

# **Лабораторная работа № 10**

**Настройка списков управления доступом (ACL)**

Демидова Екатерина Алексеевна

# Содержание

<b>1</b>	<b>Цель работы</b>	<b>4</b>
<b>2</b>	<b>Задание</b>	<b>5</b>
<b>3</b>	<b>Выполнение лабораторной работы</b>	<b>6</b>
3.1	Самостоятельная работа . . . . .	17
3.2	Контрольные вопросы . . . . .	24
<b>4</b>	<b>Выводы</b>	<b>25</b>

## Список иллюстраций

3.1	Схема сети в логической рабочей области Packet Tracer . . . . .	6
3.2	Размещение ноутбука администратора в сети other-donskaya-1 . .	7
3.3	Проверка доступа к web-серверу через барузер . . . . .	9
3.4	Проверка доступа к web-серверу с помощью ping . . . . .	10
3.5	Проверка доступа к web-серверу по протоколу FTP с устройства администратора . . . . .	11
3.6	Проверка доступа к web-серверу по протоколу FTP с устройства dk-donskaya-1 . . . . .	11
3.7	Просмотр прав доступа . . . . .	13
3.8	Проверка доступа к web-серверу по ip-адресу . . . . .	14
3.9	Проверка доступа к web-серверу по имени . . . . .	15
3.10	Просмтр номеров строк в списке контроля доступа . . . . .	16
3.11	Настройка доступа для сети Other . . . . .	16
3.12	Настройка доступа администратора к сети сетевого оборудования .	17
3.13	Проверка правил доступа для оконечного устройства на примере der-donskaya-1 с помощью команды ping . . . . .	18
3.14	Проверка правил доступа для оконечного устройства на примере der-donskaya-1 с помощью протокола ftp . . . . .	19
3.15	Проверка правил доступа для администратора с помощью команды ping . . . . .	20
3.16	Проверка правил доступа для администратора с помощью протокола ftp . . . . .	21
3.17	Настройка прав администратора на Павловской . . . . .	22
3.18	Итоговый список прав доступа . . . . .	23
3.19	Проверка правил доступа для администратора на Павловской . .	23

# **1 Цель работы**

Освоить настройку прав доступа пользователей к ресурсам сети.

## 2 Задание

1. Требуется настроить следующие правила доступа:
  - 1) web-сервер: разрешить доступ всем пользователям по протоколу HTTP через порт 80 протокола TCP, а для администратора открыть доступ по протоколам Telnet и FTP;
  - 2) файловый сервер: с внутренних адресов сети доступ открыт по портам для общедоступных каталогов, с внешних – доступ по протоколу FTP;
  - 3) 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;
  - 4) DNS-сервер: открыть порт 53 протокола UDP для доступа из внутренней сети;
  - 5) разрешить icmp-сообщения, направленные в сеть серверов;
  - 6) запретить для сети Other любые запросы за пределы сети, за исключением администратора;
  - 7) 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

Откроем проект прошлой лабораторной работы(рис. [3.1]).

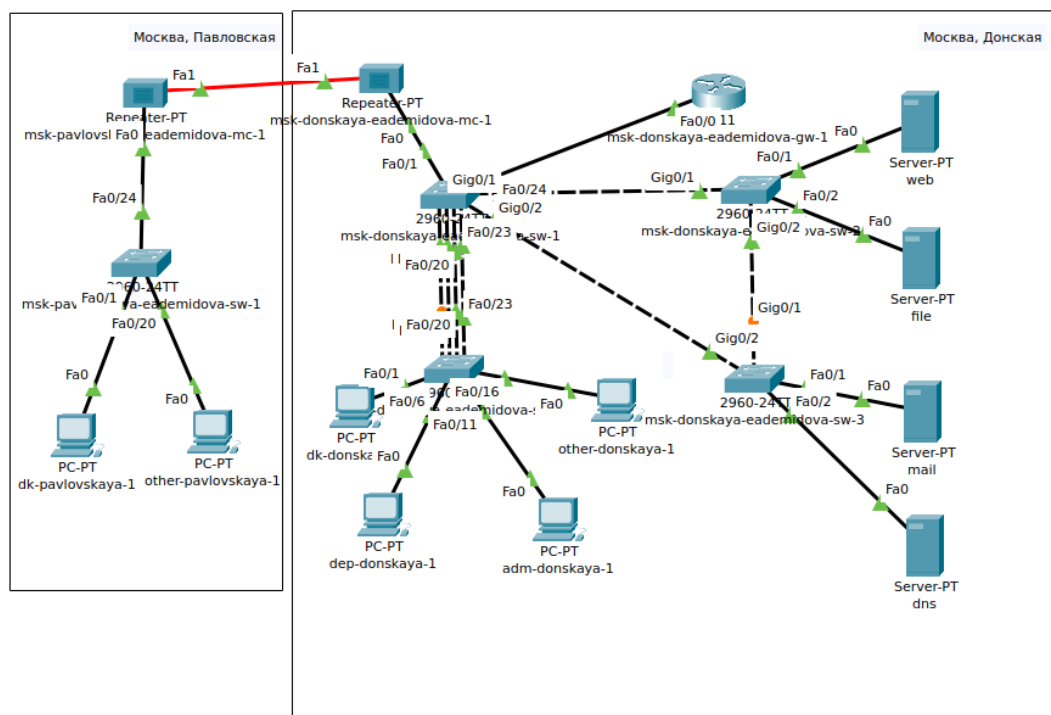


Рис. 3.1: Схема сети в логической рабочей области Packet Tracer

В рабочей области проекта подключим ноутбук администратора с именем `admin` к сети `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. [3.2]).

