Лабораторная работа 10

Настройка списков управления доступом (ACL)

Ланцова Яна Игоревна

Содержание

Список иллюстраций

Список таблиц

# 1 Цель работы

Освоить настройку прав доступа пользователей к ресурсам сети.

# 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 внутрен- ней 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.
11. При выполнении работы необходимо учитывать соглашение об именовании.

# 3 Выполнение лабораторной работы

Откроем проект прошлой 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-eademidova-sw-4 и присвоим ему статический адрес 10.128.6.200, указав в качестве gateway-адреса 10.128.6.1 и адреса DNS-сервера 10.128.0.5 (рис. 1).

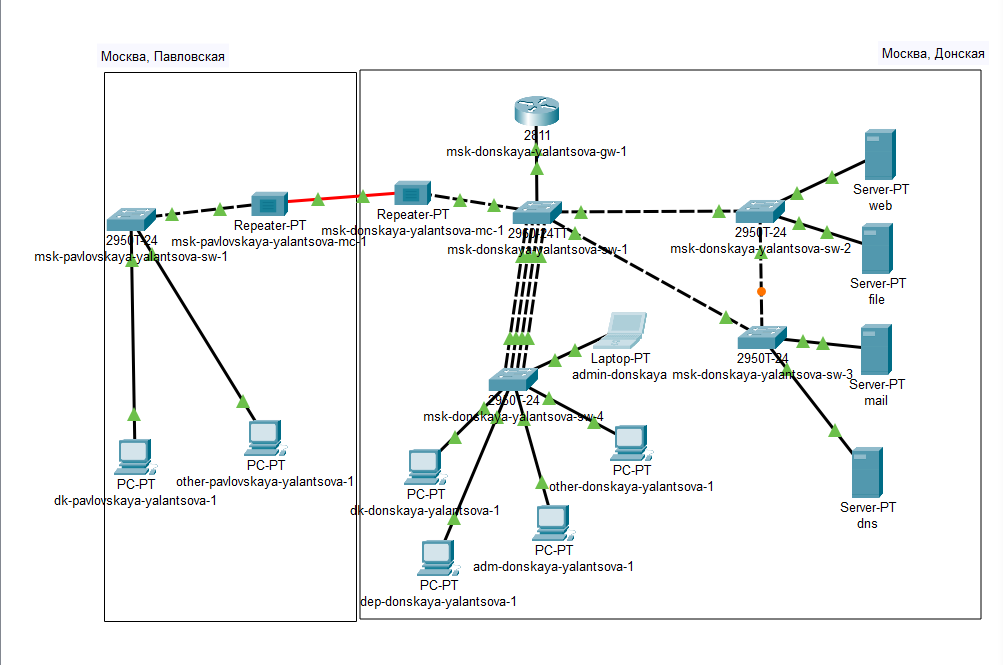


Рис. 1: Размещение ноутбука администратора в сети other-donskaya-1

Права доступа пользователей сети будем настраивать на маршрутизаторе msk-donskaya-gw-1, поскольку именно через него проходит весь трафик сети. Ограничения можно накладывать как на входящий (in), так и на исходящий (out) трафик. По отношению к маршрутизатору накладываемые ограничения будут касаться в основном исходящего трафика.

Следует помнить, что 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 рекомендуется сначала дать разрешение (permit) на какое-то действие, а уже потом накладывать ограничения (deny). Кроме того, после всех правил в конце дописывается неявное запрещение на всё, что не разрешено: deny ip any any (implicit deny).

1. Настроим доступа к web-серверу по порту tcp 80 (рис. 2):

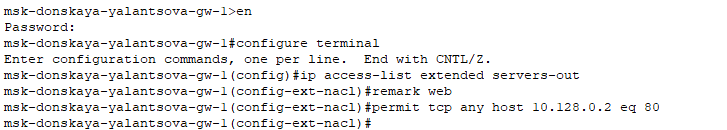


Рис. 2: Настройка доступа к web-серверу по порту tcp 80

Создан 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; дано 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.

