Отчёт по лабораторной работе №10

Администрирование локальных сетей

Ищенко Ирина НПИбд-02-22

Содержание

# 1 Цель работы

Освоить настройку прав доступа пользователей к ресурсам сети [1].

# 2 Задание

1. Требуется настроить следующие правила доступа:
2. web-сервер: разрешить доступ всем пользователям по протоколу HTTP через порт 80 протокола TCP, а для администратора открыть доступ по протоколам Telnet и FTP;
3. файловый сервер: с внутренних адресов сети доступ открыт по портам для общедоступных каталогов, с внешних — доступ по протоколу FTP;
4. почтовый сервер: разрешить пользователям работать по протоколам SMTP и POP3 (соответственно через порты 25 и 110 протокола TCP), а для администратора — открыть доступ по протоколам Telnet и FTP;
5. DNS-сервер: открыть порт 53 протокола UDP для доступа из внутренней сети;
6. разрешить icmp-сообщения, направленные в сеть серверов;
7. запретить для сети Other любые запросы за пределы сети, за исключением администратора;
8. разрешить доступ в сеть управления сетевым оборудованием только администратору сети.
9. Требуется проверить правильность действия установленных правил доступа.
10. Требуется выполнить задание для самостоятельной работы по настройке прав доступа администратора сети на Павловской.

# 3 Выполнение лабораторной работы

В рабочей области проекта подключим ноутбук администратора с именем admin к сети к other-donskaya-1 с тем, чтобы разрешить ему потом любые действия, связанные с управлением сетью. Для этого подсоединим ноутбук к порту 24 коммутатора msk-donskaya-sw-4 (рис. 1) и присвоим ему статический адрес 10.128.6.200 (рис. 2), указав в качестве gateway-адреса 10.128.6.1 и адреса DNS-сервера 10.128.0.5 (рис. 3).

