Лабораторная работа №10

Администрирование локальных сетей

Мишина Анастасия Алексеевна

Содержание

# 1 Цель работы

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

# 2 Задание

1. Требуется настроить следующие правила доступа:
   * web-сервер: разрешить доступ всем пользователям по протоколу HTTP через порт 80 протокола TCP, а для администратора открыть доступ по протоколам Telnet и FTP;
   * файловый сервер: с внутренних адресов сети доступ открыт по портам для общедоступных каталогов, с внешних — доступ по протоколу FTP;
   * 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;
   * DNS-сервер: открыть порт 53 протокола UDP для доступа из внутренней сети;
   * разрешить icmp-сообщения, направленные в сеть серверов;
   * запретить для сети Other любые запросы за пределы сети, за исключением администратора;
   * разрешить доступ в сеть управления сетевым оборудованием только администратору сети.
2. Требуется проверить правильность действия установленных правил доступа.
3. Требуется выполнить задание для самостоятельной работы по настройке прав доступа администратора сети на Павловской.
4. При выполнении работы необходимо учитывать соглашение об именовании.

# 3 Выполнение лабораторной работы

В рабочей области проекта подключим ноутбук администратора с именем admin к сети к other-donskaya-1 (рис. 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 и присвоим ему статический адрес 10.128.6.200, указав в качестве gateway-адреса 10.128.6.1 (рис. 2) и адреса DNS-сервера 10.128.0.5 (рис. 3).

