**Лабораторная работа № 13.**

**Настройка списков контроля доступа**

**на устройствах Cisco.**

Топология сети:

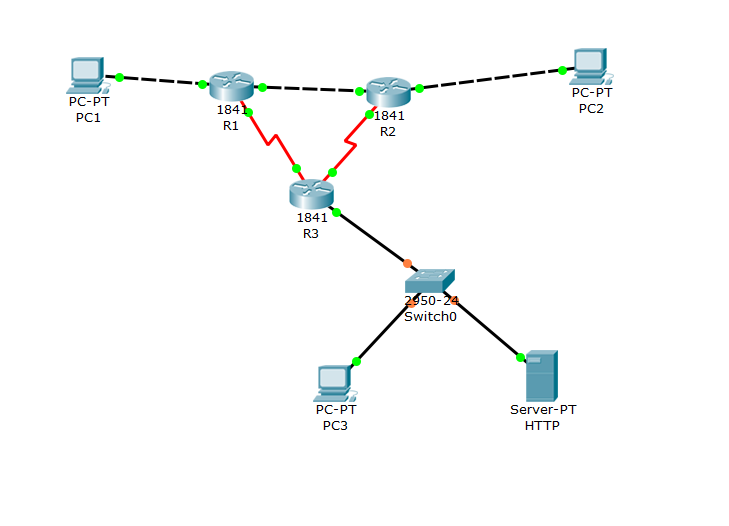
|  |  |
| --- | --- |
| **Вариант** | ***Сеть 1 - 6*** |
| **6** | 179.11.0.0/24  179.12.0.0/24  179.13.0.0/24  179.14.0.0/24  179.15.0.0/24  179.16.0.0/24 |

**Цель работы.**

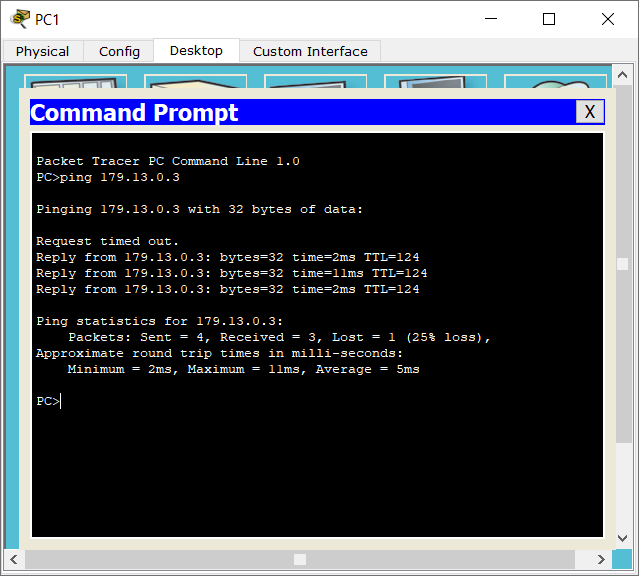
С помощью стандартного и расширенного ACL-листов запретить доступ к некоторым ресурсам сети.

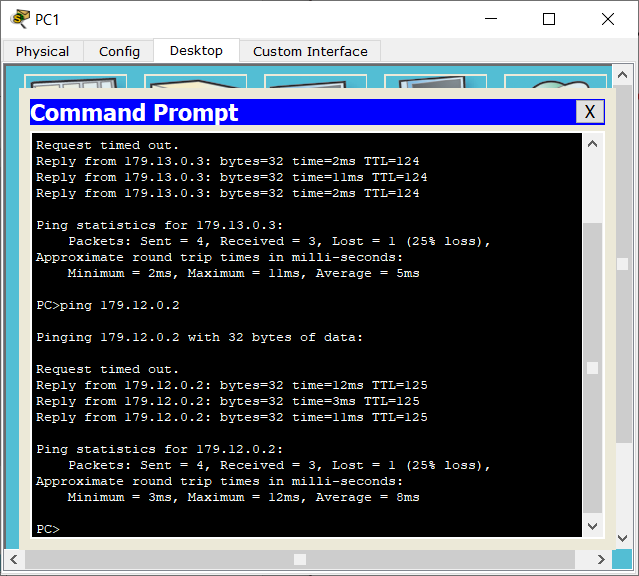
**Этапы выполнения работы.**

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***)

