0.0/24  187.20.0.0/24  187.21.0.0/24 | **11** | 192.168.1.0/24  192.168.2.0/24  192.168.3.0/24  192.168.4.0/24  192.168.5.0/24  192.168.6.0/24 | **12** | 111.0.0.0/24  112.0.0.0/24  113.0.0.0/24  114.0.0.0/24  115.0.0.0/24  116.0.0.0/24 |
| **Вариант** | Сеть 1 - 6 | **Вариант** | Сеть 1 - 6 | **Вариант** | Сеть 1 - 6 |
| **13** | 161.11.0.0/24  161.12.0.0/24  161.13.0.0/24  161.14.0.0/24  161.15.0.0/24  161.16.0.0/24 | **14** | 54.0.0.0/24  55.0.0.0/24  56.0.0.0/24  57.0.0.0/24  58.0.0.0/24  59.0.0.0/24 | **15** | 81.0.0.0/24  82.0.0.0/24  83.0.0.0/24  84.0.0.0/24  85.0.0.0/24  86.0.0.0/24 |
| **Вариант** | Сеть 1 - 6 | **Вариант** | Сеть 1 - 6 | **Вариант** | Сеть 1 - 6 |
| **16** | 101.0.0.0/24  102.0.0.0/24  103.0.0.0/24  104.0.0.0/24  105.0.0.0/24  106.0.0.0/24 | **17** | 181.79.0.0/24  181.80.0.0/24  181.81.0.0/24  181.82.0.0/24  181.83.0.0/24  181.84.0.0/24 | **18** | 171.123.0.0/24  171.124.0.0/24  171.125.0.0/24  171.126.0.0/24  171.127.0.0/24  171.128.0.0/24 |
| **Вариант** | Сеть 1 - 6 | **Вариант** | Сеть 1 - 6 | **Вариант** | Сеть 1 - 6 |
| **19** | 206.208.101.0/24  206.208.102.0/24  206.208.103.0/24  206.208.104.0/24  206.208.105.0/24  206.208.106.0/24 | **20** | 128.100.0.0/24  128.101.0.0/24  128.102.0.0/24  128.103.0.0/24  128.104.0.0/24  128.105.0.0/24 | **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 |
| **Вариант** | Сеть 1 - 6 | **Вариант** | Сеть 1 - 6 | **Вариант** | Сеть 1 - 6 |
| **22** | 221.56.1.0/24  221.56.2.0/24  221.56.3.0/24  221.56.4.0/24  221.56.5.0/24  221.56.6.0/24 | **23** | 91.0.0.0/24  92.0.0.0/24  93.0.0.0/24  94.0.0.0/24  95.0.0.0/24  96.0.0.0/24 | **24** | 121.0.0.0/24  122.0.0.0/24  123.0.0.0/24  124.0.0.0/24  125.0.0.0/24  126.0.0.0/24 |
| **Вариант** | Сеть 1 - 6 | **Вариант** | Сеть 1 - 6 | **Вариант** | Сеть 1 - 6 |
| **25** | 201.16.1.0/24  201.16.2.0/24  201.16.3.0/24  201.16.4.0/24  201.16.5.0/24  201.16.6.0/24 | **26** | 211.16.1.0/24  211.16.2.0/24  211.16.3.0/24  211.16.4.0/24  211.16.5.0/24  211.16.6.0/24 | **27** | 100.10.0.0/24  100.20.0.0/24  100.30.0.0/24  100.40.0.0/24  100.50.0.0/24  100.60.0.0/24 |