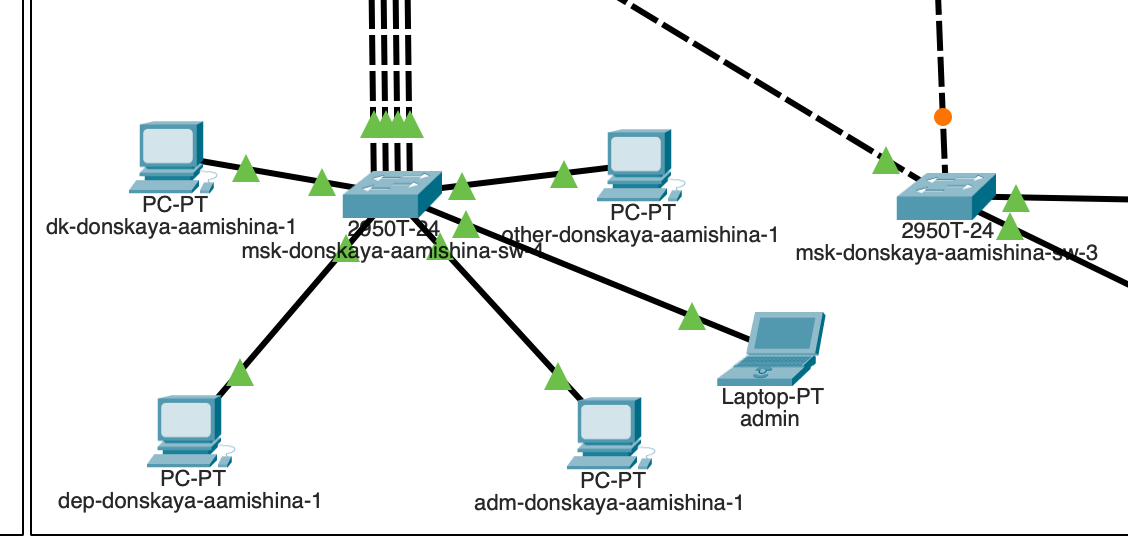


Рис. 1: Размещение ноутбука администратора в сети other-donskaya-1

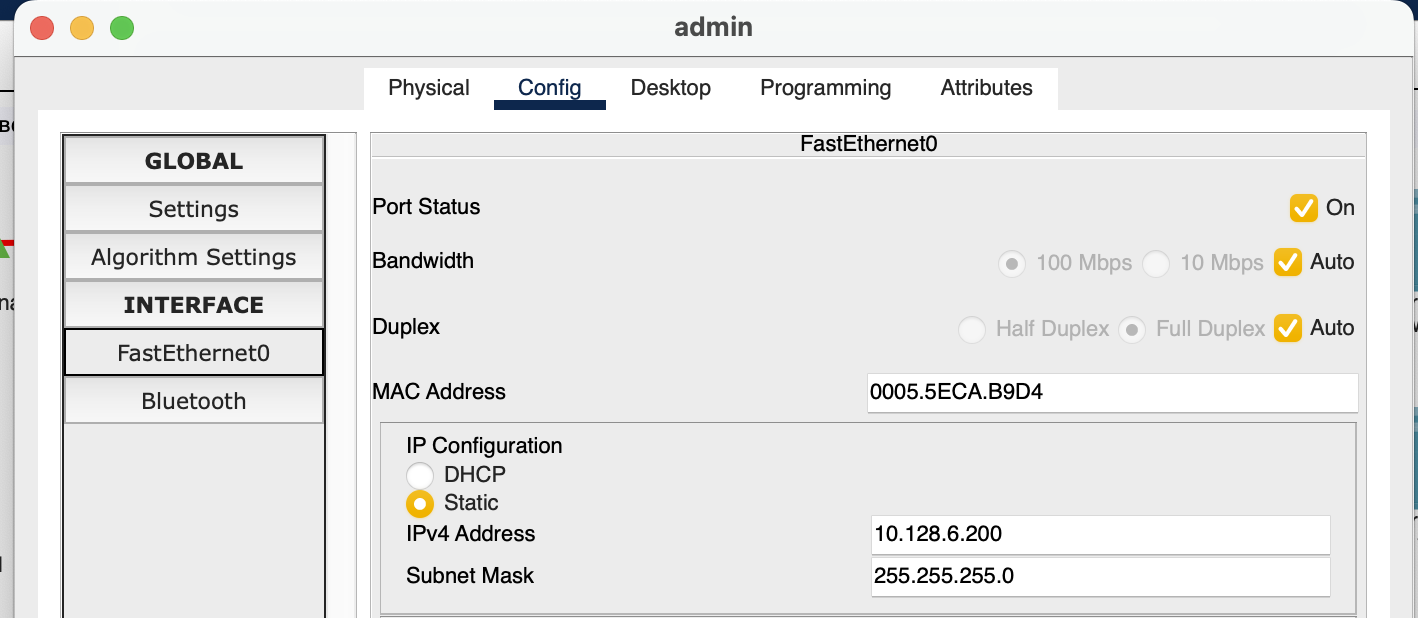


Рис. 2: Задание статического ip-адреса ноутбуку admin

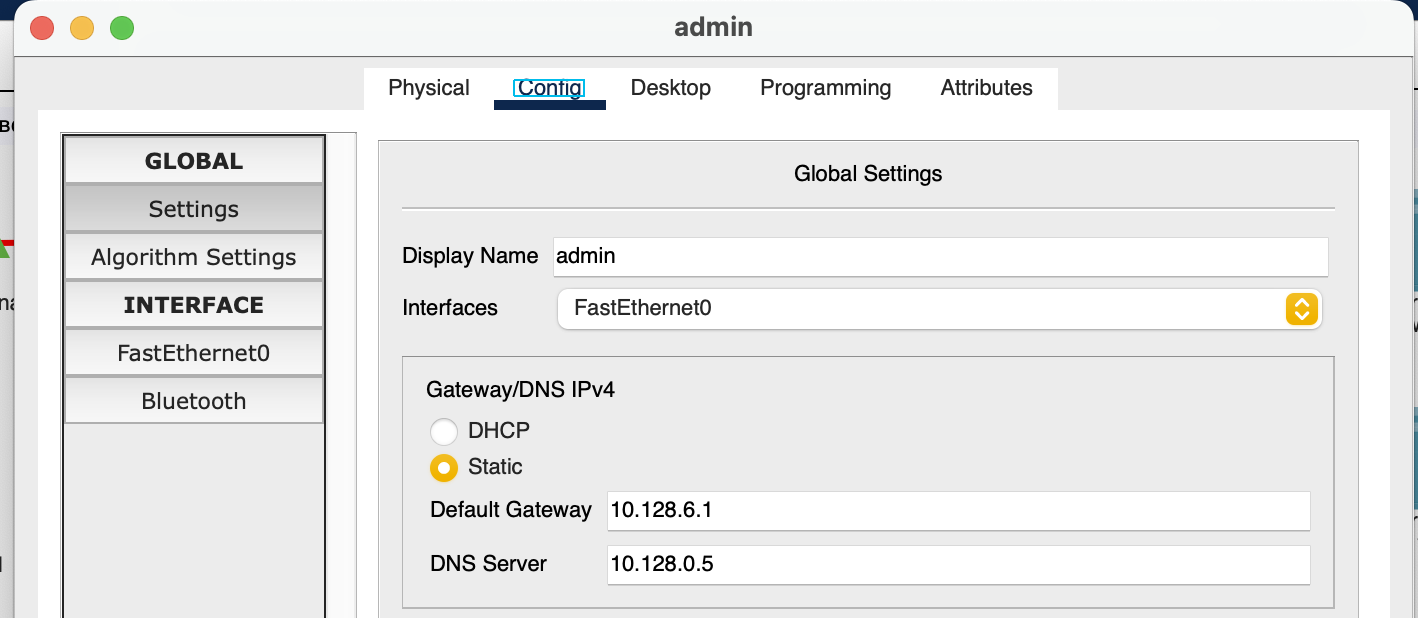


Рис. 3: Задание gateway-адреса и адреса DNS-сервера ноутбуку admin

Проверим, что у ноутбука корректно работает соединение через пингование разных устройств сети, например серверов (рис. 4).

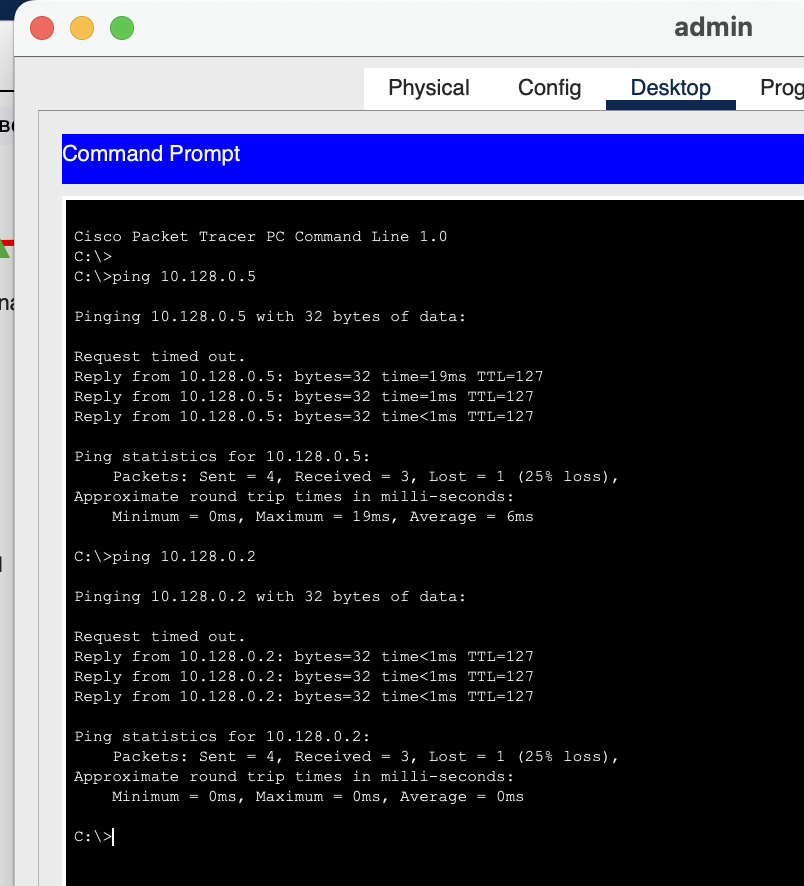


Рис. 4: Проверка работоспособности соединения ноутбука admin

На оборудовании Cisco правила в списке доступа проверяются по порядку сверху вниз до первого совпадения — как только одно из правил сработало, проверка списка правил прекращается и обработка трафика происходит на основе сработавшего правила. Поэтому сначала мы надо давать разрешение (permit) на какое-то действие, а уже потом накладывать ограничения (deny). Настроим доступ к web-серверу по порту tcp 80. Мы создаем список контроля доступа с названием servers-out (так как предполагается ограничить доступ в конкретные подсети и по отношению к маршрутизатору это будет исходящий трафик); указано (в качестве комментария-напоминания remark web), что ограничения предназначены для работы с web-сервером, а также даем разрешение доступа (permit) по протоколу TCP всем (any) пользователям сети (host) на доступ к web-серверу, имеющему адрес 10.128.0.2, через порт 80. Добавим список управления доступом к интерфейсу. К интерфейсу f0/0.3 подключается список прав доступа servers-out и применяется к исходящему трафику (out) (рис. 5).

