

# **Лабораторная работа №10**

**Настройка списков управления доступом (ACL)**

Лушин Артём Андреевич

# Содержание

1	Цель работы	4
2	Выполнение лабораторной работы	5
3	Выводы	15

# Список иллюстраций

2.1	Размещение ноутбука администратора . . . . .	5
2.2	Конфигурация ноутбука . . . . .	5
2.3	Конфигурация ноутбука . . . . .	6
2.4	Настройка доступа к web . . . . .	6
2.5	Добавление списка управления доступом . . . . .	6
2.6	ДОП доступ по протоколам . . . . .	6
2.7	Доступ по протоколу . . . . .	7
2.8	Доступ по протоколу . . . . .	7
2.9	Доступ к файловому серверу . . . . .	8
2.10	Доступ к почтовому серверу . . . . .	8
2.11	Доступ к DNS . . . . .	8
2.12	web по ip-адресу . . . . .	8
2.13	web по имени . . . . .	9
2.14	Разрешение icmp . . . . .	9
2.15	Список контроля . . . . .	9
2.16	Доступ для other . . . . .	9
2.17	Доступ к сети оборудования . . . . .	10
2.18	проверка с dep . . . . .	10
2.19	проверка с dk . . . . .	11
2.20	проверка с admin . . . . .	12
2.21	Ноутбук администратора на повловской . . . . .	12
2.22	Права доступа администратора на повловской . . . . .	13
2.23	Проверка с администратора павловской . . . . .	14

# **1 Цель работы**

Освоить настройку прав доступа пользователей к ресурсам сети.

## 2 Выполнение лабораторной работы

- 1) В рабочей области проекта подключил ноутбук администратора к сети, чтобы разрешить ему потом любые действия, связанные с управлением сетью.