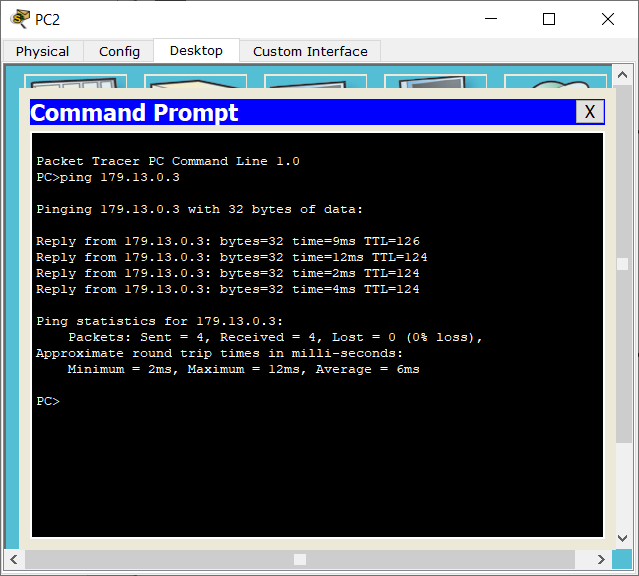


**PC1->PC3**

  
**PC1->PC2**

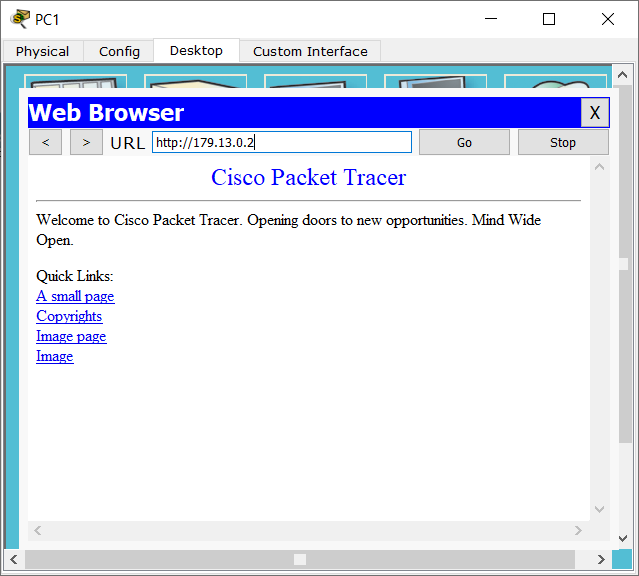


**PC2->PC3**



1. 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**

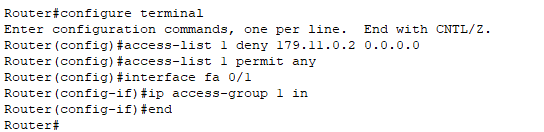
|  |  |
| --- | --- |
| access-list | Команда создания ACL |
| 1 | Номер ACL |
| deny | Команда «запретить» |
| 192.168.1.10 | Адрес, к которому надо применить команду |
| 0.0.0.0 | Wildcard маска |

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**



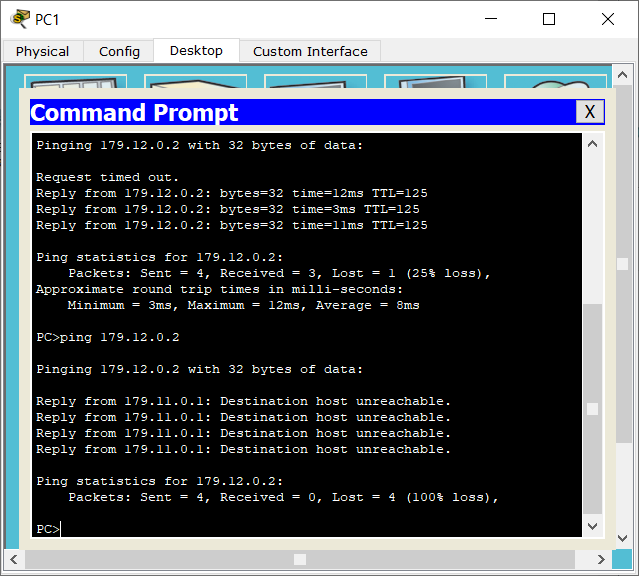
4. Проверьте правильность настройки стандартного ACL.

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.***

**PC1->PC2**



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**

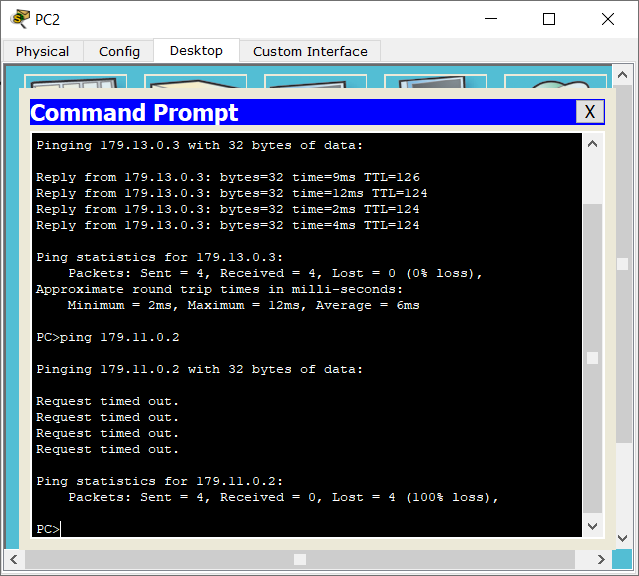
5.3. Установите ACL на интерфейсе s0/0/1 маршрутизатора R3.