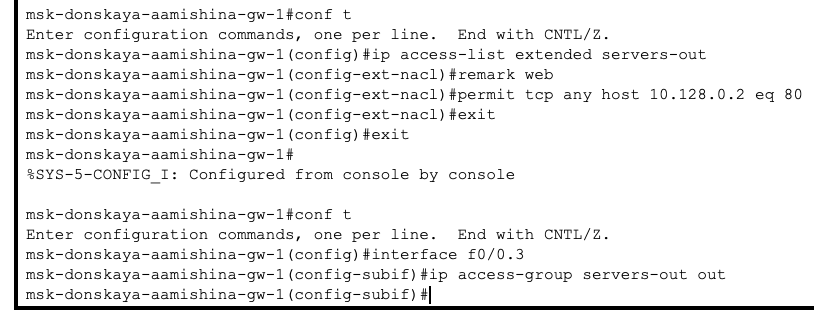


Рис. 5: Настройка доступа к web-серверу по порту tcp 80, добавление списка управления доступом к интерфейсу

Проверим, что доступ к web-серверу есть через протокол HTTP, введя в строке браузера хоста ip-адрес web-сервера (рис. 6). При этом команда ping будет демонстрировать недоступность web-сервера как по имени, так и по ip-адресу web-сервера (рис. 7).

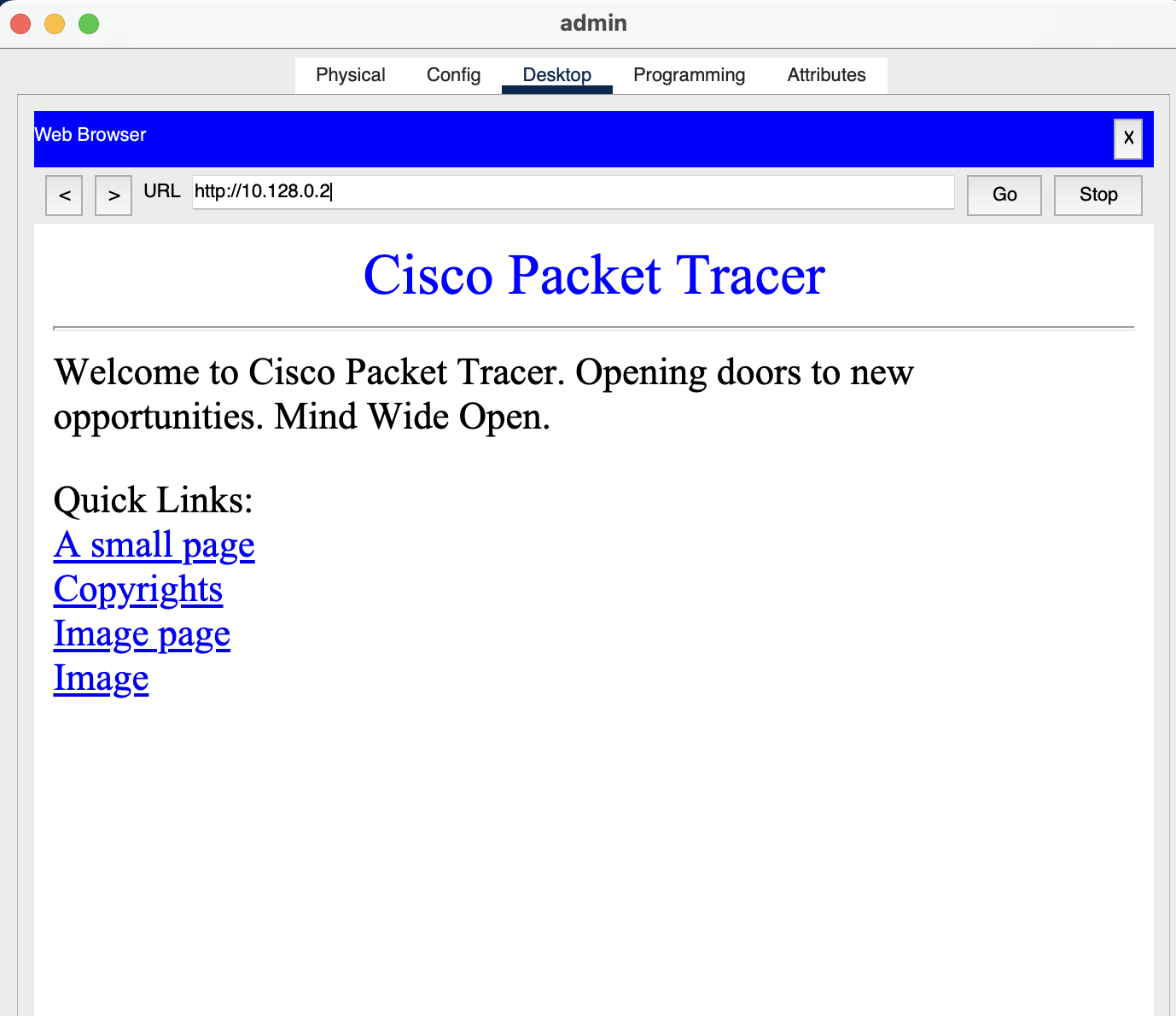


Рис. 6: Проверка доступа к web-серверу через протокол HTTP

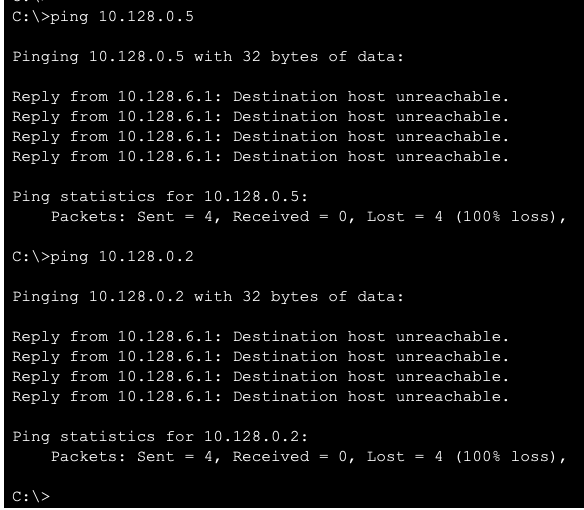


Рис. 7: Проверка недоступности web-сервера через ping

Настроим дополнительный доступ для администратора по протоколам Telnet и FTP. В список контроля доступа servers-out добавлено правило, разрешающее устройству администратора с ip-адресом 10.128.6.200 доступ на web-сервер (10.128.0.2) по протоколам FTP и telnet (рис. 8).