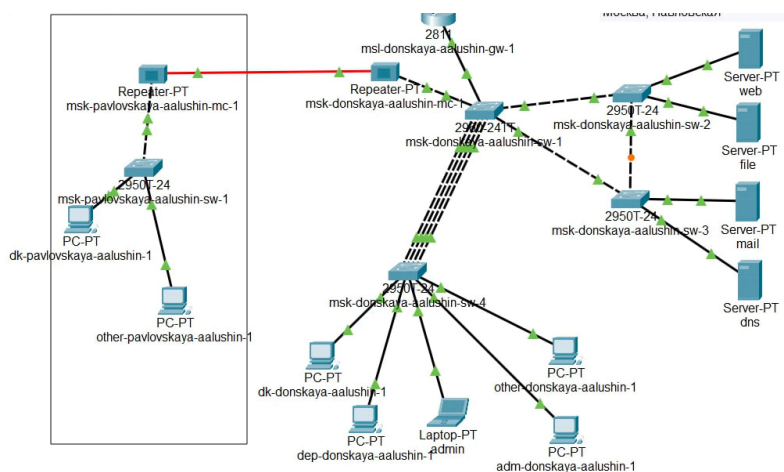


Рис. 2.1: Размещение ноутбука администратора

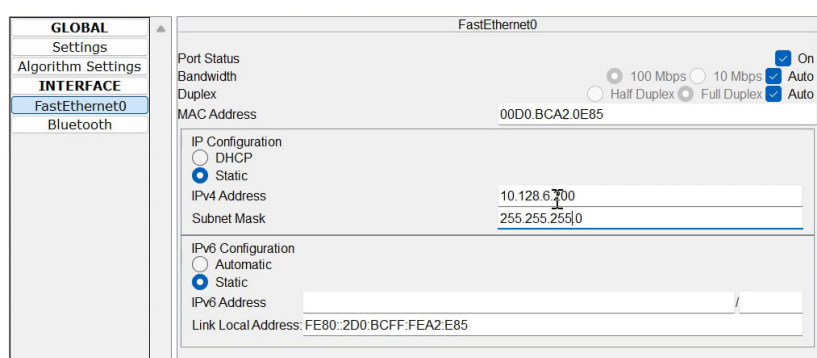


Рис. 2.2: Конфигурация ноутбука

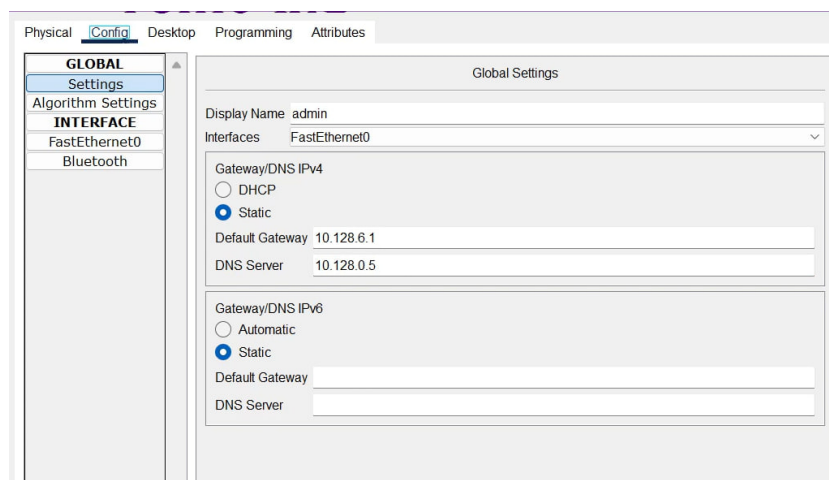


Рис. 2.3: Конфигурация ноутбука

2) Настроил доступ к web-серверу по протоколу tcp 80.

```
msk-donskaya-aalushin-gw-1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
msk-donskaya-aalushin-gw-1(config)#ip access-list extended servers-out
msk-donskaya-aalushin-gw-1(config-ext-nacl)#remark web
msk-donskaya-aalushin-gw-1(config-ext-nacl)#permit tcp any host 10.128.0.2 eq 80
msk-donskaya-aalushin-gw-1(config-ext-nacl)#
```

Рис. 2.4: Настройка доступа к web

3) Добавил список управления доступом к интерфейсу.

```
msk-donskaya-aalushin-gw-1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
msk-donskaya-aalushin-gw-1(config)#interface f0/0.3
msk-donskaya-aalushin-gw-1(config-subif)#ip access-group servers-out out
msk-donskaya-aalushin-gw-1(config-subif)#
```

Рис. 2.5: Добавление списка управления доступом

4) Настроил дополнительный доступ для администратора по протоколам telnet и ftp.

```
msk-donskaya-aalushin-gw-1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
msk-donskaya-aalushin-gw-1(config)#ip access-list extended servers-out
msk-donskaya-aalushin-gw-1(config-ext-nacl)#permit tcp host 10.128.6.200 host 10.128.0.2 range
20 ftp
msk-donskaya-aalushin-gw-1(config-ext-nacl)#permit tcp host 10.128.6.200 host 10.128.0.2 eq
telnet
msk-donskaya-aalushin-gw-1(config-ext-nacl)#
```

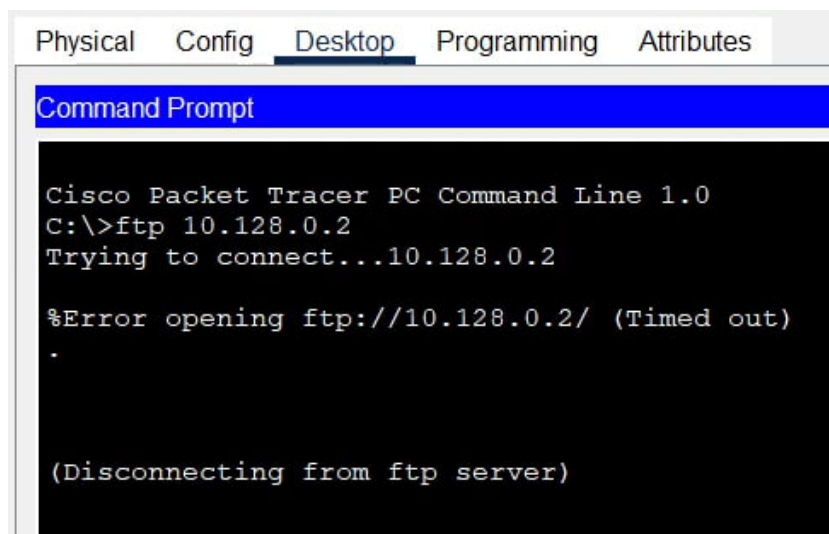
Рис. 2.6: ДОП доступ по протоколам

5) Убедился, что с узла 10.128.6.200 есть доступ по протоколу FTP.

```
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>
```

Рис. 2.7: Доступ по протоколу

6) Попробовал провести такую же процедуру с другого устройства сети. Увидел, что доступ запрещён.