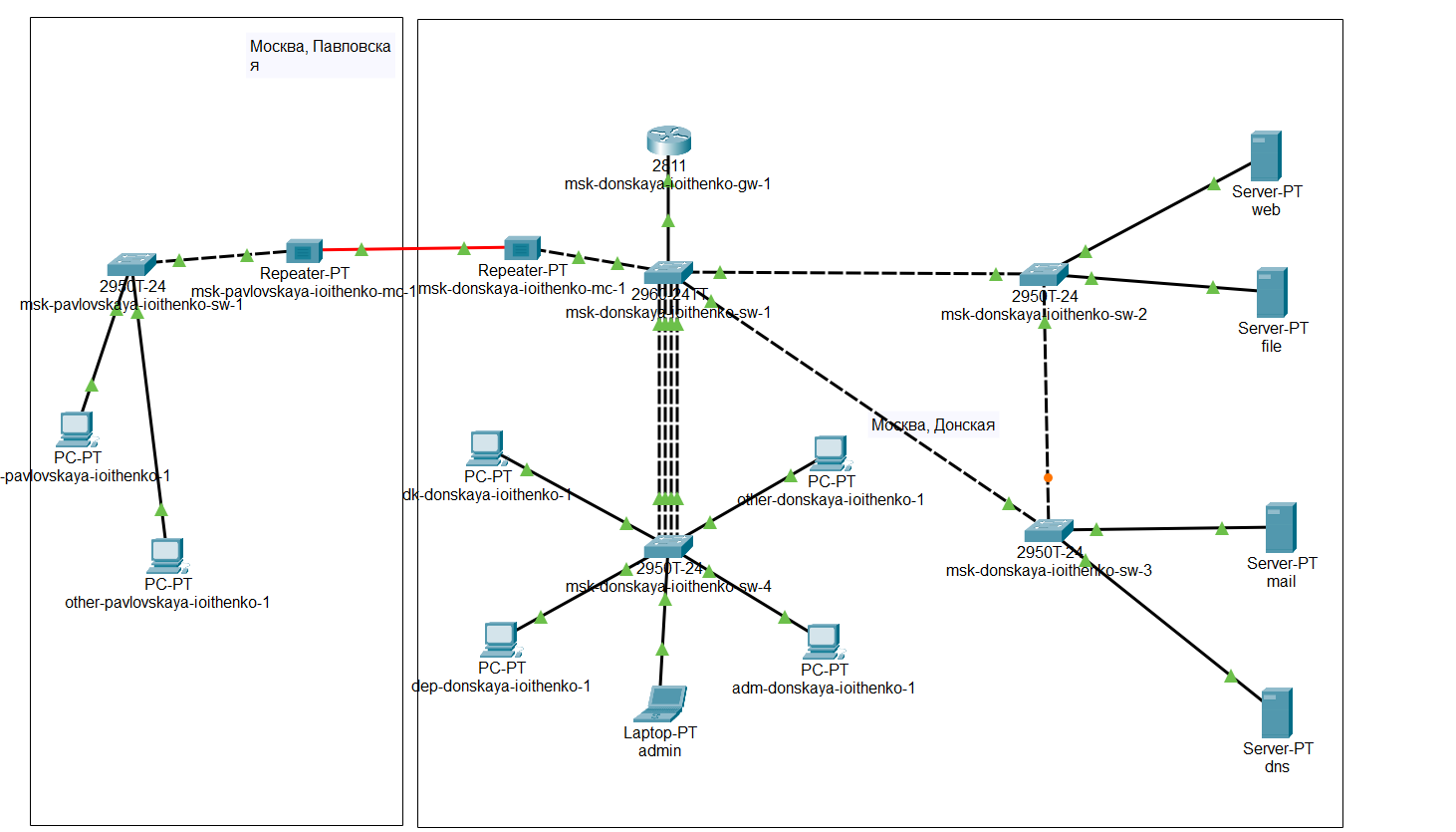


Рис. 1: Добавление ноутбука

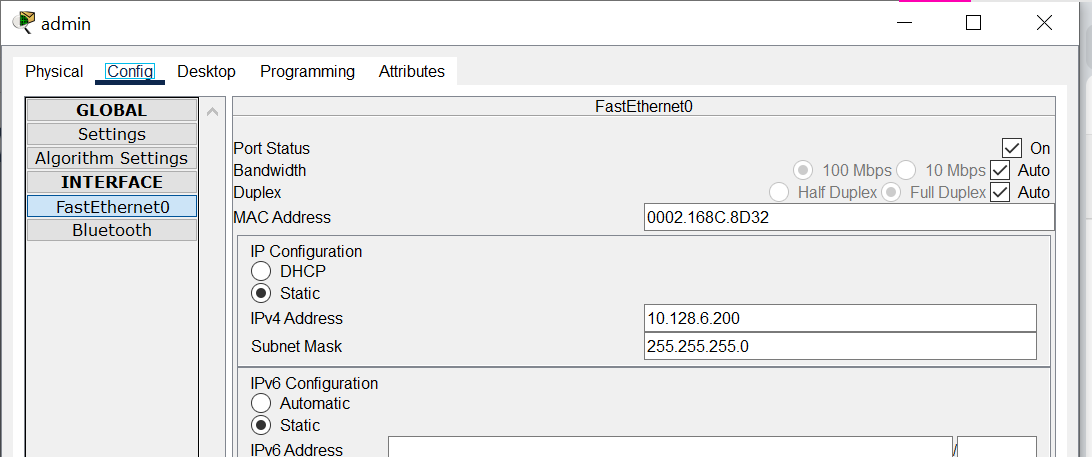


Рис. 2: IP

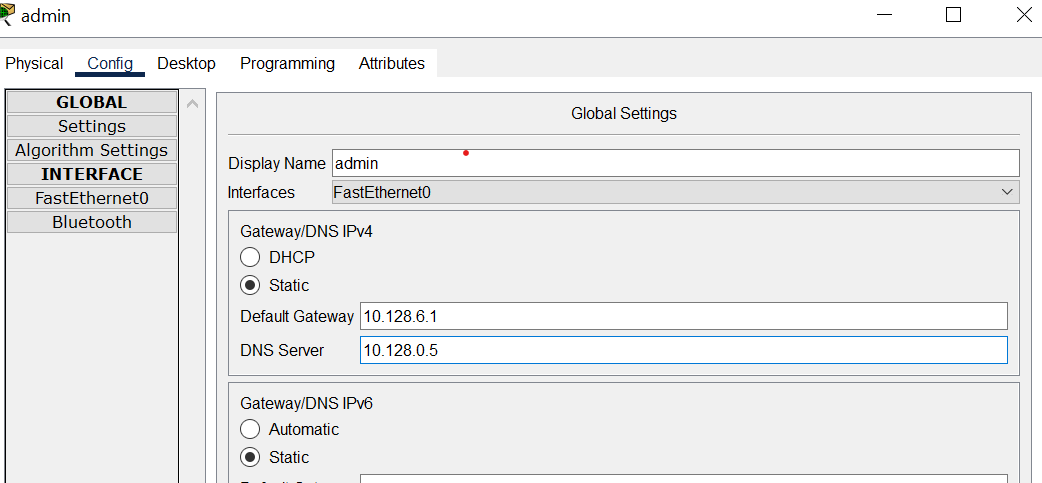


Рис. 3: Шлюз и адрес DNS-сервера

Проверим доступность устройств до настройки маршрутизатора (рис. 4).

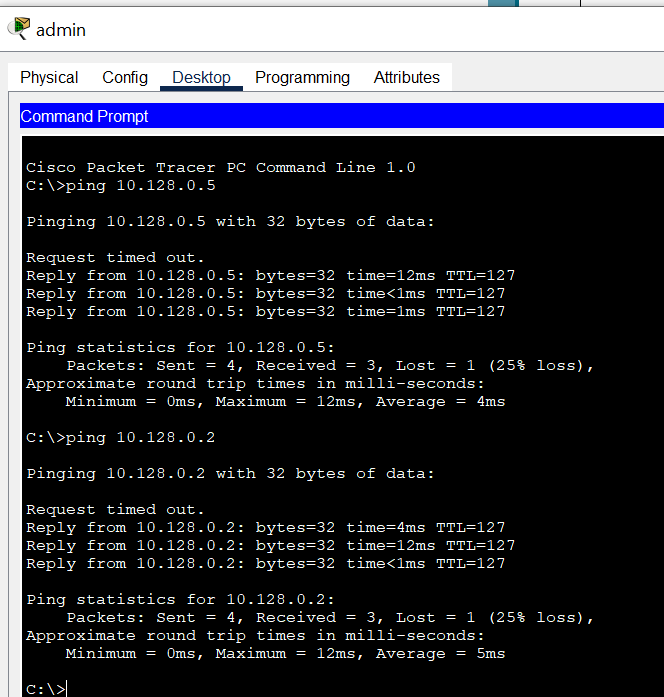


Рис. 4: Проверка пинга до настройки

Настроим доступа к web-серверу по порту tcp 80 (рис. 5).