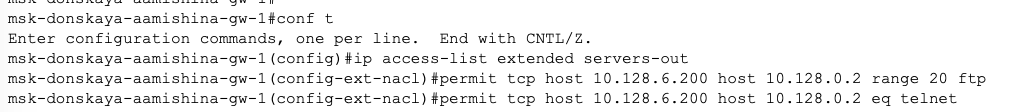


Рис. 8: Настройка дополнительного доступа для администратора по протоколам Telnet и FTP

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, увидим, что доступ действительно есть (рис. 9).

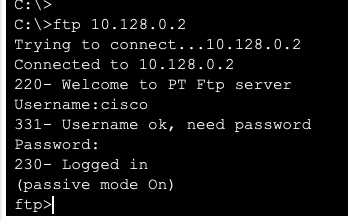


Рис. 9: Проверка работы FTP у администратора

Попробуем провести аналогичную процедуру с другого устройства сети. Увидим, что доступ запрещён (рис. 10).

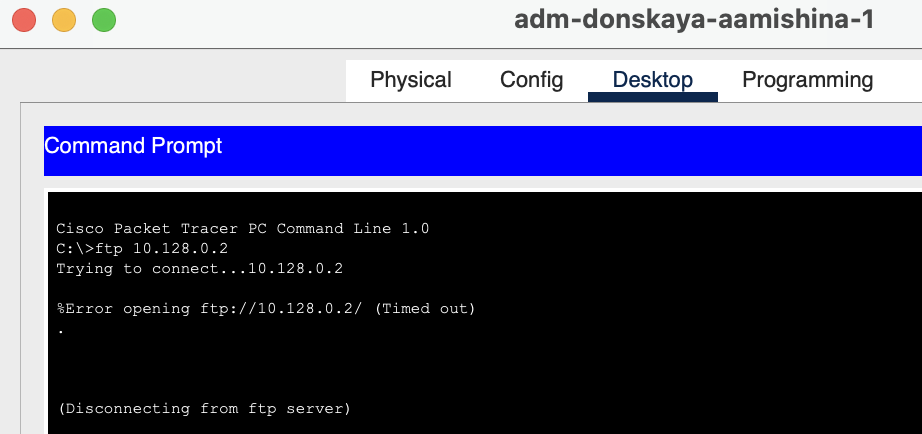


Рис. 10: Проверка недоступности подключения по FTP с другого устройства сети

Настроим доступ к файловому серверу. В списке контроля доступа servers-out указано (в качестве комментария-напоминания remark file), что следующие ограничения предназначены для работы с file-сервером; всем узлам внутренней сети (10.128.0.0) разрешён доступ по протоколу SMB (работает через порт 445 протокола TCP) к каталогам общего пользования; любым узлам разрешён доступ к file-серверу по протоколу FTP. Запись 0.0.255.255 — обратная маска (wildcard mask). Настроим доступ к почтовому серверу. В списке контроля доступа servers-out указано (в качестве комментария-напоминания remark mail), что следующие ограничения предназначены для работы с почтовым сервером; всем разрешён доступ к почтовому серверу по протоколам POP3 и SMTP. Настроим доступ к DNS-серверу. В списке контроля доступа servers-out указано (в качестве комментария-напоминания remark dns), что следующие ограничения предназначены для работы с DNS-сервером; всем узлам внутренней сети разрешён доступ к DNS-серверу через UDP-порт 53 (рис.11).

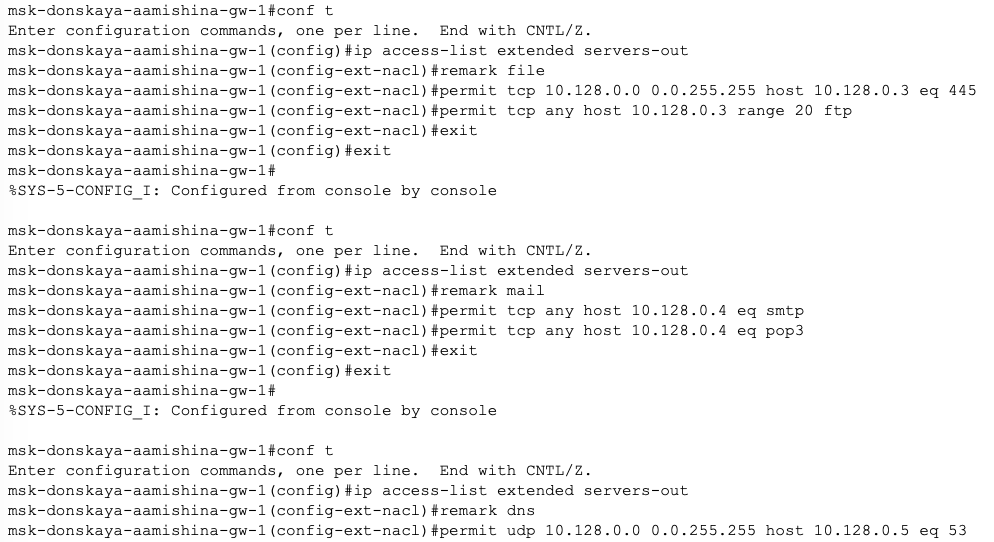


Рис. 11: Настройка доступа к файловому серверу, почтовому серверу и к DNS-серверу

Проверим доступность web-сервера (через браузер) по имени (рис.12) и по ip-адресу (рис.13).