1. Добавим список управления доступом к интерфейсу(рис. 3):

Рис. 3: Добавление список управления доступом к интерфейсу

Рис. 3: Добавление список управления доступом к интерфейсу

Здесь: к интерфейсу f0/0.3 подключается список прав доступа servers-out и применяется к исходящему трафику (out).

Можно проверить, что доступ к web-серверу есть через протокол HTTP (введя в строке браузера хоста ip-адрес web-сервера) (рис. 4):

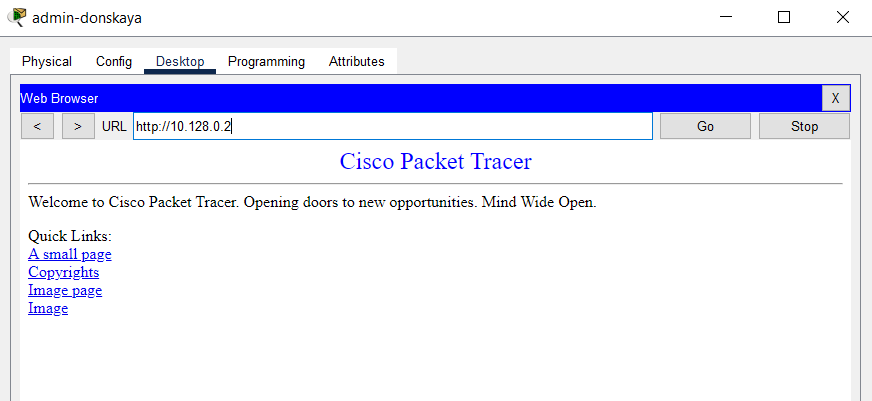


Рис. 4: Проверка доступа к web-серверу через барузер

При этом команда ping будет демонстрировать недоступность web-сервера как по имени, так и по ip-адресу web-сервера(рис. 5).

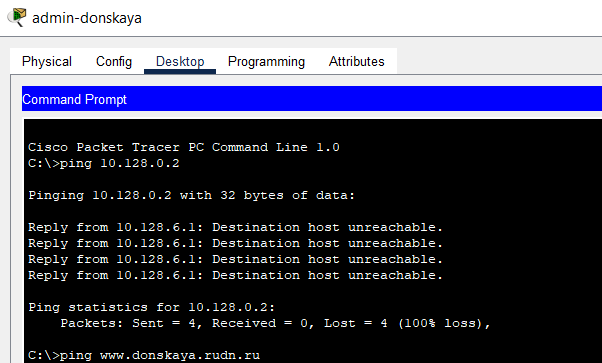


Рис. 5: Проверка доступа к web-серверу с помощью ping

1. Дополнительный доступ для администратора по протоколам Telnet и FTP(рис. 6).

Рис. 6: Настройка доступа по Telnet и FTP

Рис. 6: Настройка доступа по 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.

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. 7).

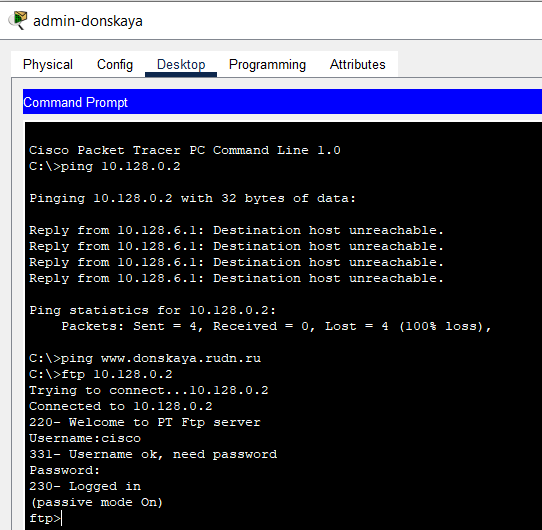


Рис. 7: Проверка доступа к web-серверу по протоколу FTP с устройства администратора

Попробуем провести аналогичную процедуру с другого устройства сети. Убедитмся, что доступ будет запрещён(рис. 8).