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

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

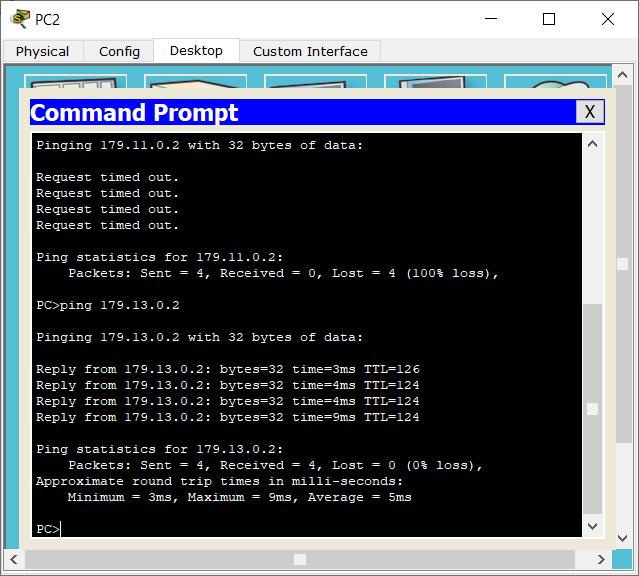
6. Проверьте правильность настройки расширенного ACL.

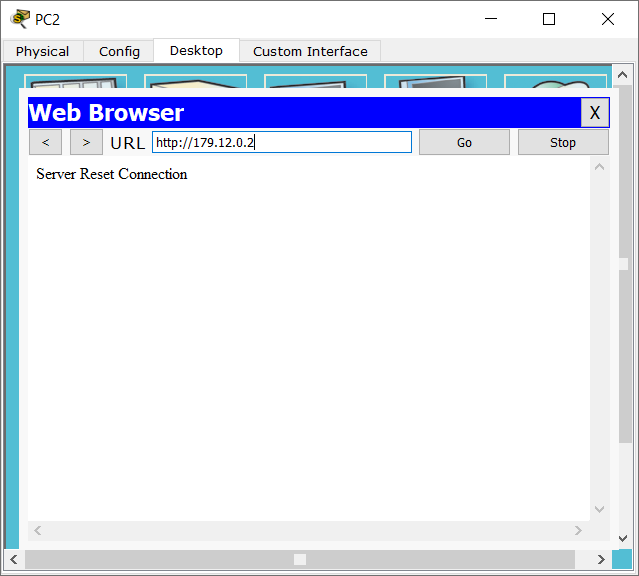
6.1. Зайдите в эмулятор командной строки на устройстве PC2. С помощью утилиты ping проверьте возможность взаимодействия устройства PC2 c любым конечным устройством сети.



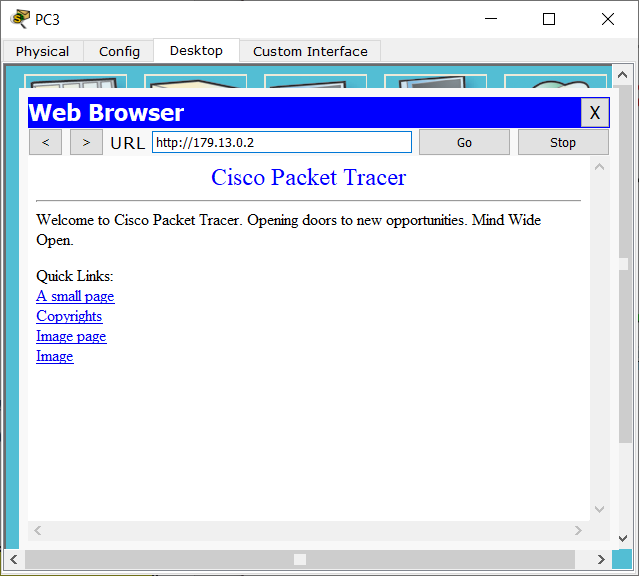
6.2. С помощью эмулятора браузера попробуйте загрузить страницу HTTP –сервера по его адресу. Если устройство PC2 получает эхо-ответы от сервера, но страницу загрузить не удаётся, значит ACL настроен правильно.

**PC2->HTTP**





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.***