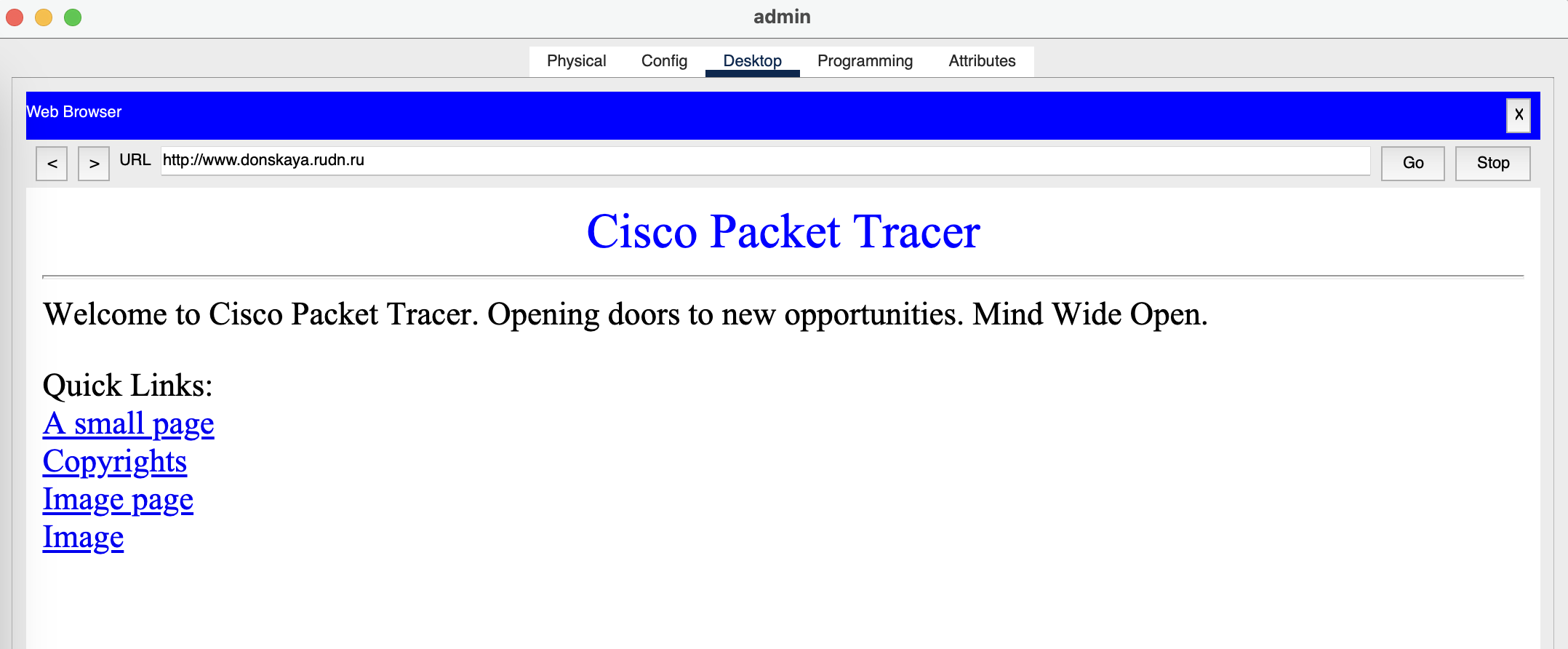


Рис. 12: Проверка доступности web-сервера по имени

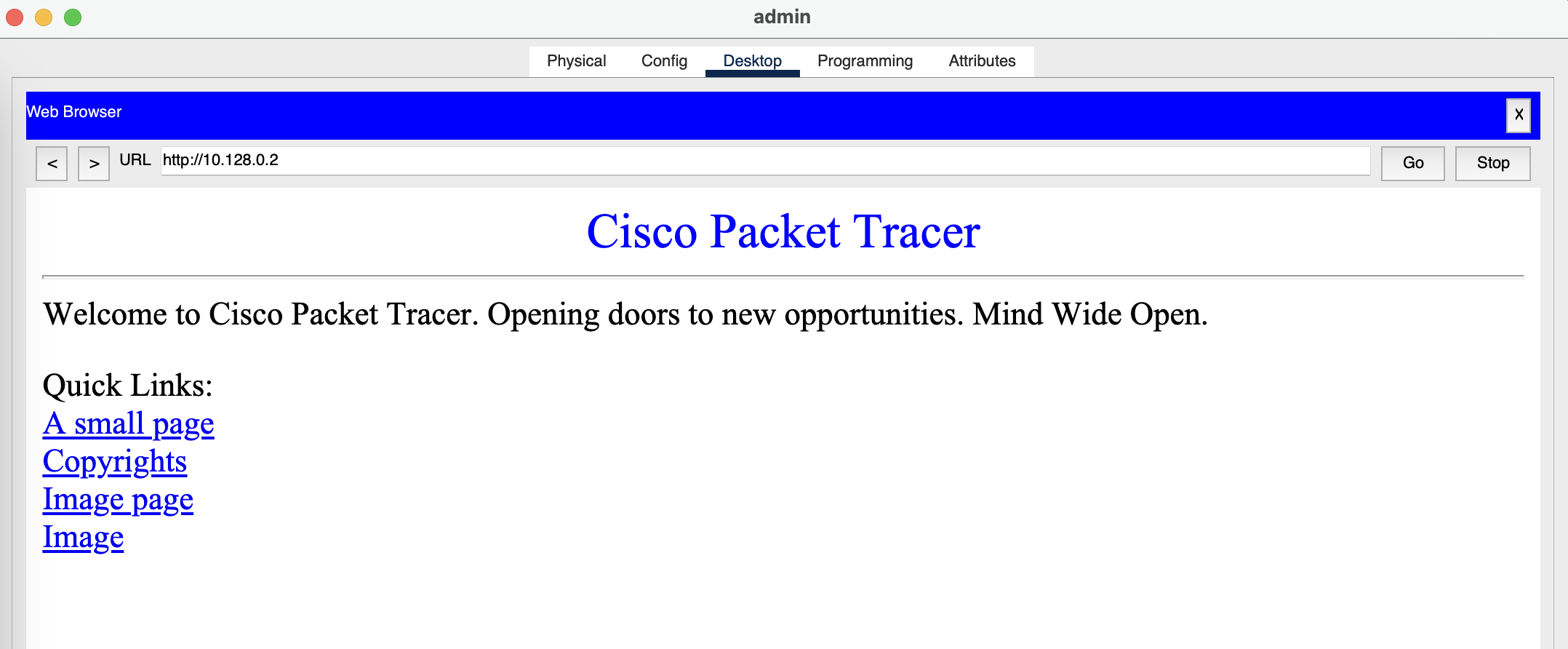


Рис. 13: Проверка доступности web-сервера по ip-адресу

Разрешим icmp-запросы. Посмотрим номера строк правил в списке контроля доступа (рис.14).

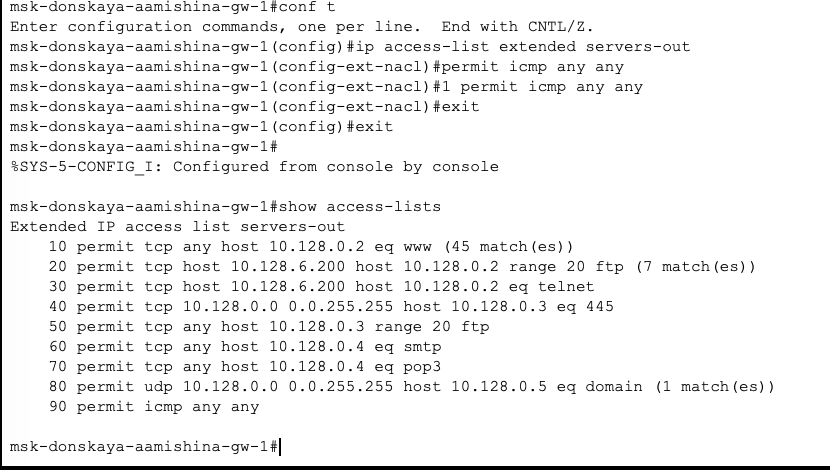


Рис. 14: Разрешение icmp-запросов и просмотр строк правил в списке контроля доступа