The screenshot shows the 'Desktop' tab of a Cisco Packet Tracer PC. The 'Command Prompt' window displays the following text:

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ftp 10.128.0.2
Trying to connect...10.128.0.2

%Error opening ftp://10.128.0.2/ (Timed out)
.

(Disconnecting from ftp server)
```

Рис. 2.8: Доступ по протоколу

7) Настроил доступ к файловым серверам.

```
msk-donskaya-aalushin-gw-1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
msk-donskaya-aalushin-gw-1(config)#ip access-list extended servers-out
msk-donskaya-aalushin-gw-1(config-ext-nacl)#remark file
msk-donskaya-aalushin-gw-1(config-ext-nacl)#permit tcp 10.128.0.0 0.0.255.255 host 10.128.0.3 eq
445
msk-donskaya-aalushin-gw-1(config-ext-nacl)#permit tcp any host 10.128.0.3 range 20 ftp
msk-donskaya-aalushin-gw-1(config-ext-nacl)#
```

Рис. 2.9: Доступ к файловому серверу

#### 8) Настроил доступ к почтовому серверу.

```
msk-donskaya-aalushin-gw-1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
msk-donskaya-aalushin-gw-1(config)#ip access-list extended servers-out
msk-donskaya-aalushin-gw-1(config-ext-nacl)#remark mail
msk-donskaya-aalushin-gw-1(config-ext-nacl)#permit tcp any host 10.128.0.4 eq smtp
msk-donskaya-aalushin-gw-1(config-ext-nacl)#permit tcp any host 10.128.0.4 eq pop3
```

Рис. 2.10: Доступ к почтовому серверу

#### 9) Настроил доступ к DNS-серверу.

```
msk-donskaya-aalushin-gw-1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
msk-donskaya-aalushin-gw-1(config)#ip access-list extended servers-out
msk-donskaya-aalushin-gw-1(config-ext-nacl)#remark dns
msk-donskaya-aalushin-gw-1(config-ext-nacl)#permit udp 10.128.0.0 0.0.255.255 host 10.128.0.5 eq
53
msk-donskaya-aalushin-gw-1(config-ext-nacl)#
```

Рис. 2.11: Доступ к DNS

#### 10) Проверил работоспособность web сервера по ip-адресу и по имени сайта.

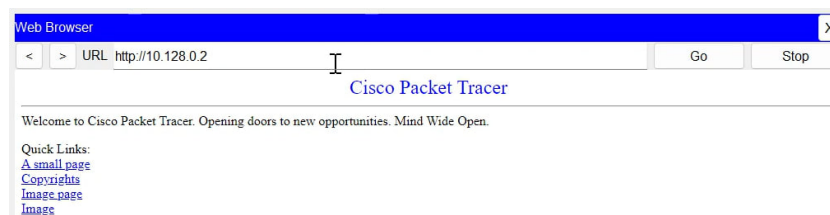


Рис. 2.12: web по ip-адресу





Рис. 2.13: web по имени

#### 11) Настроил разрешение на icmp-запросы.

```
msk-donskaya-aalushin-gw-1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
msk-donskaya-aalushin-gw-1(config)#ip access-list extended servers-out
msk-donskaya-aalushin-gw-1(config-ext-nacl)#1 permit icmp any any
msk-donskaya-aalushin-gw-1(config-ext-nacl)#
```

Рис. 2.14: Разрешение icmp

#### 12) Посмотрел номера строк правил в списке контроля.