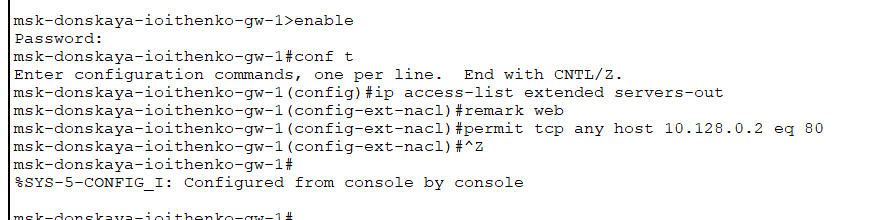


Рис. 5: Доступ к web-серверу по tcp 80

Добавим список управления доступом к интерфейсу (рис. 6).

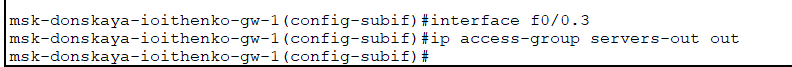


Рис. 6: Список управления доступом к интерфейсу

Проверим, что доступ к web-серверу есть через протокол HTTP (введя в строке браузера хоста ip-адрес web-сервера) (рис. 3).

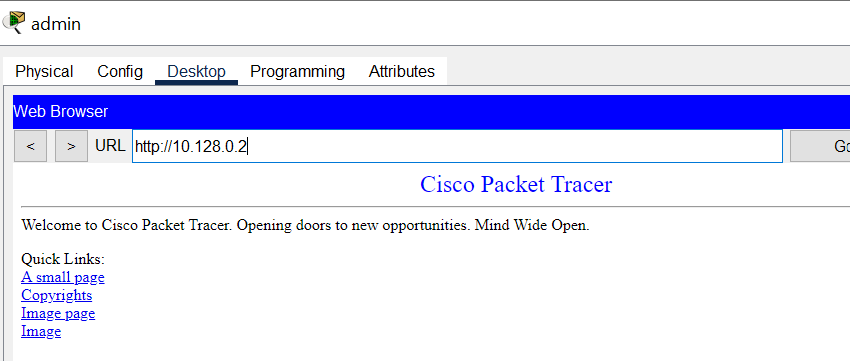


Рис. 7: Проверка доступа по HTTP

При этом команда ping будет демонстрировать недоступность web-сервера как по имени, так и по ip-адресу web-сервера (рис. 8).

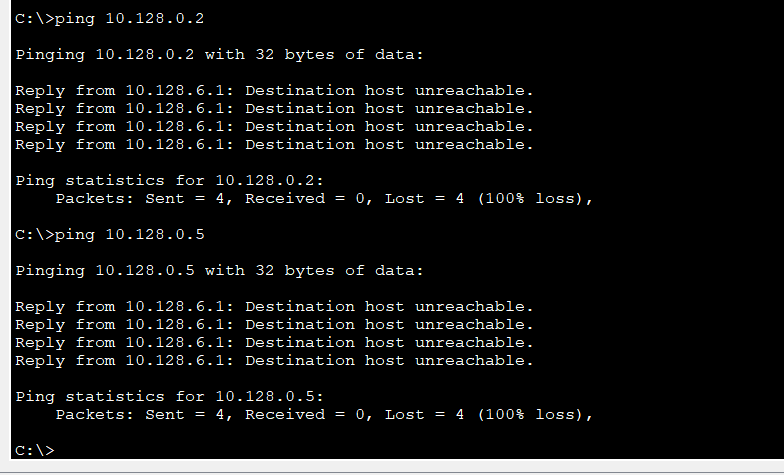


Рис. 8: Проверка пингом

Настроим дополнительный доступ для администратора по протоколам Telnet и FTP (рис. 9).

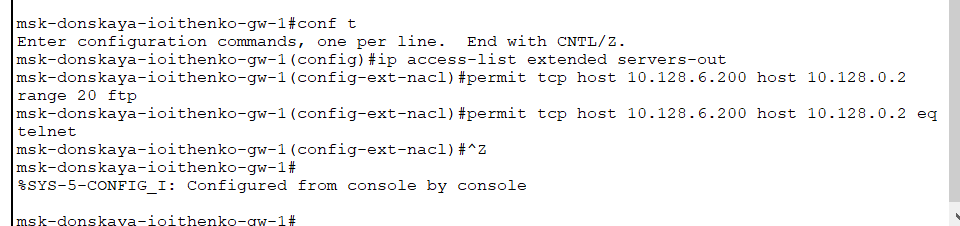


Рис. 9: Доступ для admin по Telnet и FTP

Убедимся, что с узла с ip-адресом 10.128.6.200 есть доступ по протоколу FTP. Для этого в командной строке устройства администратора введем ftp 10.128.0.2, а затем по запросу имя пользователя cisco и пароль cisco (рис. 10).

