**Министерство образования Республики Беларусь**

**БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ**

**Факультет прикладной математики и информатики**

**Чешко Ульяна геннадьевна**

**Настройка списков контроля доступа**

**на устройствах Cisco.**

Отчет по лабораторной работе № 13,

вариант 21

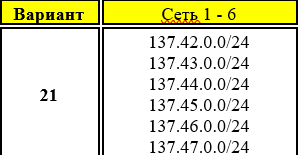
(“Компьютерные сети”)

студента 3-го курса 5-ой группы

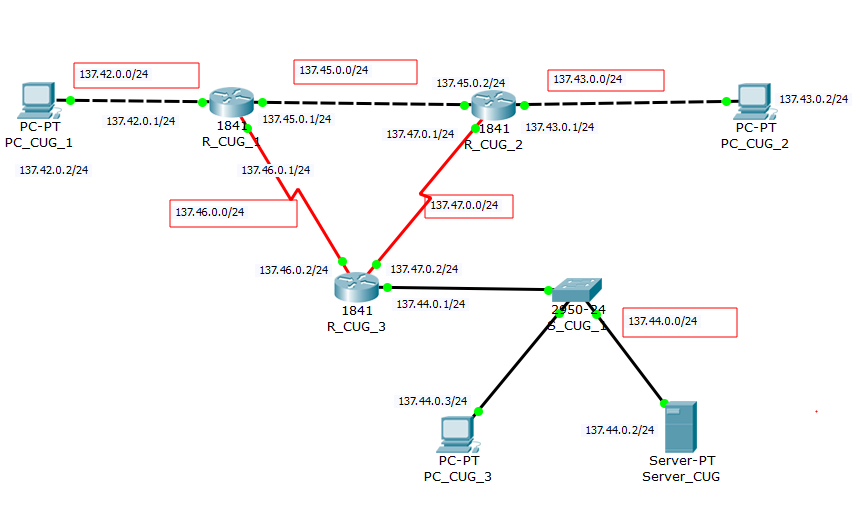
|  |  |  |
| --- | --- | --- |
|  |  | **Преподаватель** |
|  |  | **Бубен И.В.** |

**Минск 2024**

## Исходные данные для варианта задания



1. Соберите схему сети, приведенную на скриншоте. Согласно Вашему варианту, настройте маршрутизацию между узлами, задав маршруты по умолчанию.



Настройка маршрутов по умолчанию:







1. Проверьте взаимодействие с узлами сети с помощью команды ping. (***В отчет включить результаты пингов***)



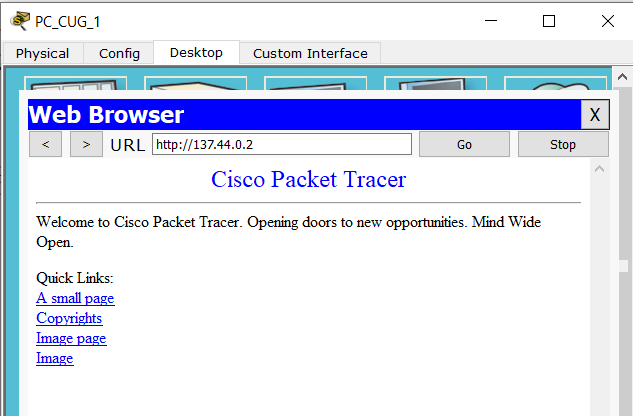


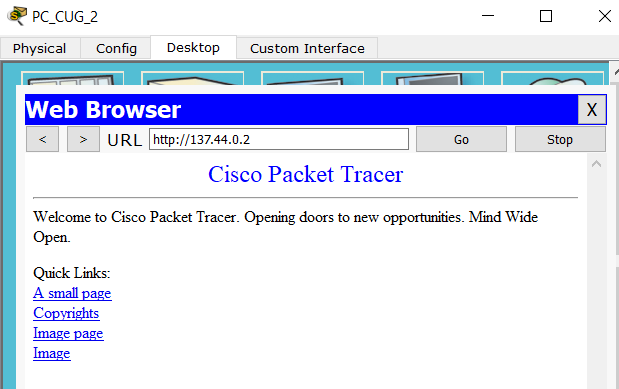


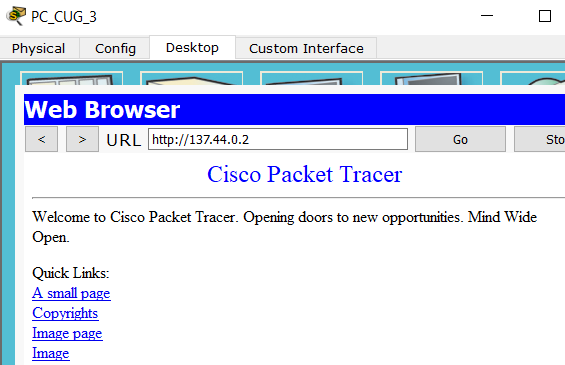
Все узлы достижимы, значит маршруты настроены верно.