```
msk-donskaya-aalushin-gw-1#show access-list
Extended IP access list servers-out
 1 permit icmp any any
10 permit tcp any host 10.128.0.2 eq www (21 match(es))
20 permit tcp host 10.128.6.200 host 10.128.0.2 range 20 ftp (15 match(es))
30 permit tcp host 10.128.6.200 host 10.128.0.2 eq telnet
40 permit tcp 10.128.0.0 0.0.255.255 host 10.128.0.3 eq 445
50 permit tcp any host 10.128.0.3 range 20 ftp
60 permit tcp any host 10.128.0.4 eq smtp
70 permit tcp any host 10.128.0.4 eq pop3
80 permit udp 10.128.0.0 0.0.255.255 host 10.128.0.5 eq domain (6 match(es))
msk-donskaya-aalushin-gw-1#
```

Рис. 2.15: Список контроля

#### 13) Настроил доступ для сети Other.

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

Рис. 2.16: Доступ для other

#### 14) Настроил доступ к сети сетевого оборудования.

```
msk-donskaya-aalushin-gw-1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
msk-donskaya-aalushin-gw-1(config)#ip access-list extended management-out
msk-donskaya-aalushin-gw-1(config-ext-nacl)#remark admin
msk-donskaya-aalushin-gw-1(config-ext-nacl)#permit ip host 10.128.6.200 10.128.1.0 0.0.0.255
msk-donskaya-aalushin-gw-1(config-ext-nacl)#exit
msk-donskaya-aalushin-gw-1(config)#int f0/0.2
msk-donskaya-aalushin-gw-1(config-subif)#ip access-group management-out out
msk-donskaya-aalushin-gw-1(config-subif)#
```

Рис. 2.17: Доступ к сети оборудования

- 15) Проверил установленные правила доступа, попытавшись получить доступ по различным протоколам с разных устройств. Пропинговать сервера получилось со всех устройств, а вот сетевое оборудование только с admin.

```
dep-donskaya-1 точка
Physical Config Desktop Programming Attributes
Command Prompt

Cisco Packet Tracer PC Command Line 1.0
C:\>ping 10.128.0.4

Pinging 10.128.0.4 with 32 bytes of data:

Request timed out.
Reply from 10.128.0.4: bytes=32 time<1ms TTL=127
Reply from 10.128.0.4: bytes=32 time<1ms TTL=127
Reply from 10.128.0.4: bytes=32 time<1ms TTL=127

Ping statistics for 10.128.0.4:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 10.128.0.2

Pinging 10.128.0.2 with 32 bytes of data:

Reply from 10.128.0.2: bytes=32 time<1ms TTL=127
Reply from 10.128.0.2: bytes=32 time<1ms TTL=127
Reply from 10.128.0.2: bytes=32 time<1ms TTL=127
Reply from 10.128.0.2: bytes=32 time<1ms TTL=127

Ping statistics for 10.128.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 10.128.1.2

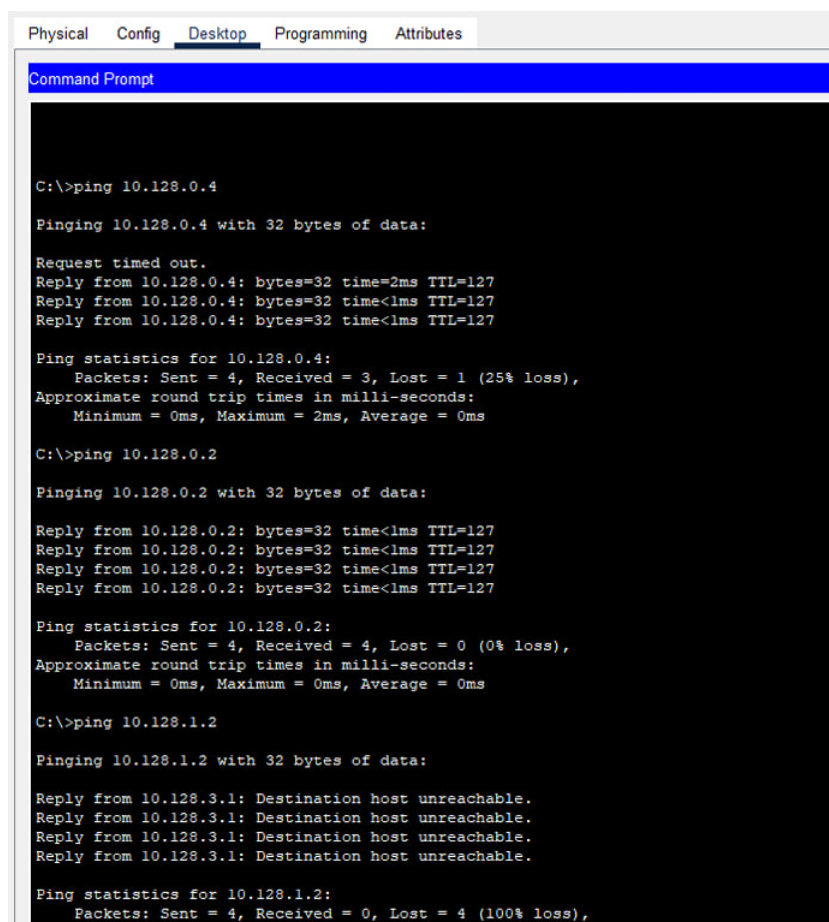
Pinging 10.128.1.2 with 32 bytes of data:

Reply from 10.128.4.1: Destination host unreachable.
Reply from 10.128.4.1: Destination host unreachable.
Reply from 10.128.4.1: Destination host unreachable.
Reply from 10.128.4.1: Destination host unreachable.

Ping statistics for 10.128.1.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

Рис. 2.18: проверка с dep



The screenshot shows a network configuration application with tabs for Physical, Config, Desktop, Programming, and Attributes. The 'Desktop' tab is active, displaying a 'Command Prompt' window. The window shows the results of three ping tests performed from the C:\ directory.

```
C:\>ping 10.128.0.4

Pinging 10.128.0.4 with 32 bytes of data:

Request timed out.
Reply from 10.128.0.4: bytes=32 time=2ms TTL=127
Reply from 10.128.0.4: bytes=32 time<1ms TTL=127
Reply from 10.128.0.4: bytes=32 time<1ms TTL=127

Ping statistics for 10.128.0.4:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 2ms, Average = 0ms

C:\>ping 10.128.0.2

Pinging 10.128.0.2 with 32 bytes of data:

Reply from 10.128.0.2: bytes=32 time<1ms TTL=127
Reply from 10.128.0.2: bytes=32 time<1ms TTL=127
Reply from 10.128.0.2: bytes=32 time<1ms TTL=127
Reply from 10.128.0.2: bytes=32 time<1ms TTL=127

Ping statistics for 10.128.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 10.128.1.2

Pinging 10.128.1.2 with 32 bytes of data:

Reply from 10.128.3.1: Destination host unreachable.
Reply from 10.128.3.1: Destination host unreachable.
Reply from 10.128.3.1: Destination host unreachable.
Reply from 10.128.3.1: Destination host unreachable.

Ping statistics for 10.128.1.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Рис. 2.19: проверка с dk

```

C:\>ping 10.128.0.4

Pinging 10.128.0.4 with 32 bytes of data:

Reply from 10.128.0.4: bytes=32 time<1ms TTL=127
Reply from 10.128.0.4: bytes=32 time=9ms TTL=127
Reply from 10.128.0.4: bytes=32 time=1ms TTL=127
Reply from 10.128.0.4: bytes=32 time<1ms TTL=127

Ping statistics for 10.128.0.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 9ms, Average = 2ms

C:\>ping 10.128.0.2

Pinging 10.128.0.2 with 32 bytes of data:

Reply from 10.128.0.2: bytes=32 time<1ms TTL=127
Reply from 10.128.0.2: bytes=32 time<1ms TTL=127
Reply from 10.128.0.2: bytes=32 time<1ms TTL=127
Reply from 10.128.0.2: bytes=32 time<1ms TTL=127

Ping statistics for 10.128.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 10.128.1.2

Pinging 10.128.1.2 with 32 bytes of data:

Request timed out.
Request timed out.
Reply from 10.128.1.2: bytes=32 time<1ms TTL=254
Reply from 10.128.1.2: bytes=32 time<1ms TTL=254