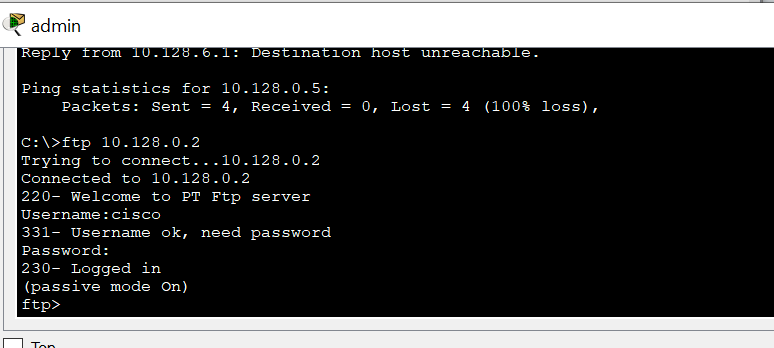


Рис. 10: Проверка FTP

Попробуем провести аналогичную процедуру с другого устройства сети. Убедимся, что доступ будет запрещён (рис. 11).

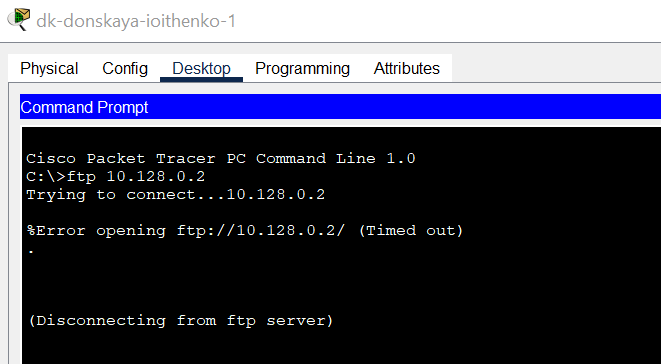


Рис. 11: Проверка FTP

Настроим доступ к файловому серверу. Настроим доступ к почтовому серверу, доступ к DNS-серверу. Разрешим icmp-запросы (рис. 12).

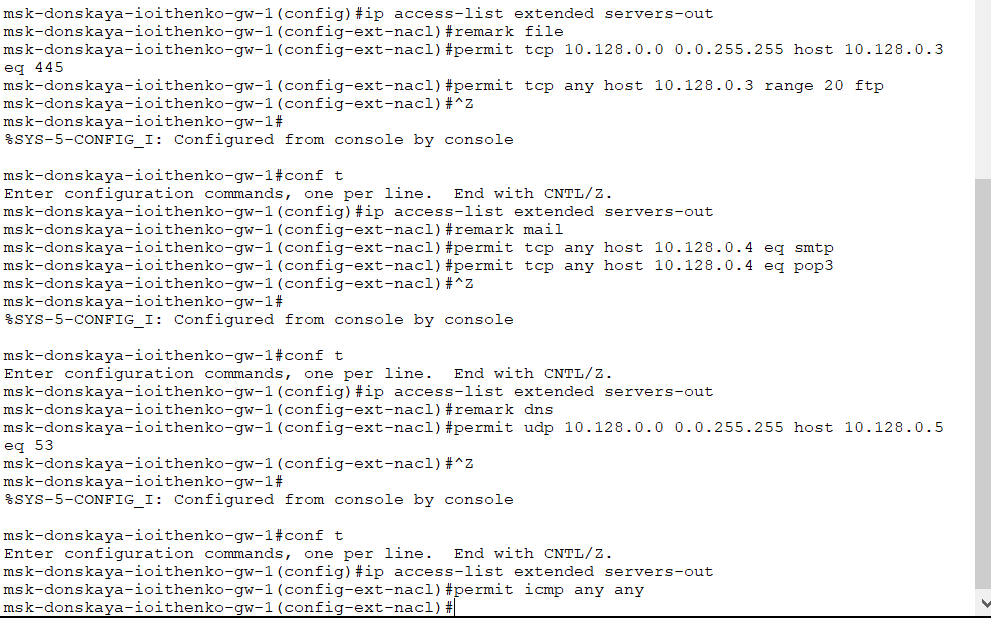


Рис. 12: Файловый, почтовый и DNS сервер

Настроим доступ для сети Other (требуется наложить ограничение на исходящий из сети Other трафик, который по отношению к маршрутизатору msk-donskaya-gw-1 является входящим трафиком) (рис. 13).

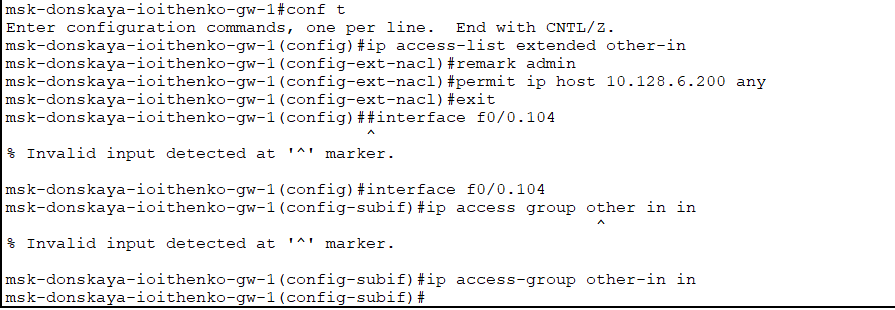


Рис. 13: Доступ для сети Other

Настроим доступ администратора к сети сетевого оборудования (рис. 14).