Настроим доступ для сети Other. Наложим ограничение на исходящий из сети Other трафик, который по отношению к маршрутизатору msk-donskaya-gw-1 является входящим трафиком. В списке контроля доступа other-in указано, что следующие правила относятся к администратору сети; даётся разрешение устройству с адресом 10.128.6.200 на любые действия (any); к интерфейсу f0/0.104 подключается список прав доступа other-in и применяется к входящему трафику (in). Настроим доступ администратора к сети сетевого оборудования. В списке контроля доступа management-out указано (в качестве комментария-напоминания remark admin), что устройству администратора с адресом 10.128.6.200 разрешён доступ к сети сетевого оборудования (10.128.1.0); к интерфейсу f0/0.2 подключается список прав доступа management-out и применяется к исходящему трафику (out) (рис.15).

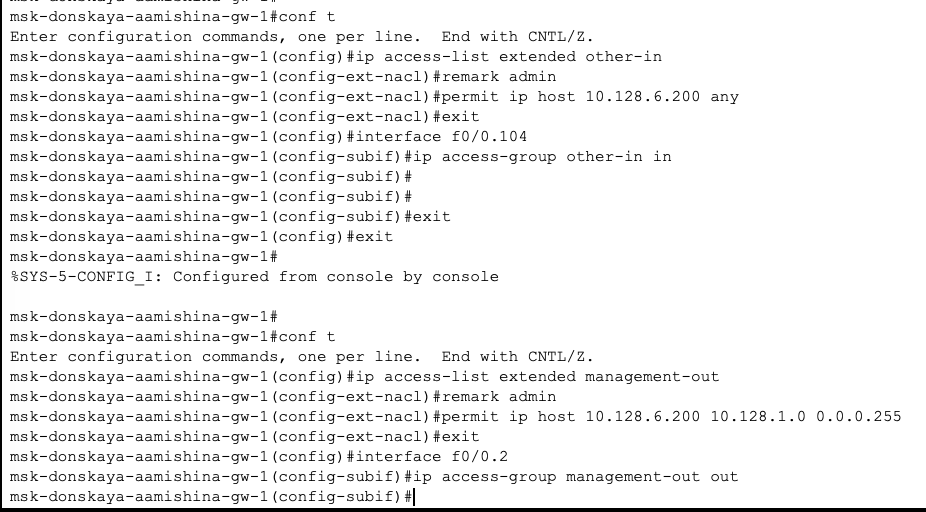


Рис. 15: Настройка доступа для сети Other и доступа администратора к сети сетевого оборудования

# 4 Самостоятельная работа

1. 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-aamishina-1 и пропингуем разные устройства. Увидим, что серверы и другие оконечные устройства пингуются, однако к сетевому оборудованию доступа нет, как и должно быть (рис.16).

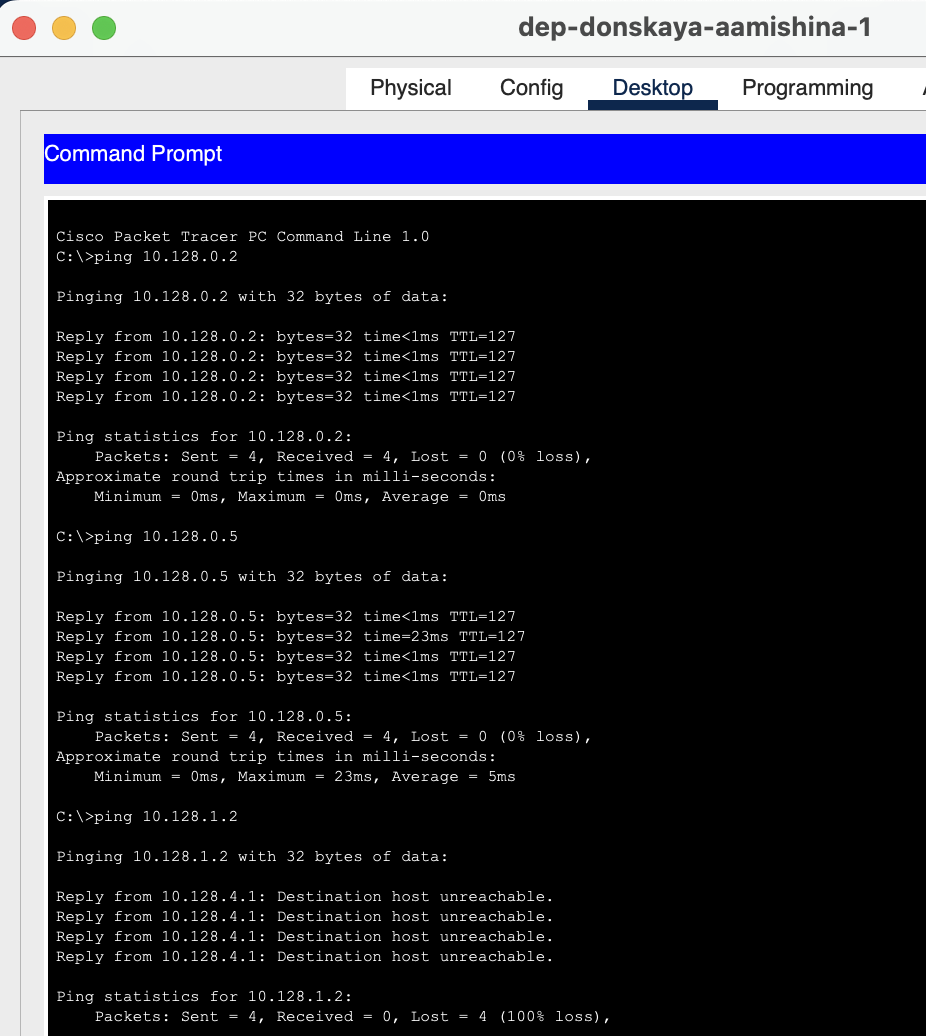


Рис. 16: Пингование устройств с dep-donskaya-aamishina-1

Откроем терминал dk-donskaya-aamishina-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.17).