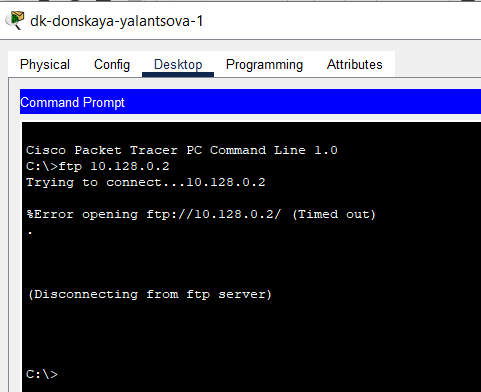


Рис. 8: Проверка доступа к web-серверу по протоколу FTP с устройства dk-donskaya-1

1. Настройка доступа к файловому серверу(рис. 9).

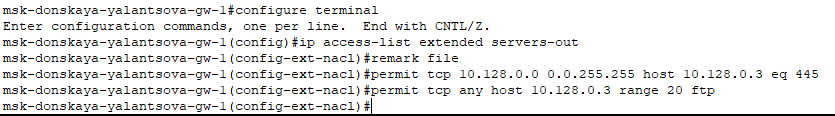


Рис. 9: Настройка доступа к файловому серверу

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).

1. Настройка доступа к почтовому серверу(рис. 10).

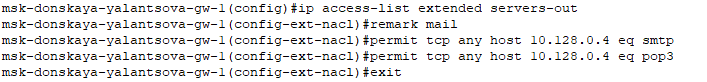


Рис. 10: Настройка доступа к почтовому серверу

Здесь: 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.

1. Настройка доступа к DNS-серверу(рис. 11).

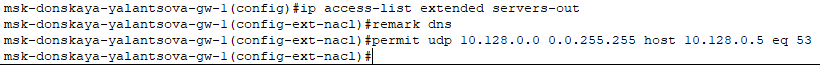


Рис. 11: Настройка доступа к DNS-серверу

Здесь: 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.

Проверм доступность web-сервера (через браузер) не только по ip-адресу, но и по имени (рис. 12, 13).