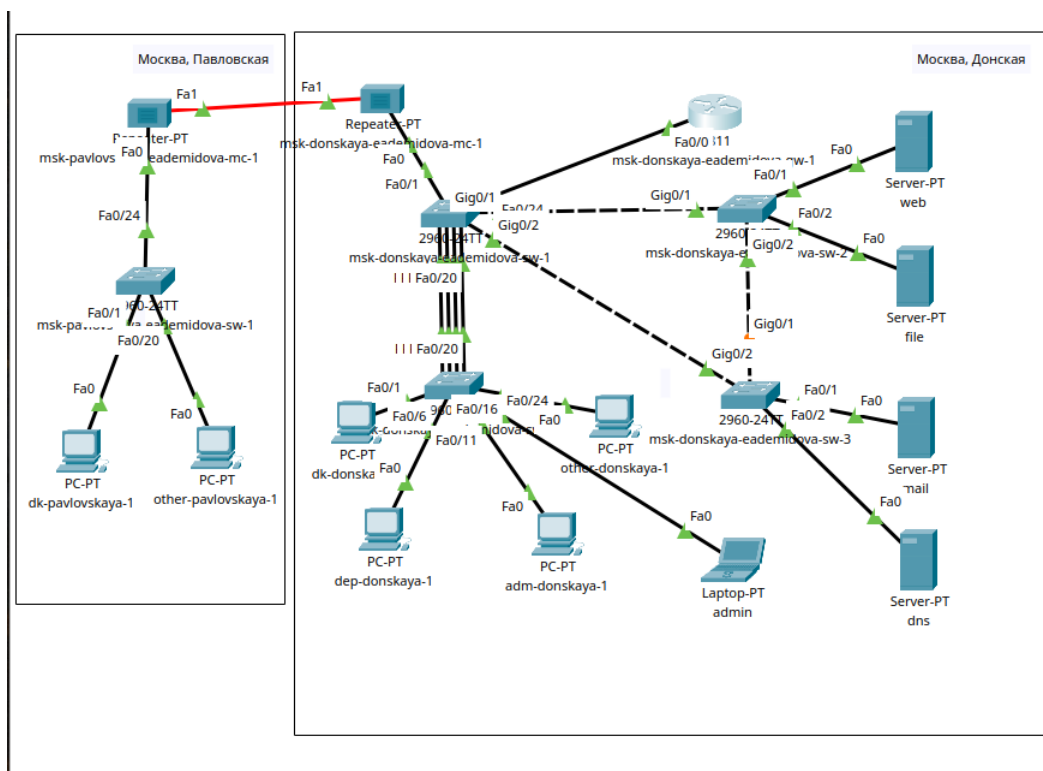


Рис. 3.2: Размещение ноутбука администратора в сети other-donskaya-1

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:

```
msk-donskaya-gw-1# configure terminal
msk-donskaya-gw-1(config)#ip access -list extended servers -out
msk-donskaya-gw-1(config-ext-nacl)#remark web
msk-donskaya-gw-1(config-ext-nacl)#permit tcp any host 10.128.0.2 eq 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.

## 2. Добавим список управления доступом к интерфейсу.

```
msk-donskaya-gw-1# configure terminal
msk-donskaya-gw-1(config)# interface f0 /0.3
msk-donskaya-gw-1(config-subif)# ip access-group servers-out out
```

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. [3.3]).



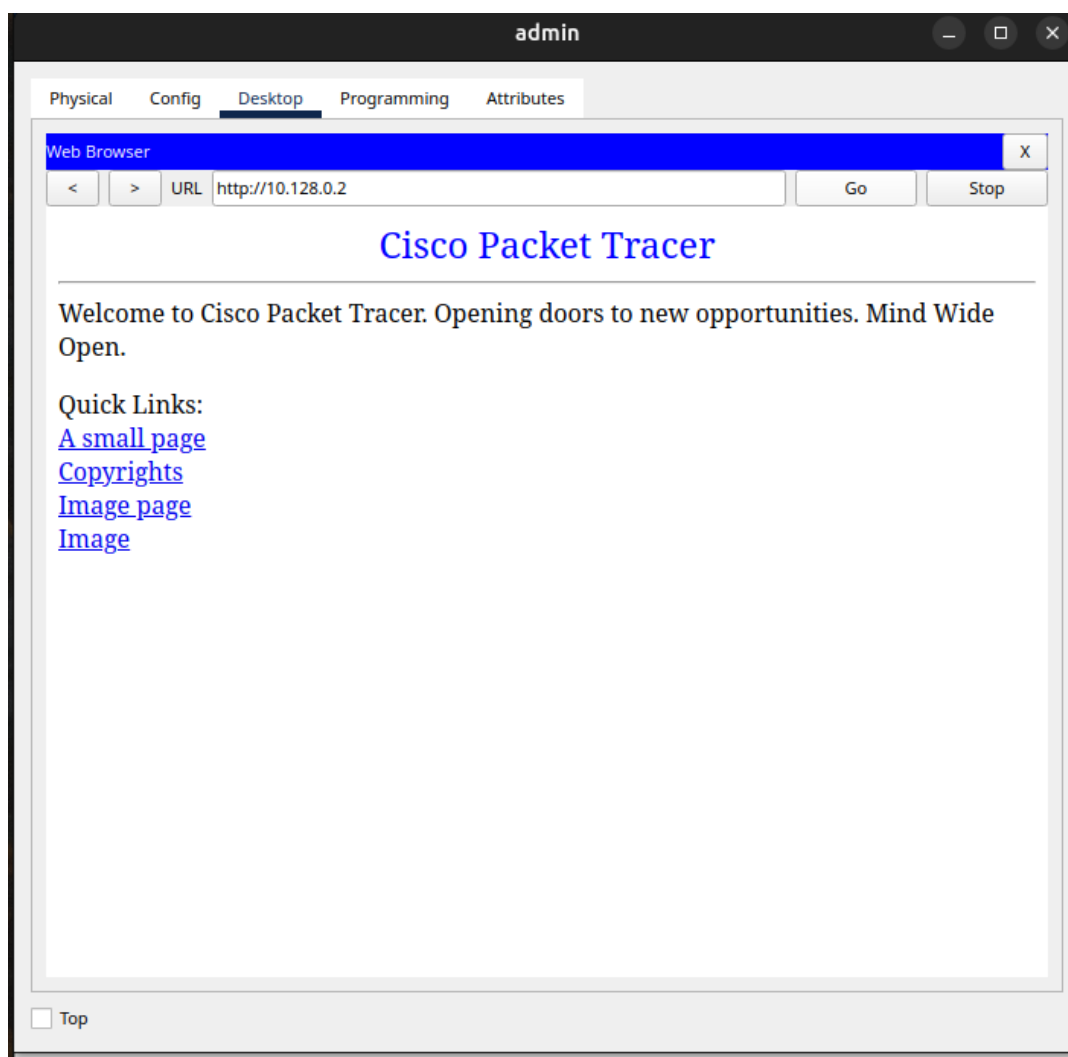


Рис. 3.3: Проверка доступа к web-серверу через браузер

При этом команда `ping` будет демонстрировать недоступность web-сервера как по имени, так и по ip-адресу web-сервера(рис. [3.4]).

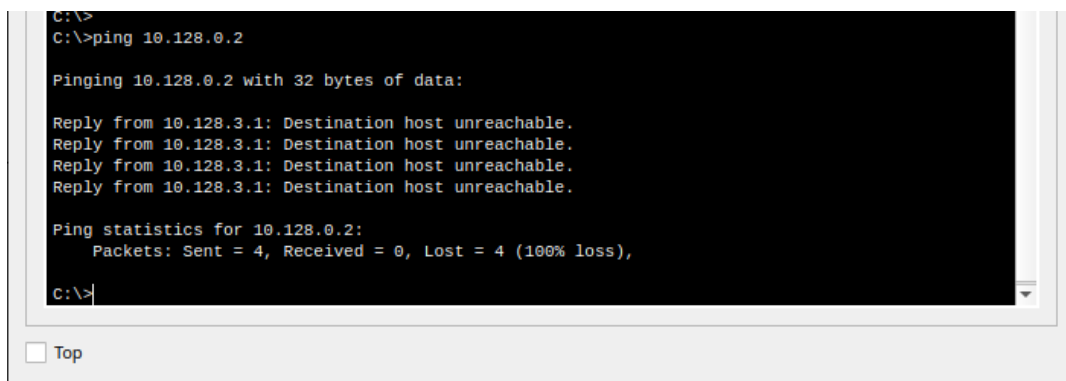


Рис. 3.4: Проверка доступа к web-серверу с помощью ping

### 3. Дополнительный доступ для администратора по протоколам Telnet и FTP:

```
msk-donskaya-gw-1# configure terminal
msk-donskaya-gw-1(config)# ip access-list extended servers-out
msk-donskaya-gw-1(config-ext-nacl)# permit tcp host 10.128.6.200 host
10.128.0.2 range 20 ftp
msk-donskaya-gw-1(config-ext-nacl)#permit tcp host 10.128.6.200 host
10.128.0.2 eq telnet
```

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. [3.5]):

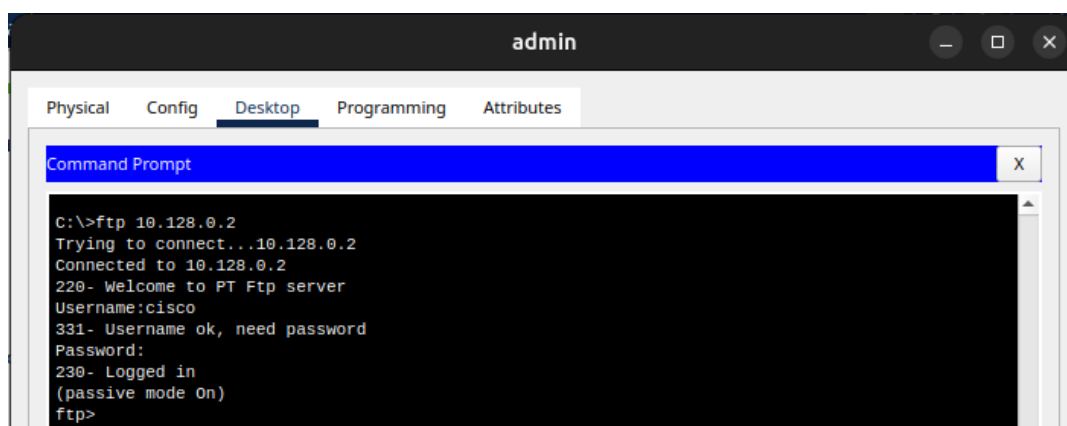


Рис. 3.5: Проверка доступа к web-серверу по протоколу FTP с устройства администратора

Попробуем провести аналогичную процедуру с другого устройства сети. Убедитесь, что доступ будет запрещён(рис. [3.6]).



Рис. 3.6: Проверка доступа к web-серверу по протоколу FTP с устройства dk-donskaya-1

#### 4. Настройка доступа к файловому серверу:

```
msk-donskaya-gw-1# configure terminal
```

```
msk-donskaya-gw-1(config)#ip access-list extended servers-out
```

```
msk-donskaya-gw-1(config-ext-nacl)#remark file
```

```
msk-donskaya-gw-1(config-ext-nacl)#permit tcp 10.128.0.0 0.0.255.255
```

```
host 10.128.0.3 eq 445
msk-donskaya-gw-1(config-ext-nacl)#permit tcp any host 10.128.0.3
range 20 ftp
```

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).

#### 5. Настройка доступа к почтовому серверу:

```
msk-donskaya-gw-1# configure terminal
msk-donskaya-gw-1(config)#ip access-list extended servers-out
msk-donskaya-gw-1(config-ext-nacl)#remark mail
msk-donskaya-gw-1(config-ext-nacl)#permit tcp any host 10.128.0.4 eq smtp
msk-donskaya-gw-1(config-ext-nacl)#permit tcp any host 10.128.0.4 eq pop3
```

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.

#### 6. Настройка доступа к DNS-серверу:

```
msk-donskaya-gw-1# configure terminal
msk-donskaya-gw-1(config)#ip access-list extended servers-out
msk-donskaya-gw-1(config-ext-nacl)#remark dns
msk-donskaya-gw-1(config-ext-nacl)#permit udp 10.128.0.0 0.0.255.255
host 10.128.0.5 eq 53
```

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.

Проверим правильность всех введённых прав доступа(рис. [3.7]).

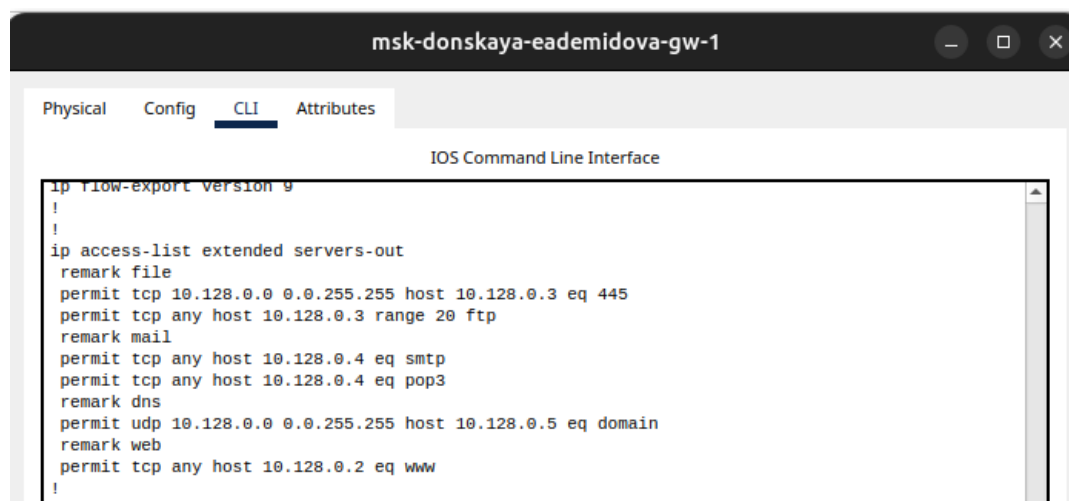


Рис. 3.7: Просмотр прав доступа

Проверим доступность web-сервера (через браузер) не только по ip-адресу, но и по имени(рис. [3.8], [3.9]):

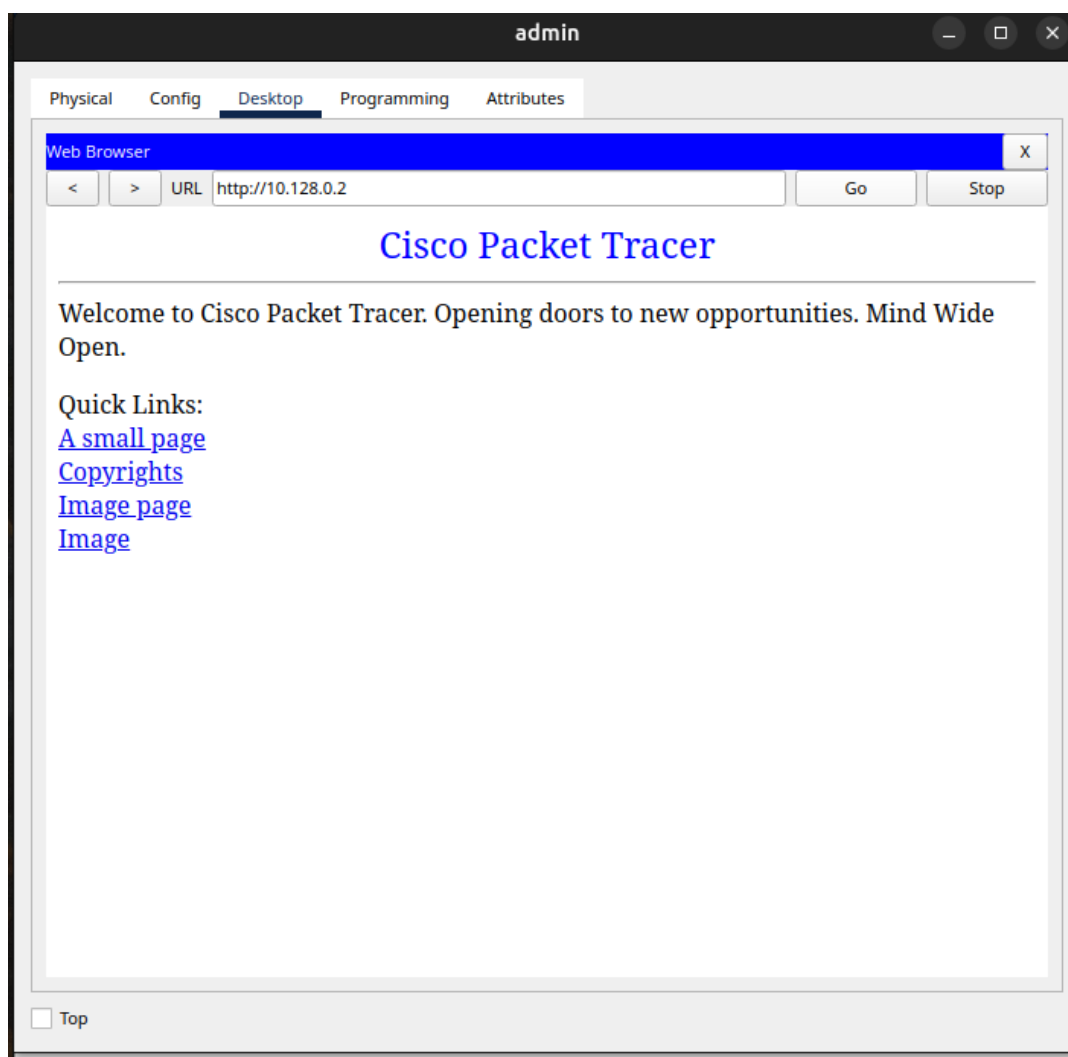


Рис. 3.8: Проверка доступа к web-серверу по ip-адресу

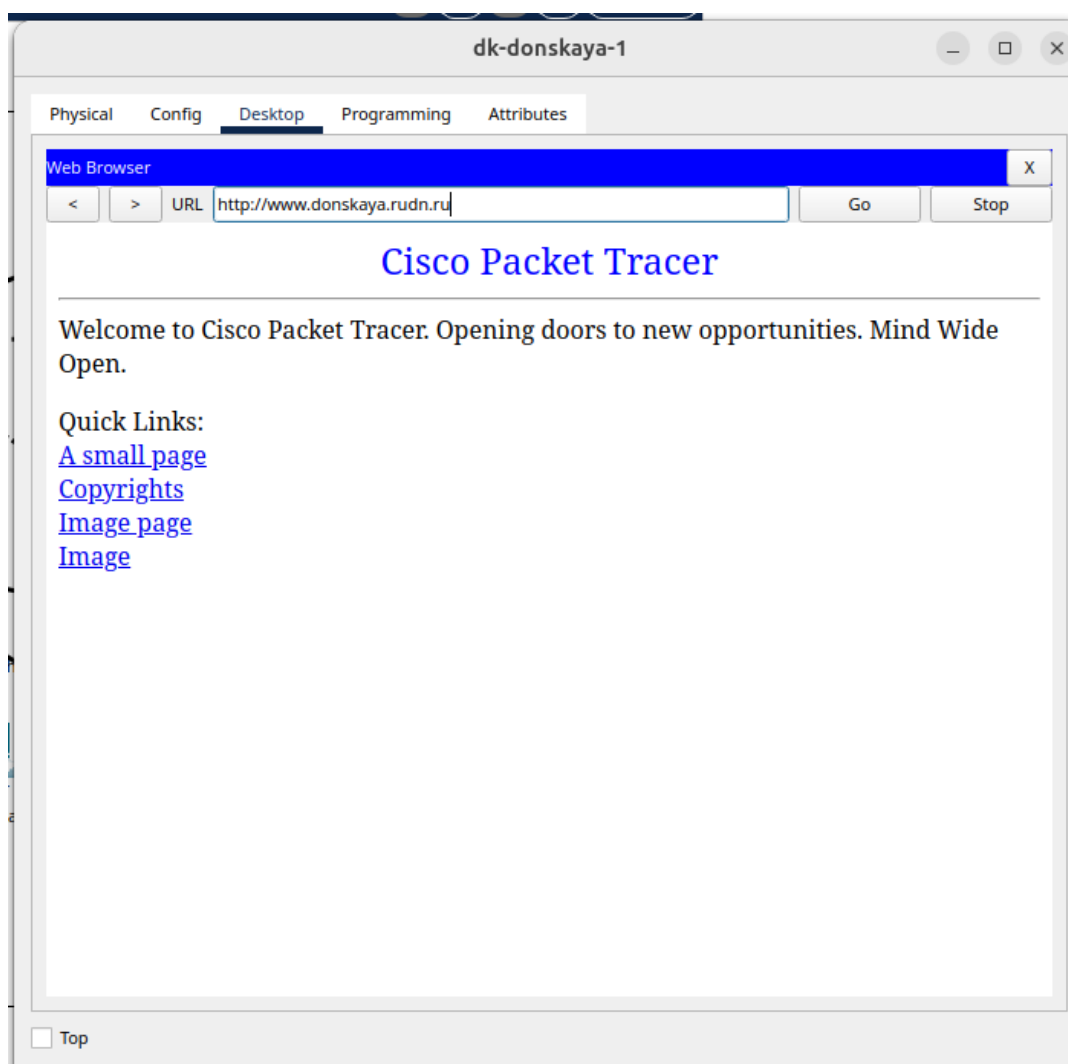


Рис. 3.9: Проверка доступа к web-серверу по имени

#### 7. Разрешение icmp-запросов:

```
msk-donskaya-gw-1# configure terminal
msk-donskaya-gw-1(config)#ip access-list extended servers-out
msk-donskaya-gw-1(config-ext-nacl)#1 permit icmp any any
```

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(рис. [3.10]).

```
msk-donskaya-eademidova-gw-1(config)#ip access-list extended servers-out
msk-donskaya-eademidova-gw-1(config-ext-nacl)#1 permit icmp any any
msk-donskaya-eademidova-gw-1(config-ext-nacl)#exit
msk-donskaya-eademidova-gw-1(config)#exit
msk-donskaya-eademidova-gw-1#
%SYS-5-CONFIG_I: Configured from console by console

msk-donskaya-eademidova-gw-1#wr me
Building configuration...
[OK]
msk-donskaya-eademidova-gw-1#sh acce
msk-donskaya-eademidova-gw-1#sh access-lists
Extended IP access list servers-out
 1 permit icmp any any
10 permit tcp 10.128.0.0 0.0.255.255 host 10.128.0.3 eq 445
20 permit tcp any host 10.128.0.3 range 20 ftp
30 permit tcp any host 10.128.0.4 eq smtp
40 permit tcp any host 10.128.0.4 eq pop3
50 permit udp 10.128.0.0 0.0.255.255 host 10.128.0.5 eq domain (3 match(es))
60 permit tcp any host 10.128.0.2 eq www (30 match(es))

msk-donskaya-eademidova-gw-1#
```

Рис. 3.10: Просмотр номеров строк в списке контроля доступа

8. Настройка доступа для сети Other (требуется наложить ограничение на исходящий из сети Other трафик, который по отношению к маршрутизатору msk-donskaya-eademidova-gw-1 является входящим трафиком)(рис. [3.11]).

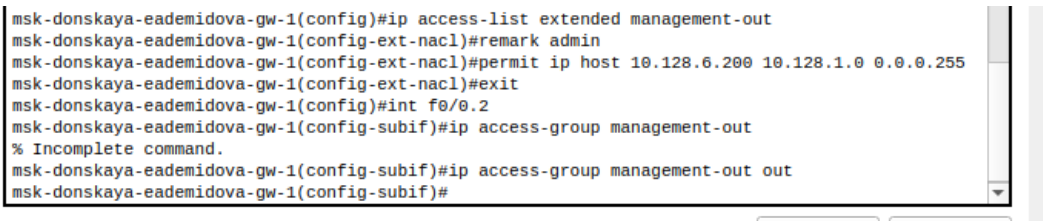
```
Enter configuration commands, one per line. End with CNTL/Z.
msk-donskaya-eademidova-gw-1(config)#ip access-list extended servers-out
msk-donskaya-eademidova-gw-1(config-ext-nacl)#exit
msk-donskaya-eademidova-gw-1(config)#ip access-list extended other-in
msk-donskaya-eademidova-gw-1(config-ext-nacl)#remark admin
msk-donskaya-eademidova-gw-1(config-ext-nacl)#permit ip host 10.128.6.200 any
msk-donskaya-eademidova-gw-1(config-ext-nacl)#exit
msk-donskaya-eademidova-gw-1(config)#int f0/0.104
msk-donskaya-eademidova-gw-1(config-subif)#ip acce
msk-donskaya-eademidova-gw-1(config-subif)#ip access-group other-in in
msk-donskaya-eademidova-gw-1(config-subif)#
```

Рис. 3.11: 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).

9. Настройка доступа администратора к сети сетевого оборудования(рис. [3.12]).