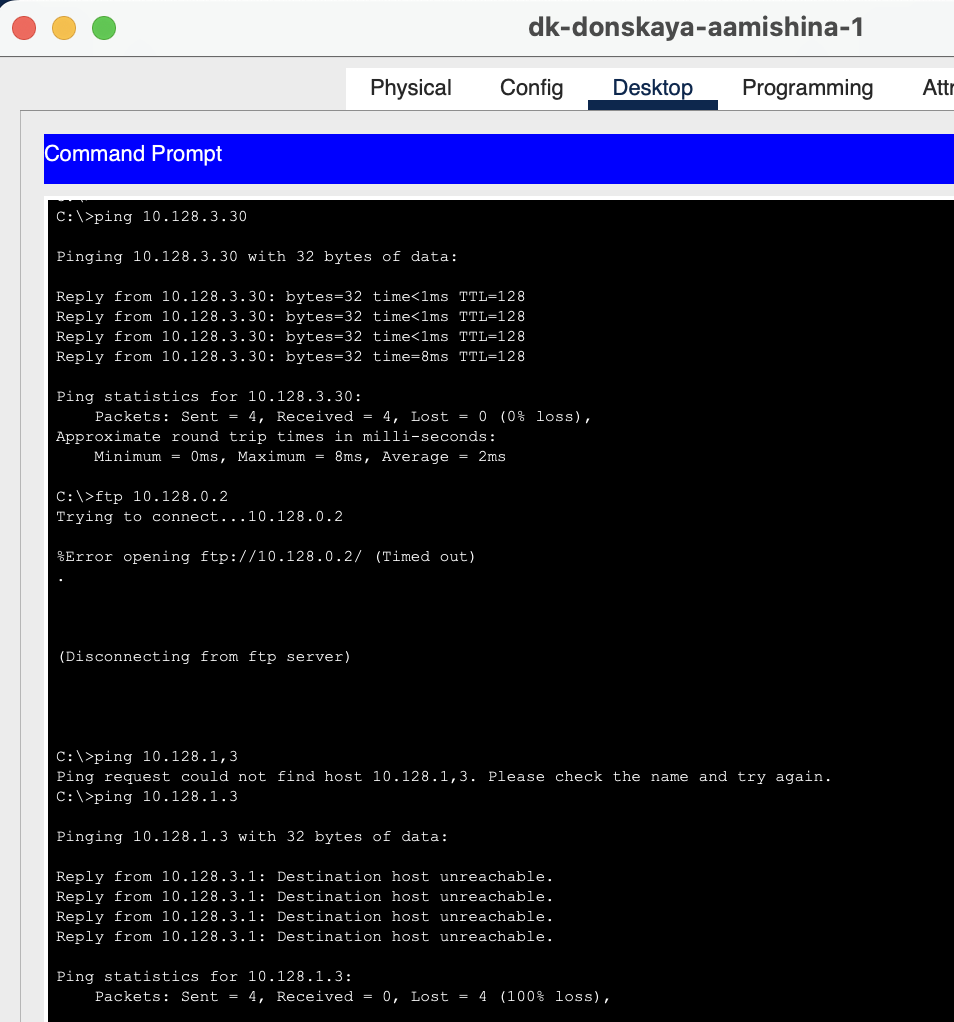


Рис. 17: Пингование устройств с dk-donskaya-aamishina-1

Теперь проверим корректность настроенного доступа с admin. Есть доступ к серверу по ftp, а также успешно пингуется сетевое оборудование (рис.18).

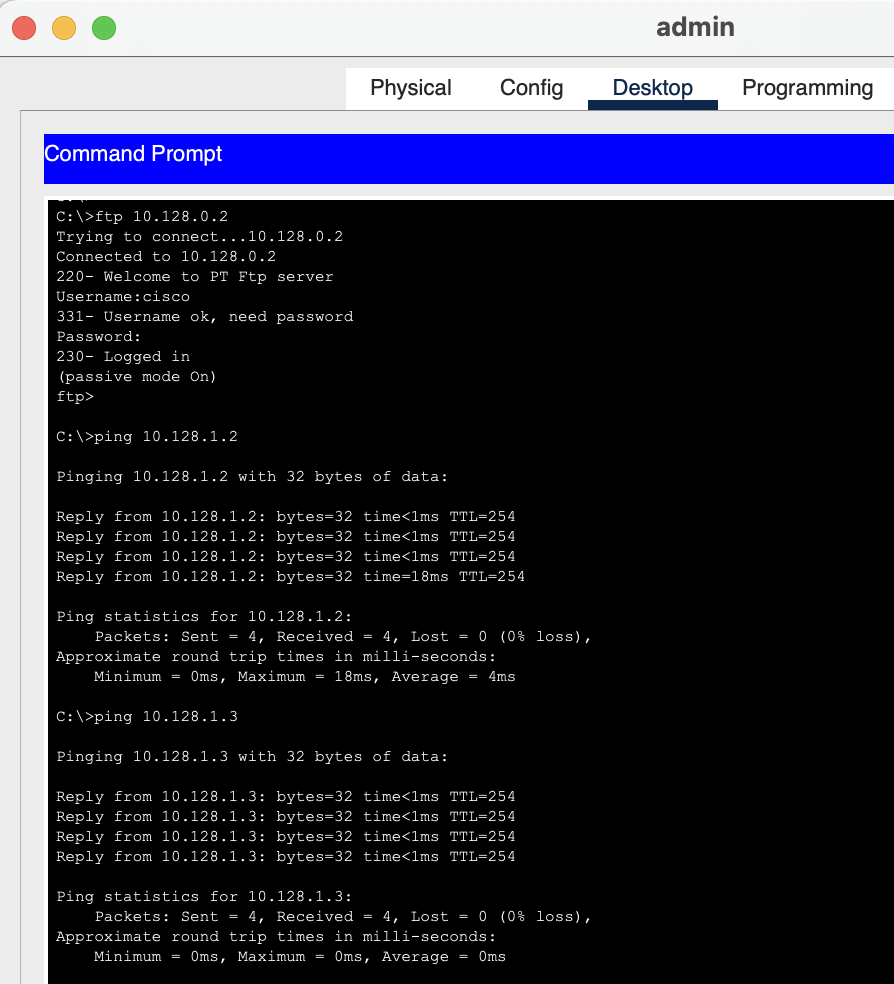


Рис. 18: Пингование устройств с admin

1. Разрешим администратору из сети Other на Павловской действия, аналогичные действиям администратора сети Other на Донской.

Разместим в рабочей области ноутбук admin-pavlovskaya на Павловской (рис.19).