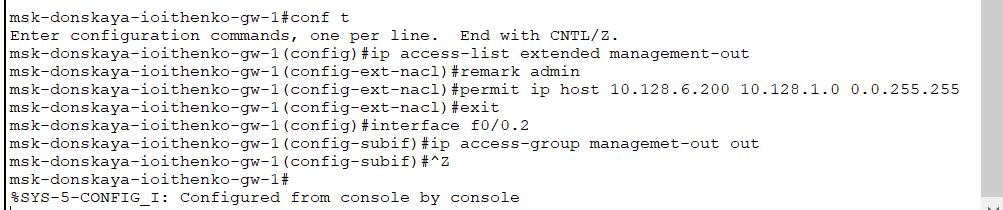


Рис. 14: Доступ к сети сетевого оборудования

Проверим корректность установленных правил доступа, попытавшись получить доступ по различным протоколам с разных устройств сети к подсети серверов и подсети сетевого оборудования. Откроем терминал dep-donskaya-1 и пропингуем разные устройства. Увидим, что серверы и другие оконечные устройства пингуются, однако к сетевому оборудованию доступа нет, как и должно быть. (рис. 15).

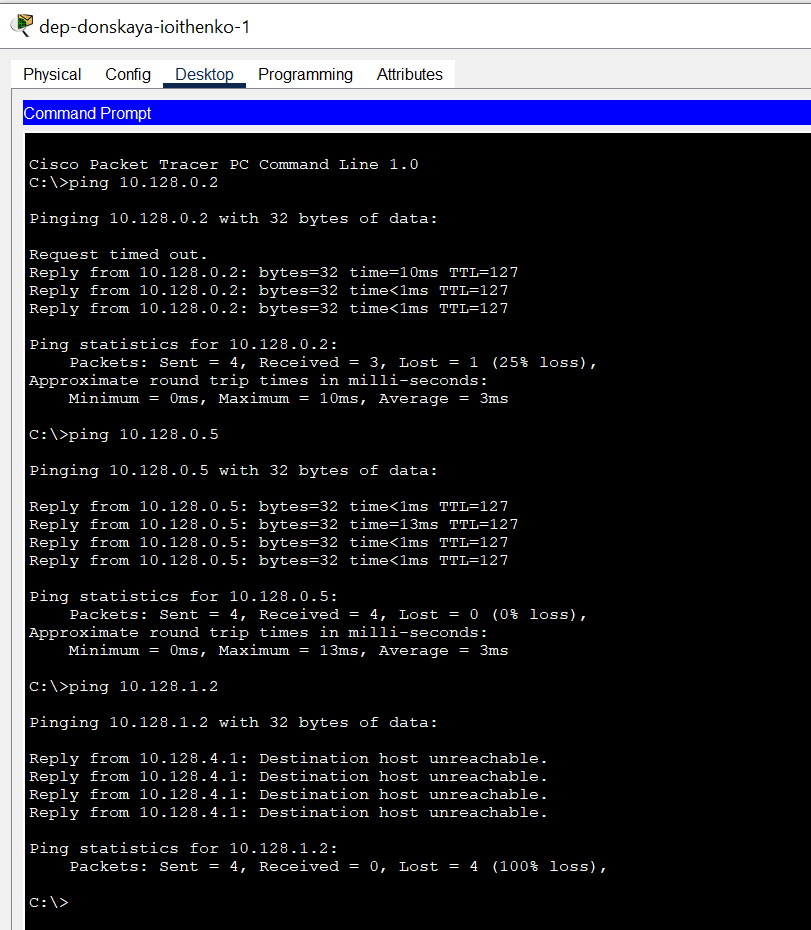


Рис. 15: Проверка доступа

Откроем терминал dk-donskaya-dmbelicheva-1 и пропингуем разные устройства. Увидим, что серверы и другие оконечные устройства пингуются, однако к сетевому оборудованию доступа нет, как и должно быть. Также попробуем подключится к web-серверу по ftp, доступ закрыт (рис. 16).

