МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ,

СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ

ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФ. М.А. БОНЧ-БРУЕВИЧА»

(СПбГУТ)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Факультет Инфокоммуникационных сетей и систем

Кафедра Защищенных систем связи

Дисциплина Безопасность компьютерных сетей

ЛАБОРАТОРНАЯ РАБОТА №5

Configure IP ACLs to Mitigate Attacks

Направление/специальность подготовки

11.03.02 Инфокоммуникационные технологии и системы связи

Студенты:

Громов А. А., ИКТЗ-83 \_\_\_\_\_\_\_\_\_

*(Ф.И.О., № группы) (подпись)*

Жиляков Г. В., ИКТЗ-83 \_\_\_\_\_\_\_\_\_

*(Ф.И.О., № группы) (подпись)*

Миколаени М. С., ИКТЗ-83 \_\_\_\_\_\_\_\_\_

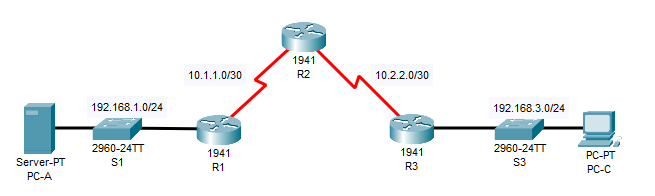
*(Ф.И.О., № группы) (подпись)*

Проверил:

К.т.н., доцент каф. ЗСС, Кушнир Д. В.

*(подпись)*

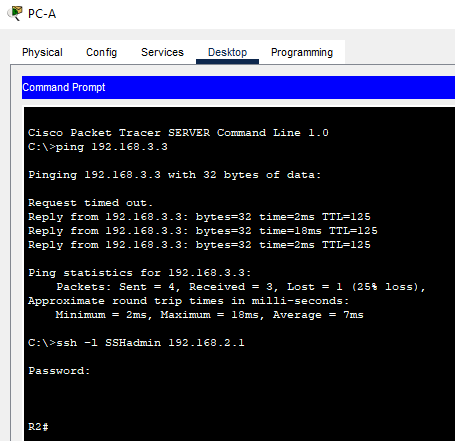
# Топология:



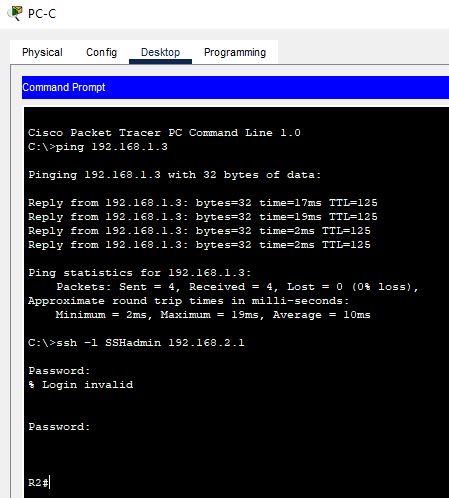
# Ход работы:

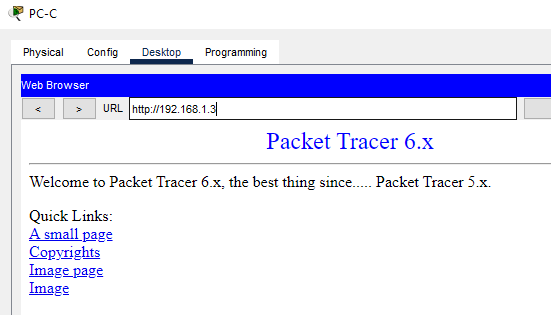
Часть 1. Проверка базовой связи по сети

Шаг 1. С компьютера PC-A проверьте связь с компьютером PC-C и маршрутизатором R2.



Шаг 2. С компьютера PC-C проверьте связь с компьютером PC-A и маршрутизатором R2.



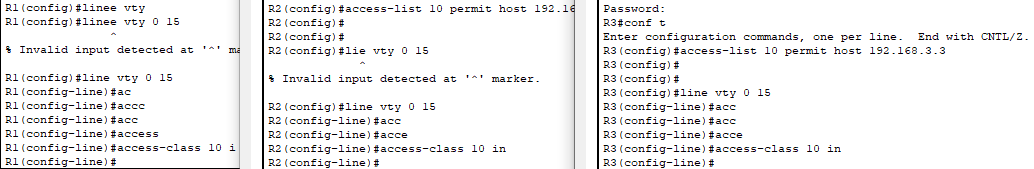


Часть 2. Защита доступа к маршрутизаторам

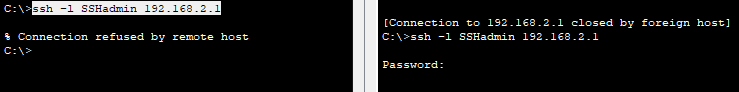
Шаг 1. Настройте список ACL 10 для блокировки удаленного доступа к маршрутизаторам со всех устройств, кроме PC-C.