Ping statistics for 10.128.1.2:
    Packets: Sent = 4, Received = 2, Lost = 2 (50% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
  
```

Рис. 2.20: проверка с admin

- 16) Разрешил администратору из сети Other действия, аналогичные действиям администратора из другой сети.

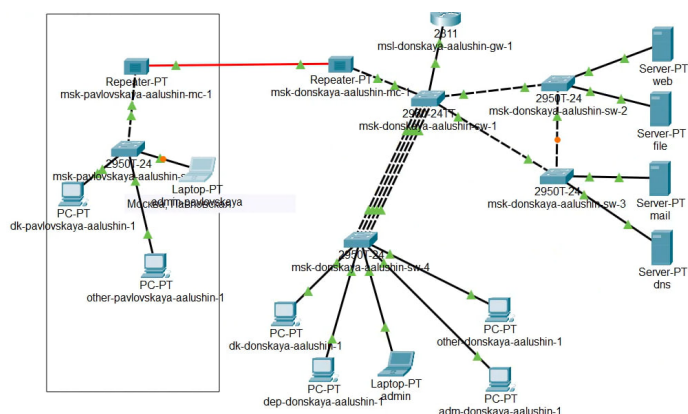


Рис. 2.21: Ноутбук администратора на повловской

```
msk-donskaya-aalushin-gw-1>en
Password:
msk-donskaya-aalushin-gw-1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
msk-donskaya-aalushin-gw-1(config)#ip access-list extended servers-out
msk-donskaya-aalushin-gw-1(config-ext-nacl)#permit tcp host 10.128.6.201 host 10.128.0.2 range
20 ftp
msk-donskaya-aalushin-gw-1(config-ext-nacl)#permit tcp host 10.128.6.201 host 10.128.0.2 eq
telnet
msk-donskaya-aalushin-gw-1(config-ext-nacl)#ip access-list extended other-in
msk-donskaya-aalushin-gw-1(config-ext-nacl)#remark admin
msk-donskaya-aalushin-gw-1(config-ext-nacl)#permit ip host 10.128.6.201 any
msk-donskaya-aalushin-gw-1(config-ext-nacl)#exit
msk-donskaya-aalushin-gw-1(config)#int f0/0.104
msk-donskaya-aalushin-gw-1(config-subif)#ip access-group other-in in
msk-donskaya-aalushin-gw-1(config-subif)#ip access-list extended management-out
msk-donskaya-aalushin-gw-1(config-ext-nacl)#remark admi-pavlovskaya
msk-donskaya-aalushin-gw-1(config-ext-nacl)#permit ip host 10.128.6.201 10.128.1.0 0.0.0.255
msk-donskaya-aalushin-gw-1(config-ext-nacl)#exit
msk-donskaya-aalushin-gw-1(config)#int f0/0.2
msk-donskaya-aalushin-gw-1(config-subif)#ip access-group management-out out
msk-donskaya-aalushin-gw-1(config-subif)#exit
msk-donskaya-aalushin-gw-1(config)#exi
```

Рис. 2.22: Права доступа администратора на повловской

17) Проверил корректность установленных правил доступа.

The screenshot shows a network configuration application with tabs for Physical, Config, Desktop, Programming, and Attributes. The 'Desktop' tab is active, displaying a 'Command Prompt' window. The window shows the execution of two ping commands and an ftp command. The first ping is to 10.128.0.2, showing successful results with 0% loss. The second ping is to 10.128.1.2, also showing successful results with 0% loss. The third command is an ftp connection to 10.128.0.2, which is successful, showing a welcome message and login status.

```
C:\>ping 10.128.0.2

Pinging 10.128.0.2 with 32 bytes of data:

Reply from 10.128.0.2: bytes=32 time<lms TTL=127
Reply from 10.128.0.2: bytes=32 time<lms TTL=127
Reply from 10.128.0.2: bytes=32 time<lms TTL=127
Reply from 10.128.0.2: bytes=32 time<lms TTL=127

Ping statistics for 10.128.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 10.128.1.2

Pinging 10.128.1.2 with 32 bytes of data:

Reply from 10.128.1.2: bytes=32 time<lms TTL=254
Reply from 10.128.1.2: bytes=32 time=8ms TTL=254
Reply from 10.128.1.2: bytes=32 time<lms TTL=254
Reply from 10.128.1.2: bytes=32 time<lms TTL=254

Ping statistics for 10.128.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 8ms, Average = 2ms

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>
```

Рис. 2.23: Проверка с администратора павловской

## **3 Выводы**

Я освоил настройку прав доступа пользователей к ресурсам сети.