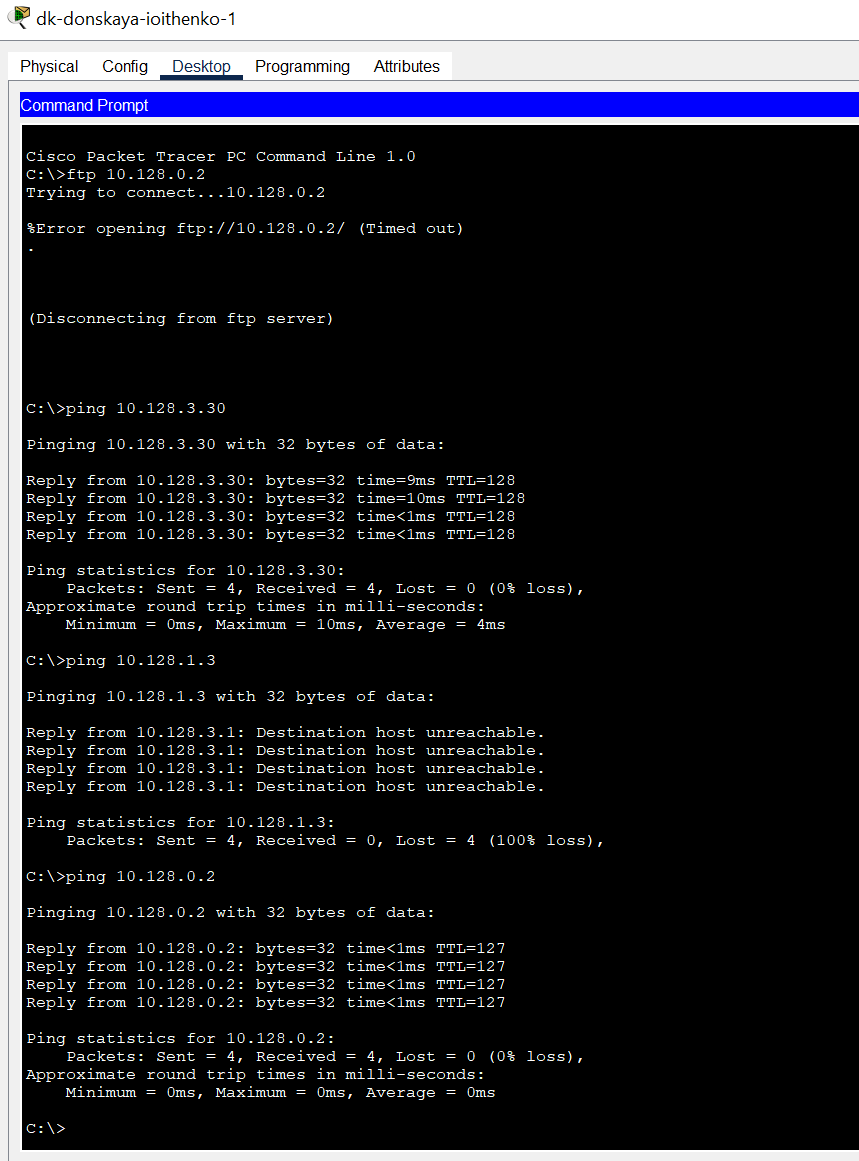


Рис. 16: Проверка доступа

Теперь проверим корректность настроенного доступа с admin. Есть доступ к серверу по ftp, а также успешно пингуется сетевое оборудование (рис. 17).

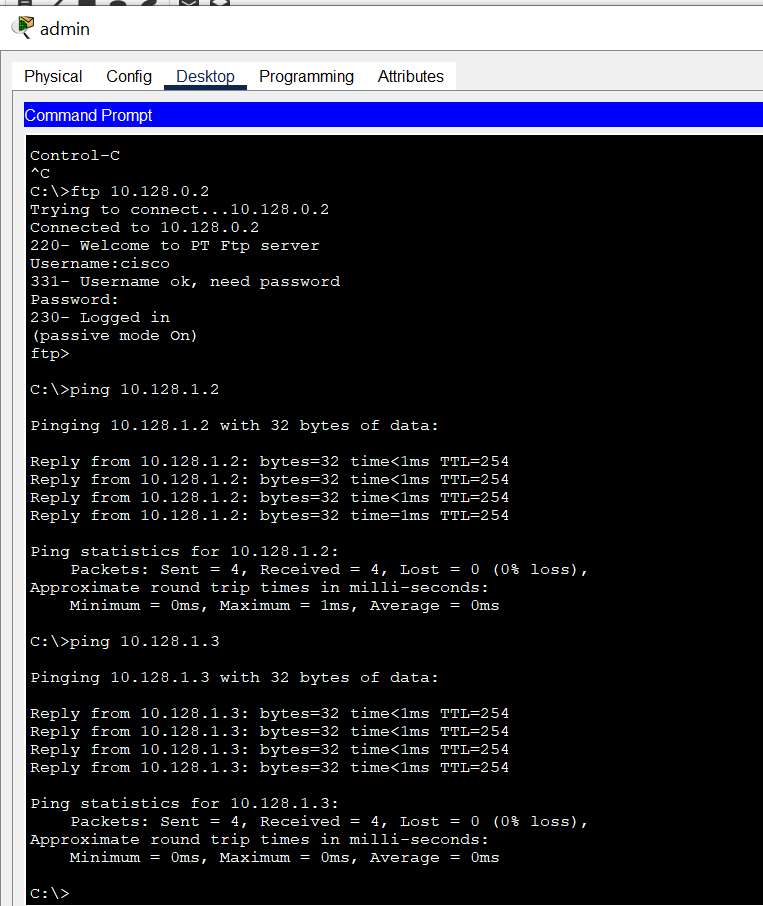


Рис. 17: Проверка доступа

Разместим еще один ноутбук admin на Павловской (рис. 18).