Шаг 2. Примените список ACL 10 к входному трафику на линиях VTY.

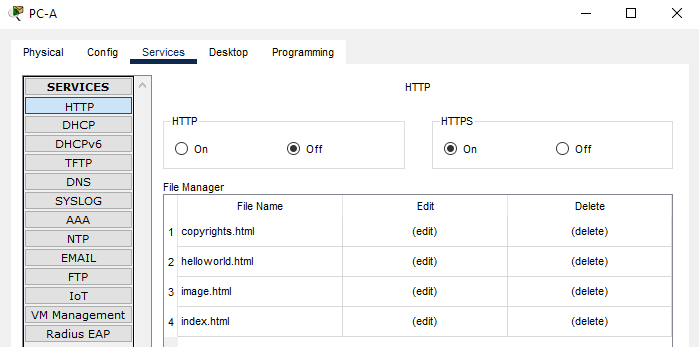


Шаг 3. Проверьте монопольный доступ со станции управления PC-C.

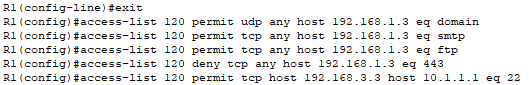


Часть 3. Создание нумерованного списка ACL 120 для IP на маршрутизаторе R1

Шаг 1. Убедитесь, что компьютер PC-C может получать доступ к PC-A по протоколу HTTPS с помощью веб-браузера.



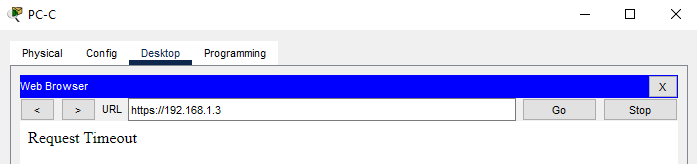
Шаг 2. Настройте список ACL 120 для разрешения и отклонения указанного трафика.



Шаг 3. Примените список ACL к интерфейсу S0/0/0.

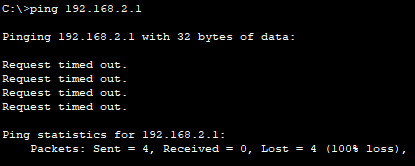


Шаг 4. Убедитесь, что компьютер PC-C не может получить доступ к PC-A по протоколу HTTPS с помощью веб-браузера.



Часть 4. Изменение существующего списка ACL на маршрутизаторе R1

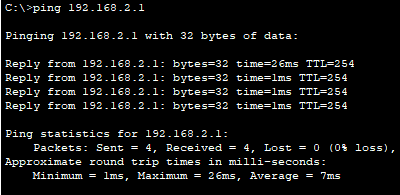
Шаг 1. Убедитесь, что компьютер PC-A не может успешно отправлять эхо-запросы интерфейсу loopback на маршрутизаторе R2.



Шаг 2. Внесите необходимые изменения в список ACL 120 для разрешения и отклонения указанного трафика.



Шаг 3. Убедитесь, что компьютер PC-A может успешно отправлять эхо-запросы интерфейсу loopback на маршрутизаторе R2.



Часть 5. Создание нумерованного списка ACL 110 для IP на маршрутизаторе R3

Шаг 1. Настройте список ACL 110 для разрешения только трафика из внутренней сети.

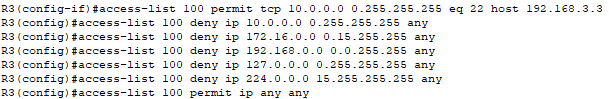


Шаг 2. Примените список ACL к интерфейсу G0/1.



Часть 6. Создание нумерованного списка ACL 100 для IP на маршрутизаторе R3

Шаг 1. Настройте список ACL 100 для блокировки всего указанного трафика из внешней сети.

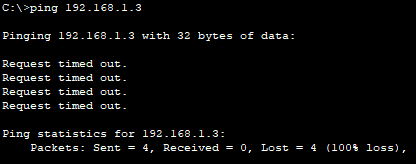


Шаг 2. Примените список ACL к интерфейсу Serial 0/0/1.



Шаг 3. Убедитесь, что указанный трафик, поступающий на интерфейс Serial 0/0/1, обрабатывается правильно.





**Шаг 4. Проверьте результаты.**