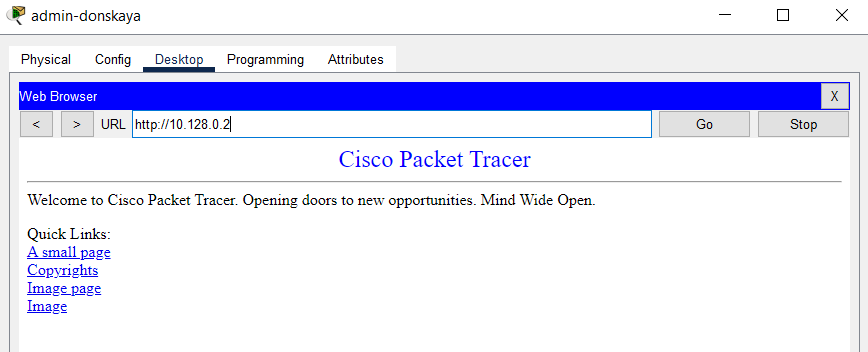


Рис. 12: Проверка доступа к web-серверу по ip-адресу

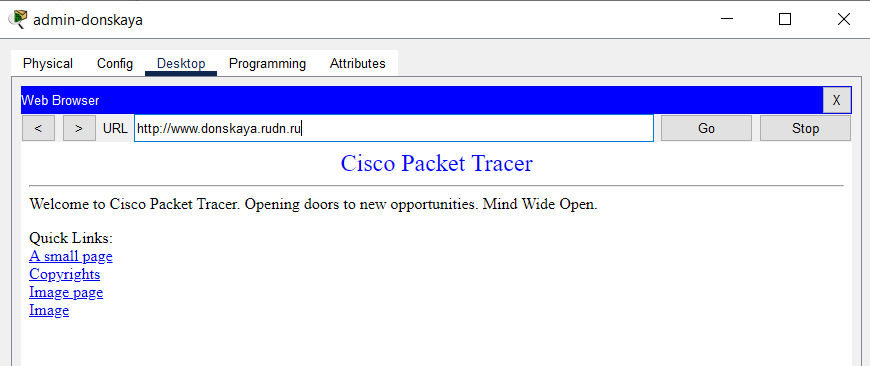


Рис. 13: Проверка доступа к web-серверу по имени

1. Разрешение icmp-запросов (рис. 14).

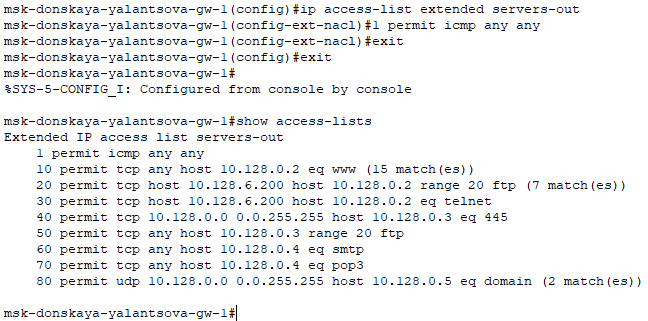


Рис. 14: Разрешение icmp-запросов

Здесь демонстрируется явное управление порядком размещения правил — правило разрешения для icmp-запросов добавляется в начало списка контроля доступа. Номера строк правил в списке контроля доступа можно посмотреть с помощью команды sh access-lists.

1. Настройка доступа для сети Other (требуется наложить ограничение на исходящий из сети Other трафик, который по отношению к маршрутизатору msk-donskaya-yalantsova-gw-1 является входящим трафиком)(рис. 15).

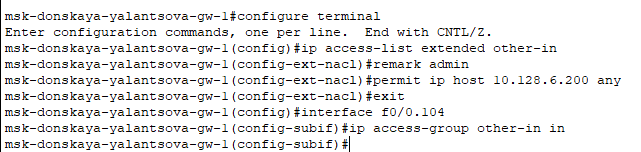


Рис. 15: Настройка доступа для сети Other

Здесь: в списке контроля доступа other-in указано, что следующие правила относятся к администратору сети; даётся разрешение устройству с адресом 0.128.6.200 на любые действия (any); к интерфейсу f0/0.104 подключается список прав доступа other-in и применяется к входящему трафику (in).

1. Настройка доступа администратора к сети сетевого оборудования(рис. 16).

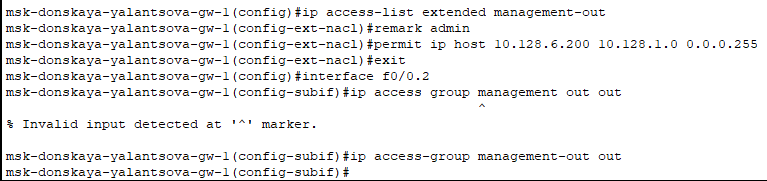


Рис. 16: Настройка доступа администратора к сети сетевого оборудования

Здесь: 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).

Перейдем к выполенению самостоятельной работы

Проверим доступность устройств с помощью команды ping. С устройства dep-donskaya-1 пингуются серверы и другие оконечные устройства, однако доступ к сетевому оборудованию запрещен, а также нет доступа по ftp(рис. 17, 18).