```
msk-donskaya-eademidova-gw-1(config)#ip access-list extended management-out
msk-donskaya-eademidova-gw-1(config-ext-nacl)#remark admin
msk-donskaya-eademidova-gw-1(config-ext-nacl)#permit ip host 10.128.6.200 10.128.1.0 0.0.0.255
msk-donskaya-eademidova-gw-1(config-ext-nacl)#exit
msk-donskaya-eademidova-gw-1(config)#int f0/0.2
msk-donskaya-eademidova-gw-1(config-subif)#ip access-group management-out
% Incomplete command.
msk-donskaya-eademidova-gw-1(config-subif)#ip access-group management-out out
msk-donskaya-eademidova-gw-1(config-subif)#
```

Рис. 3.12: 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).

### 3.1 Самостоятельная работа

Проверим доступность устройств с помощью команды ping. С устройства der-donskaya-1 пингуются серверы и другие конечные устройства, однако доступ к сетевому оборудованию запрещен, а также нет доступа по ftp(рис. [3.13], [3.14]).

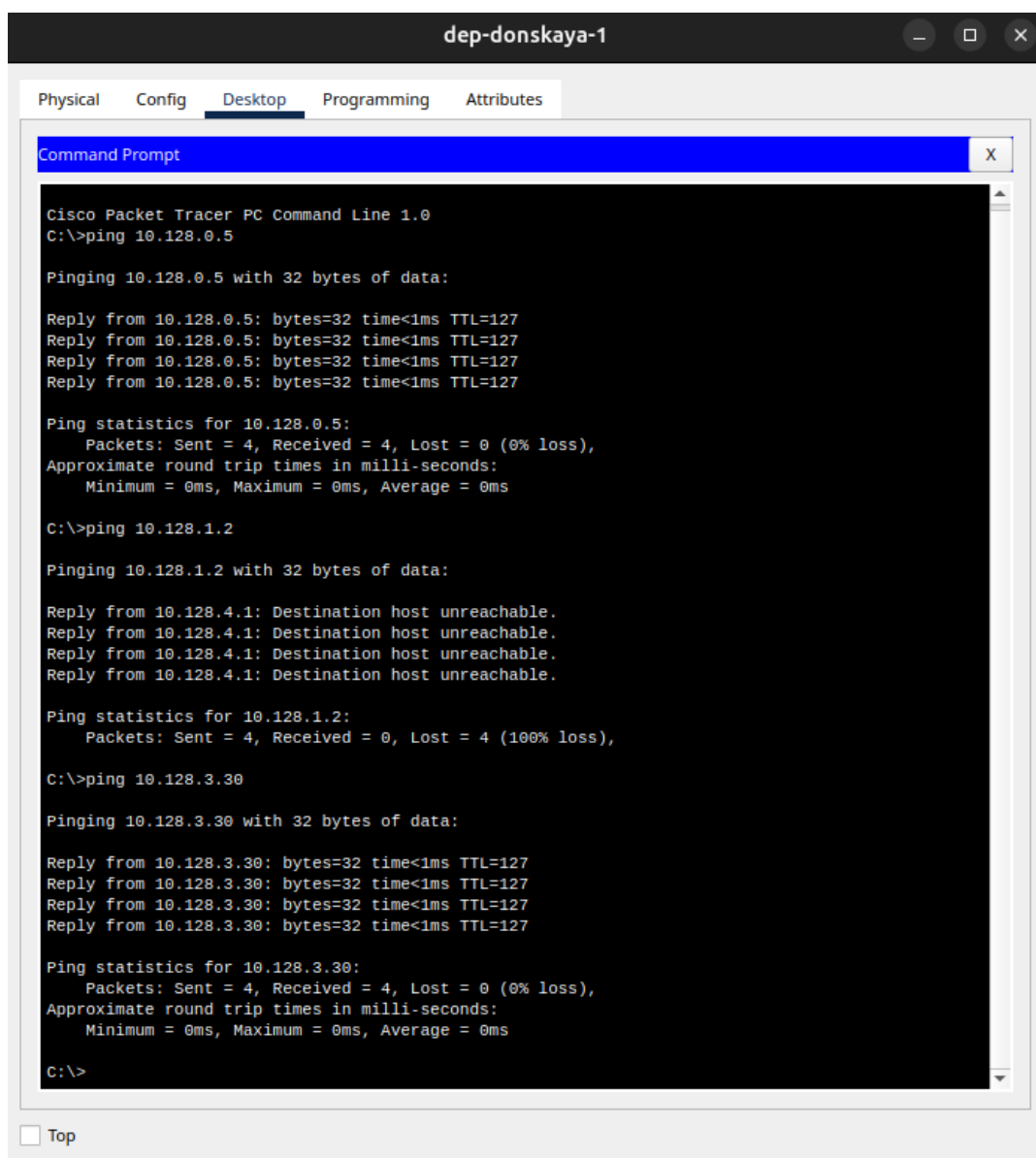


Рис. 3.13: Проверка правил доступа для оконечного устройства на примере dep-donskaya-1 с помощью команды ping



Рис. 3.14: Проверка правил доступа для оконечного устройства на примере der-donskaya-1 с помощью протокола ftp

С устройства администратора есть доступ ко всем устройствам сети по истр-запросам, а также есть доступ к web-серверу по ftp(рис. [3.15], [3.16]).

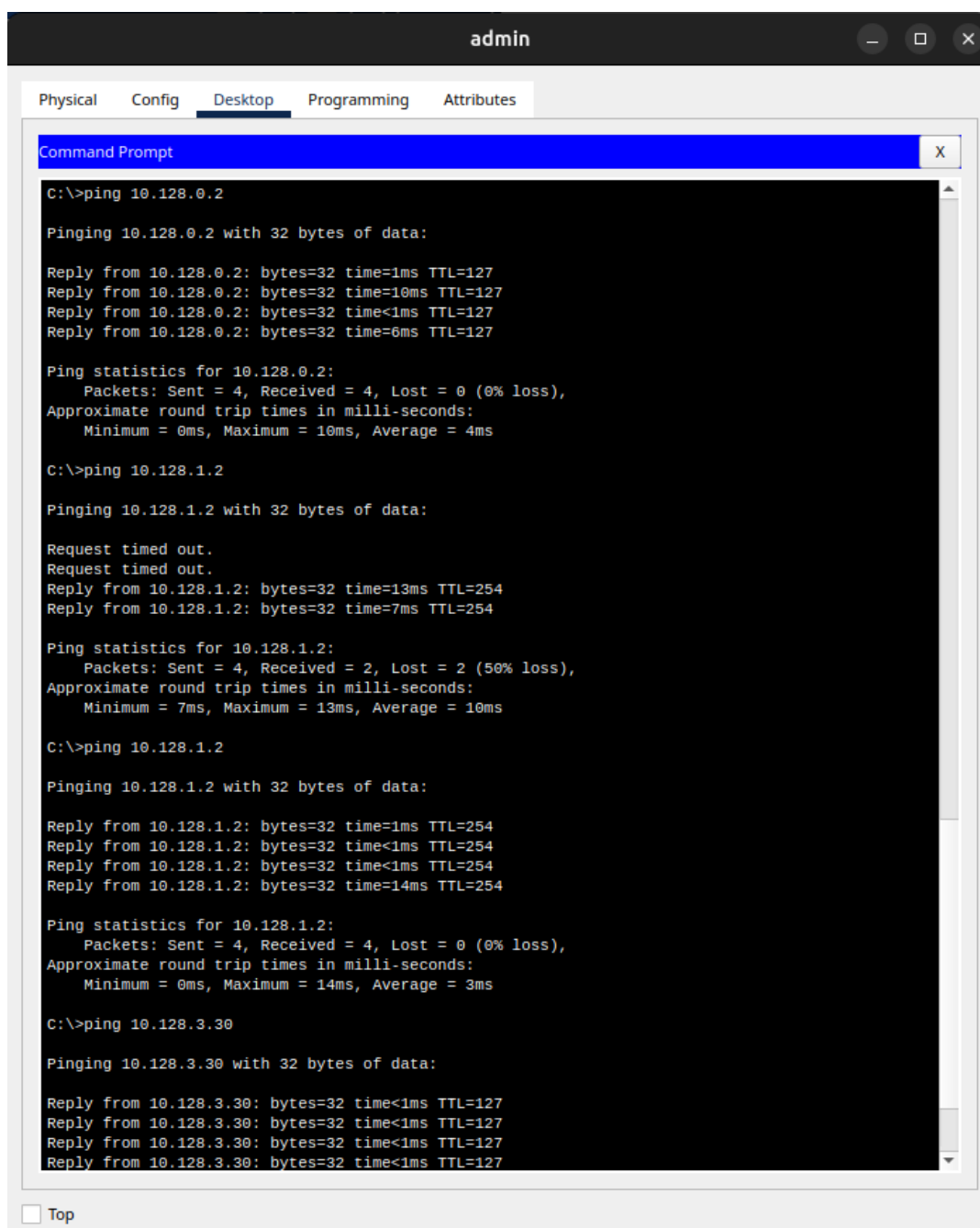


Рис. 3.15: Проверка правил доступа для администратора с помощью команды ping

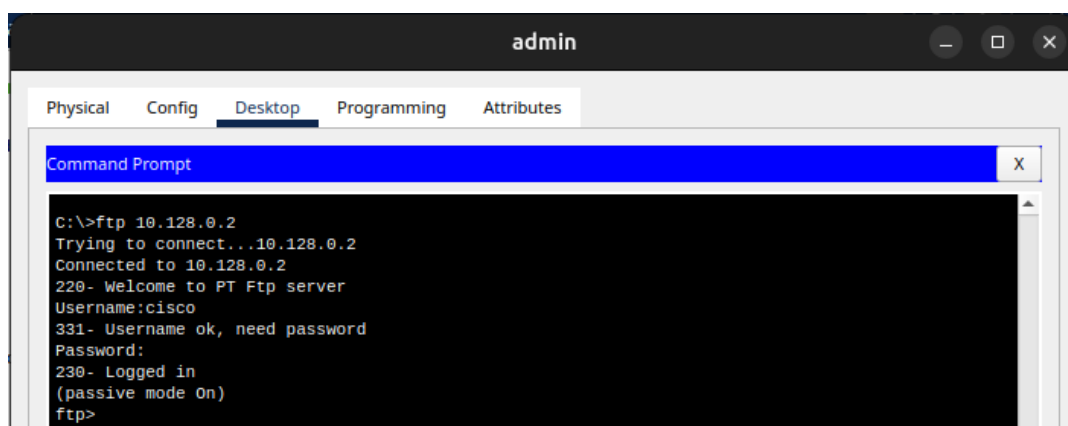


Рис. 3.16: Проверка правил доступа для администратора с помощью протокола ftp

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. [3.17], [3.18]).

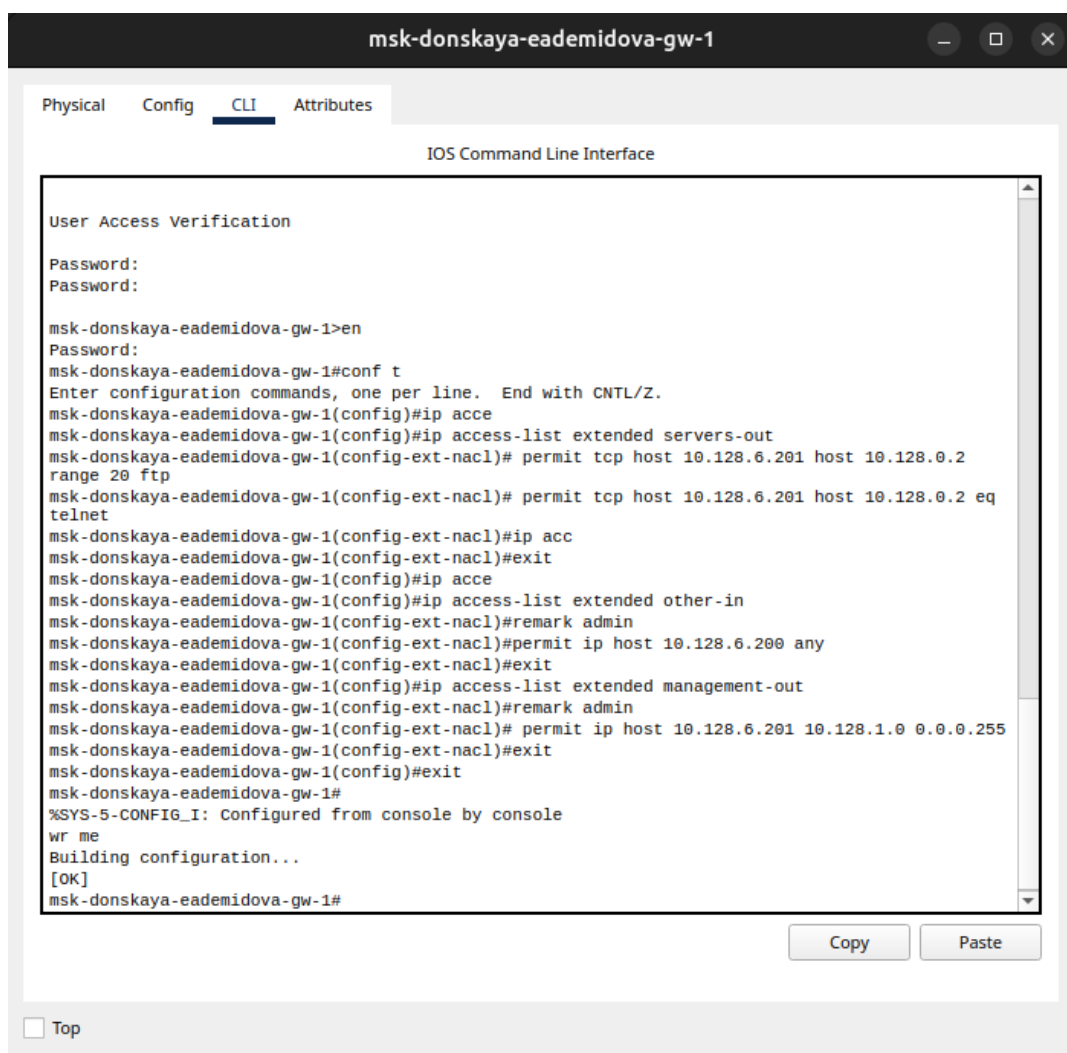


Рис. 3.17: Настройка прав администратора на Павловской