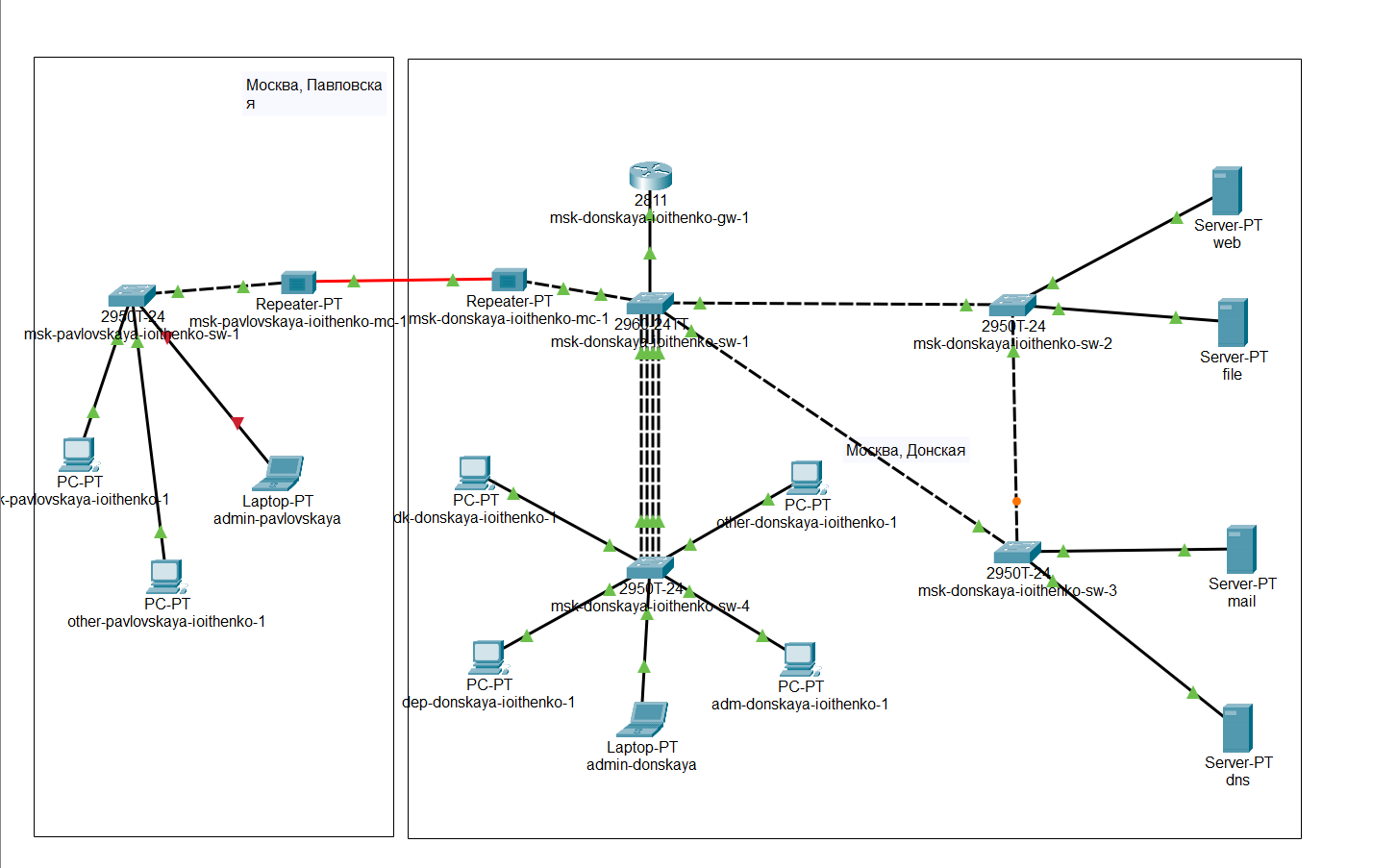


Рис. 18: Размещение устройства

Разрешим администратору из сети Other на Павловской действия, аналогичные действиям администратора сети Other на Донской (рис. 19).

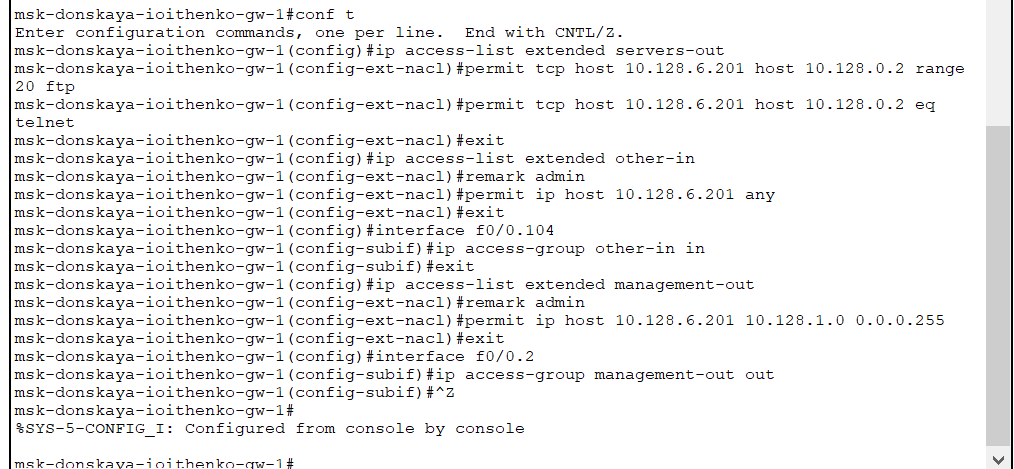


Рис. 19: Правила

Просмотрим список правил в нашей сети. После выполнения была изменена обратная маска в правилах для их корректной работы (рис. 20).