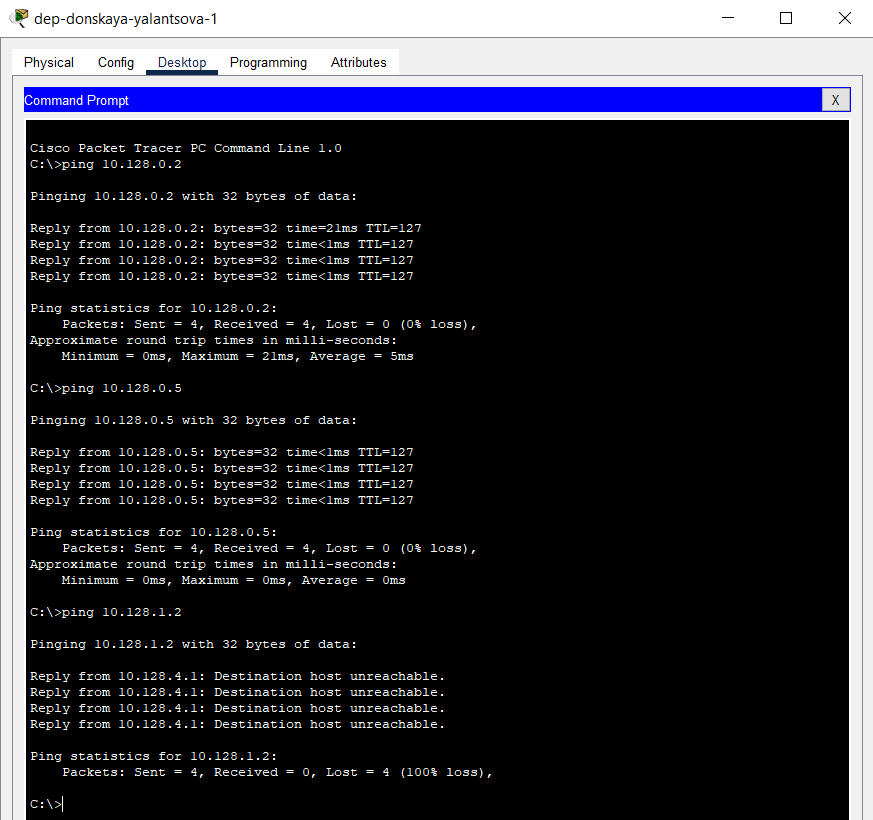


Рис. 17: Проверка правил доступа для оконечного устройтсва на примере dep-donskaya-1 с помощью команды ping

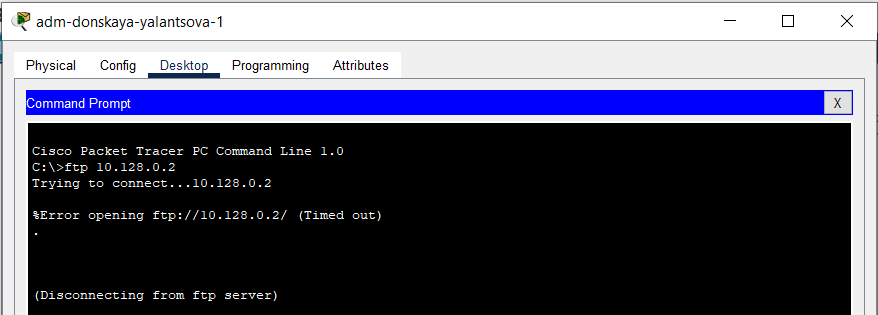


Рис. 18: Проверка правил доступа для оконечного устройтсва на примере dep-donskaya-1 с помощью протокола ftp

С устройства администратора есть доступ ко всем устройствам сети по icmp-запросам, а также есть доступ к web-серверу по ftp(рис. 19, 20).