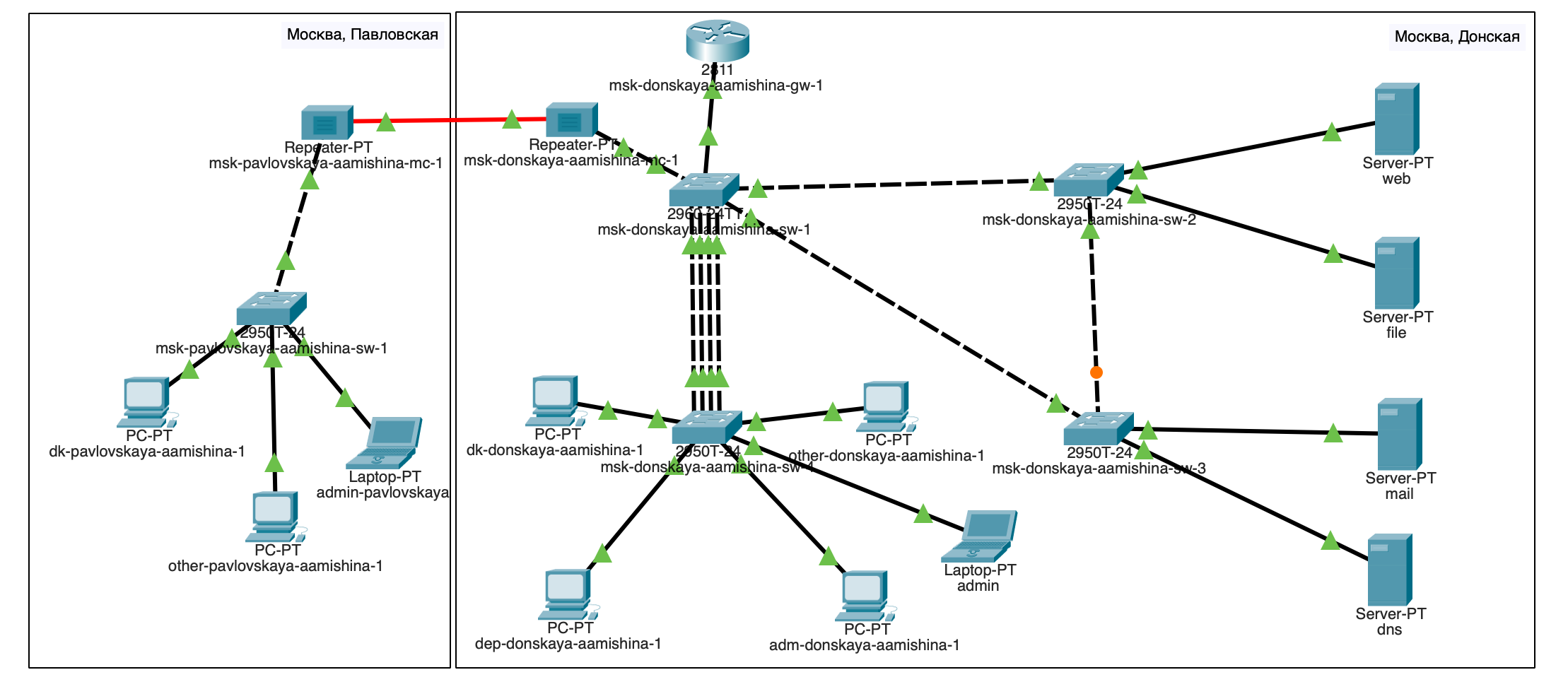


Рис. 19: Логическая область с размещенным ноутбуком admin на Павловской

Настроим доступ для администратора на Павловской по протоколам Telnet и FTP, дадим разрешение устройству с адресом 10.128.6.201 на любые действия (any), Настроим доступ администратора к сети сетевого оборудования (рис.20).



Рис. 20: Настройка доступа для admin-pavlovskaya

Проверим получившийся список контроля доступа (рис.21).

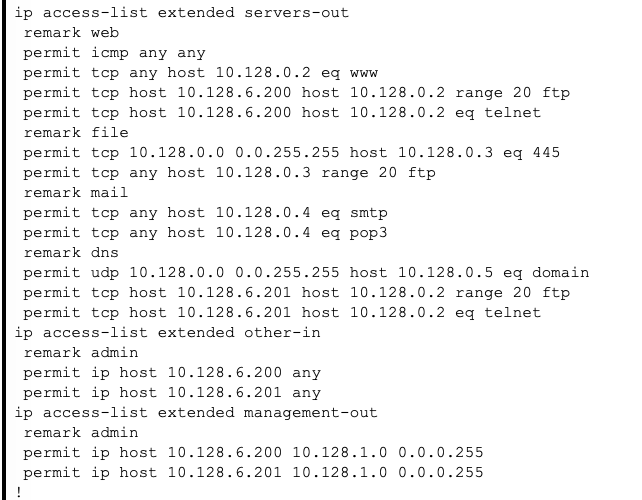


Рис. 21: Проверка списка контроля доступа

Проверим, что наша настройка доступов работает корректно (рис.22).

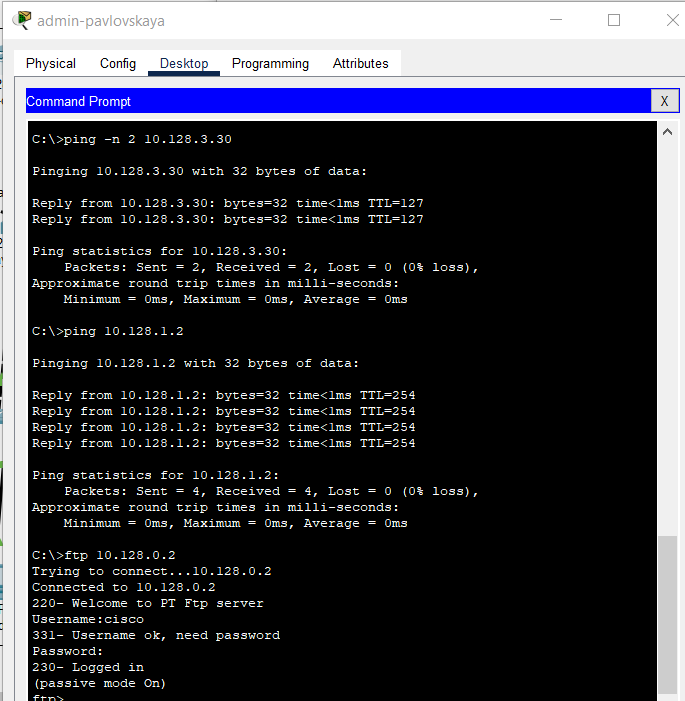


Рис. 22: Проверка корректности настроенного доступа

# 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.

# 6 Выводы

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

# Список литературы

1. Кулябов Д.С., Королькова А.В. Администрирование локальных систем: лабораторные работы : учебное пособие. Москва: РУДН, 2017. 119 с.