1. Через эмулятор браузера на узлах проверьте доступность HTTP-

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







HTTP-сервер доступен со всех узлов.

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





|  |  |
| --- | --- |
| access-list | Команда создания ACL |
| 21 | Номер ACL |
| deny | Команда «запретить» |
| 137.42.0.2 | Адрес PC\_CUG\_1 |
| 0.0.0.0 | Wildcard маска |

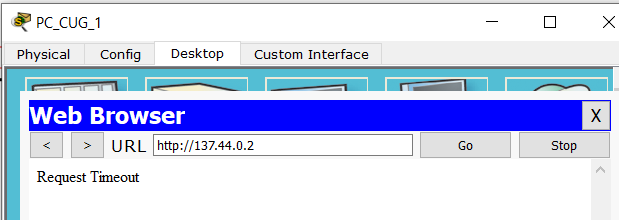
* 1. Установите ACL на интерфейсе fa0/0 маршрутизатора R1.



1. Проверьте правильность настройки стандартного ACL. 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.

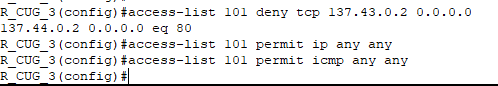
***В отчёте отразите результаты работы утилиты ping.***

******

******

После настройки ACL, запрещающего взаимодействовать PC\_CUG\_1 с устройствами других сетей, PC\_CUG\_1 не получает эхо-ответы, значит ACL настроен правильно.

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



|  |  |
| --- | --- |
| access-list | Команда создания ACL |
| 101 | Номер ACL |
| deny | Команда «запретить» |
| tcp | Протокол транспортного уровня |
| 137.43.0.2 | Адрес PC\_CUG\_2 |
| 0.0.0.0 | Wildcard маска для адреса источника |
| 137.44.0.2 | Адрес сервера |
| 0.0.0.0 | Wildcard маска для адреса получателя |
| eq 80 | Порт назначения, по которому нужно запретить взаимодействие |

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

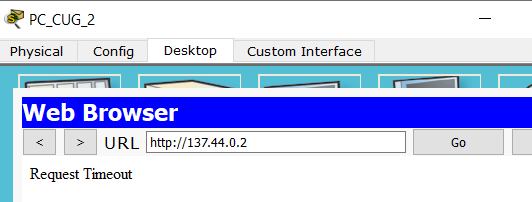


1. Проверьте правильность настройки расширенного ACL.Зайдите в эмулятор командной строки на устройстве PC2. С помощью утилиты ping проверьте возможность взаимодействия устройства PC2 c любым конечным устройством сети.



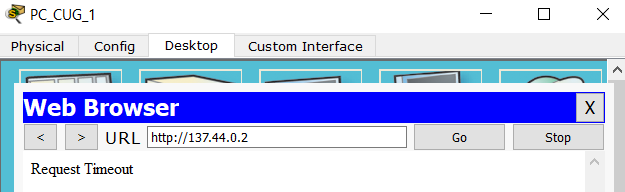
PC\_CUG\_1 не достижим, так как для него был установлен ACL, запрещающий взаимодействие с устройствами из других сетей, а PC\_CUG\_3 достижим.

7.1 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.

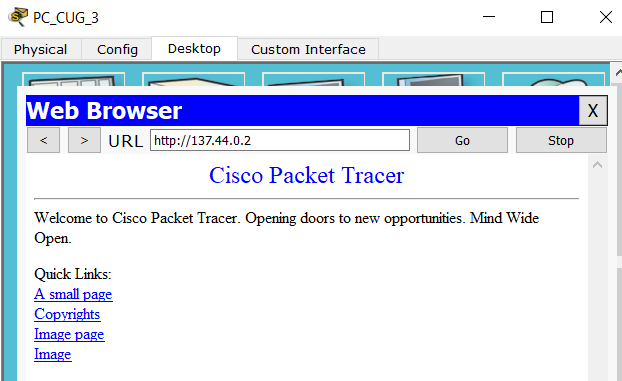




PC\_CUG\_2 получает эхо-ответы от сервера, но страницу загрузить не удаётся, значит ACL настроен правильно.



Помимо PC\_CUG\_2 доступа к HTTP нет и у PC\_CUG\_1, поскольку мы полностью запретили ему взаимодействовать с устройствами другой сети.



У PC\_CUG\_3 есть доступ к HTTP-серверу.