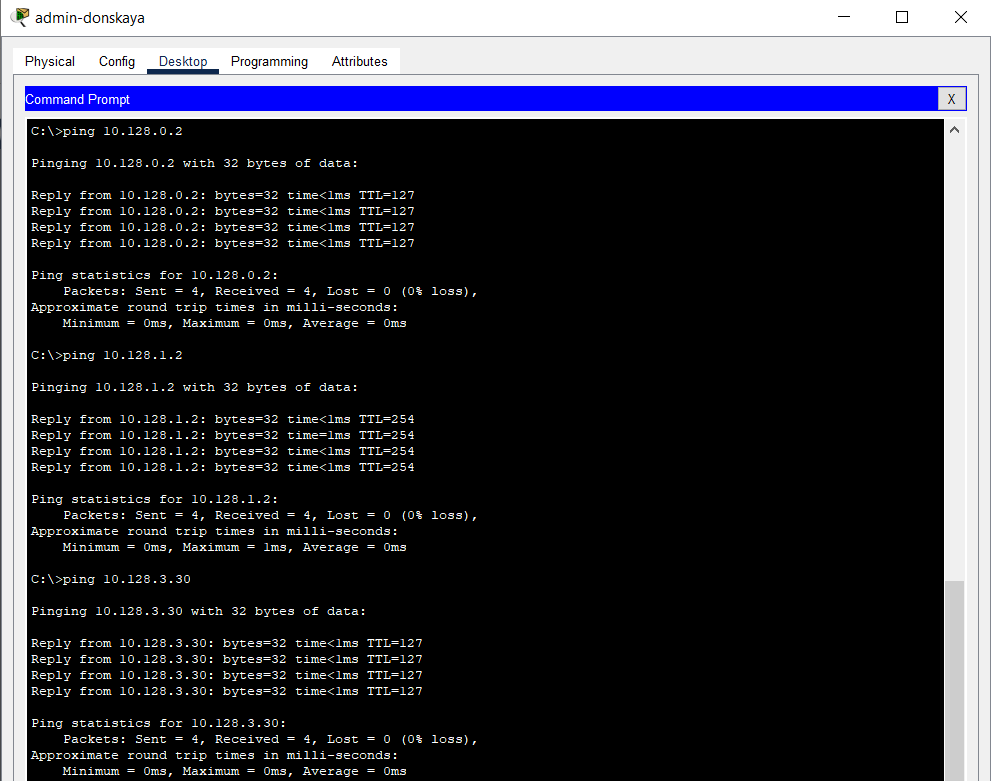


Рис. 19: Проверка правил доступа для администратора с помощью команды ping

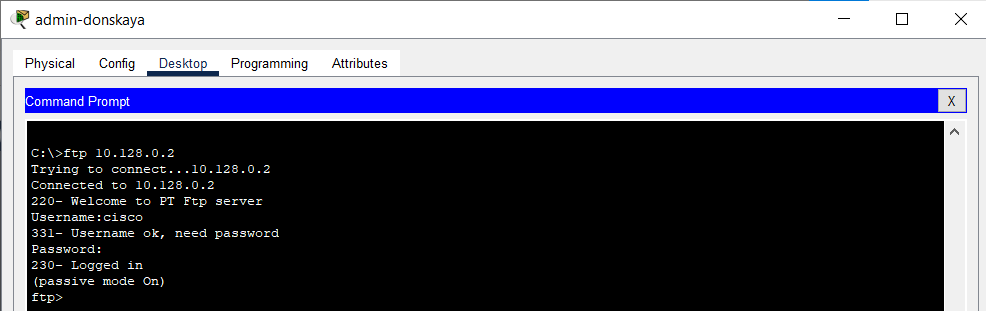


Рис. 20: Проверка правил доступа для администратора с помощью протокола ftp

Разрешим администратору из сети Other на Павловской действия, аналогичные действиям администратора сети Other на Донской. А именно дадим дополнительный доступ для администратора по протоколам Telnet и FTP, настроим доступ для сети Other и настроим доступ к сети сетевого оборудования(рис. 21).