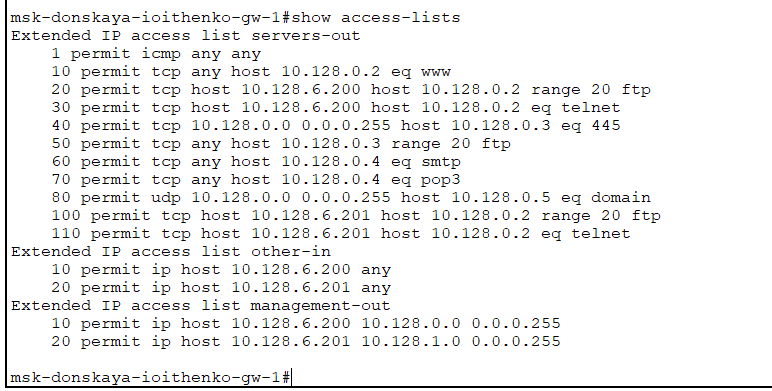


Рис. 20: Список правил

Проверим работу устройства администратора (рис. 21).

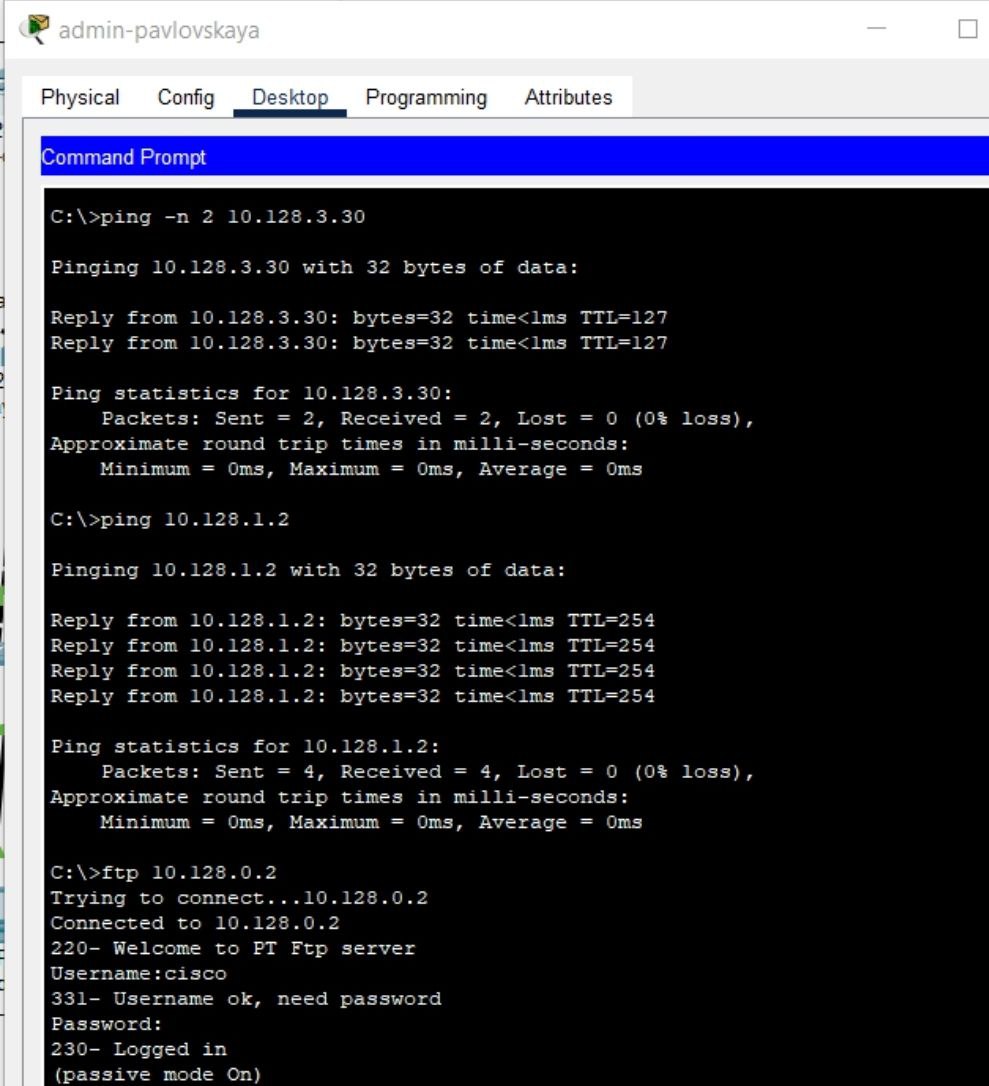


Рис. 21: Проверка

# 4 Выводы

В ходе выполнения лабораторной работы я освоила настройку прав доступа пользователей к ресурсам сети.

# 5 Контрольные вопросы

1. Как задать действие правила для конкретного протокола?

Например, permit tcp any host 10.128.0.4 eq pop3.

1. Как задать действие правила сразу для нескольких портов?

Для этого нужна команда interface range.

1. Как узнать номер правила в списке прав доступа?

С помощью команды show access-lists.

1. Каким образом можно изменить порядок применения правил в списке контроля доступа?

Команда access-list <номер в списке> permit.

# Список литературы

1. Королькова А. В. К.Д.С. Администрирование сетевых подсистем. Лабораторный практикум : учебное пособие. Москва: РУДН, 2021. 137 с.