```
msk-donskaya-eademidova-gw-1#sh access-lists
Extended IP access list servers-out
 10 permit icmp any any
 20 permit tcp 10.128.0.0 0.0.255.255 host 10.128.0.3 eq 445
 30 permit tcp any host 10.128.0.3 range 20 ftp
 40 permit tcp any host 10.128.0.4 eq smtp
 50 permit tcp any host 10.128.0.4 eq pop3
 60 permit udp 10.128.0.0 0.0.255.255 host 10.128.0.5 eq domain
 70 permit tcp any host 10.128.0.2 eq www
 80 permit tcp host 10.128.6.200 host 10.128.0.2 range 20 ftp
 90 permit tcp host 10.128.6.200 host 10.128.0.2 eq telnet
100 permit tcp host 10.128.6.201 host 10.128.0.2 range 20 ftp
110 permit tcp host 10.128.6.201 host 10.128.0.2 eq telnet
Extended IP access list other-in
 10 permit ip host 10.128.6.200 any
 20 permit ip host 10.128.6.201 any
Extended IP access list management-out
 10 permit ip host 10.128.6.200 10.128.1.0 0.0.0.255
 20 permit ip host 10.128.6.201 10.128.1.0 0.0.0.255

msk-donskaya-eademidova-gw-1#
```

Copy Paste

Рис. 3.18: Итоговый список прав доступа

Проверим корректность внесенных прав доступа(рис. [3.19]).

admin-pavlovskaya

Physical Config Desktop Programming Attributes

Command Prompt X

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ftp 10.128.0.2
Trying to connect...10.128.0.2
Connected to 10.128.0.2
220- Welcome to PT Ftp server
Username:cisco
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>

C:\>ping 10.128.1.6

Pinging 10.128.1.6 with 32 bytes of data:

Request timed out.
Request timed out.
Reply from 10.128.1.6: bytes=32 time<1ms TTL=254
Reply from 10.128.1.6: bytes=32 time=1ms TTL=254

Ping statistics for 10.128.1.6:
    Packets: Sent = 4, Received = 2, Lost = 2 (50% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>
```

Рис. 3.19: Проверка правил доступа для администратора на Павловской

## 3.2 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
```

2. Как задать действие правила сразу для нескольких портов?

Нужно использовать команду `interface range` и порты через дефис.

3. Как узнать номер правила в списке прав доступа?

С помощью команды `show access-lists`.

4. 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`.



## 4 Выводы

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