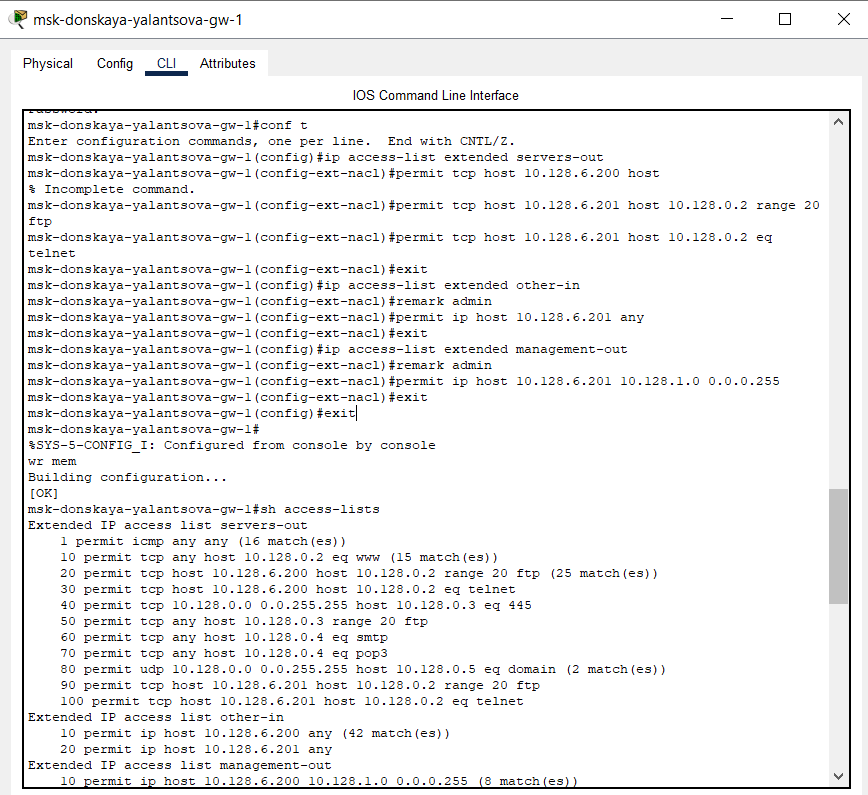


Рис. 21: Настройка прав администратора на Павловской

Проверим корректность внесенных прав доступа(рис. 22).

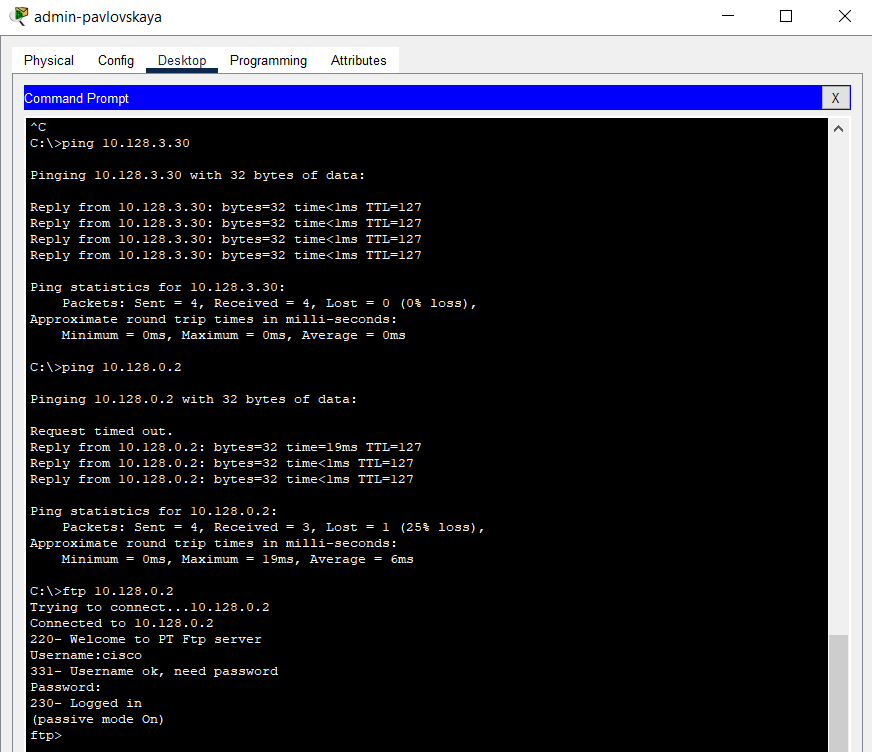


Рис. 22: Проверка правил доступа для администратора на Павловской

Итоговый проект выглядит следующим образом (рис. 23).

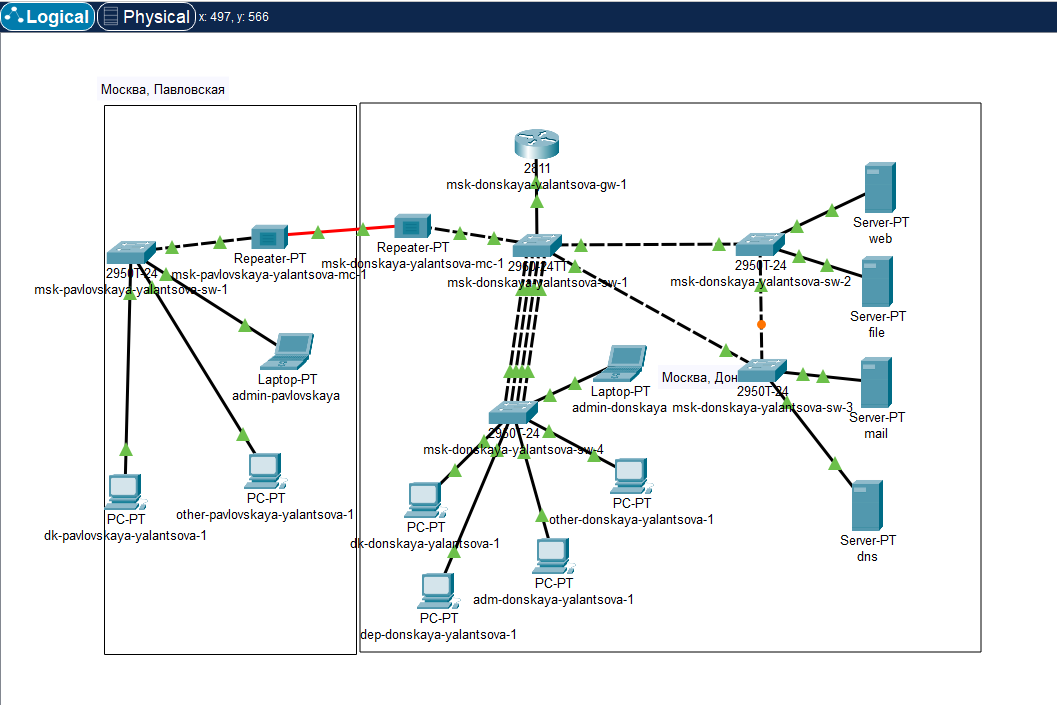


Рис. 23: Схема сети в логической рабочей области Packet Tracer

# 4 Выводы

В результате выполнения лабораторной работы освоили настройку прав доступа пользователей к ресурсам сети.

# 5 Контрольные вопросы

1. Как задать действие правила для конкретного протокола?

Указать протокол в конце записи команды permit. Примеры:

permit tcp any host 10.128.0.3 range 20 ftp  
  
permit tcp any host 10.128.0.4 eq smtp

1. Как задать действие правила сразу для нескольких портов?

Нужно использовать команду interface range и порты через дефис.

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?

Необходимо указать права доступа с номерами в нужном порядке, используя команду access-list <Номер в списке> permit.