

# **Отчёт по лабораторной работе №10**

**Администрирование локальных сетей**

Ищенко Ирина НПИбд-02-22

# Содержание

<b>1</b>	<b>Цель работы</b>	<b>5</b>
<b>2</b>	<b>Задание</b>	<b>6</b>
<b>3</b>	<b>Выполнение лабораторной работы</b>	<b>7</b>
<b>4</b>	<b>Выводы</b>	<b>18</b>
<b>5</b>	<b>Контрольные вопросы</b>	<b>19</b>
	<b>Список литературы</b>	<b>20</b>

# Список иллюстраций

3.1	Добавление ноутбука . . . . .	7
3.2	IP . . . . .	8
3.3	Шлюз и адрес DNS-сервера . . . . .	8
3.4	Проверка пинга до настройки . . . . .	9
3.5	Доступ к web-серверу по tcp 80 . . . . .	9
3.6	Список управления доступом к интерфейсу . . . . .	9
3.7	Проверка доступа по HTTP . . . . .	10
3.8	Проверка пингом . . . . .	10
3.9	Доступ для admin по Telnet и FTP . . . . .	11
3.10	Проверка FTP . . . . .	11
3.11	Проверка FTP . . . . .	11
3.12	Файловый, почтовый и DNS сервер . . . . .	12
3.13	Доступ для сети Other . . . . .	12
3.14	Доступ к сети сетевого оборудования . . . . .	12
3.15	Проверка доступа . . . . .	13
3.16	Проверка доступа . . . . .	14
3.17	Проверка доступа . . . . .	15
3.18	Размещение устройства . . . . .	16
3.19	Правила . . . . .	16
3.20	Список правил . . . . .	17
3.21	Проверка . . . . .	17

## **Список таблиц**

# 1 Цель работы

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

## 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.

### 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. 3.1) и присвоим ему статический адрес 10.128.6.200 (рис. 3.2), указав в качестве gateway-адреса 10.128.6.1 и адреса DNS-сервера 10.128.0.5 (рис. 3.3).

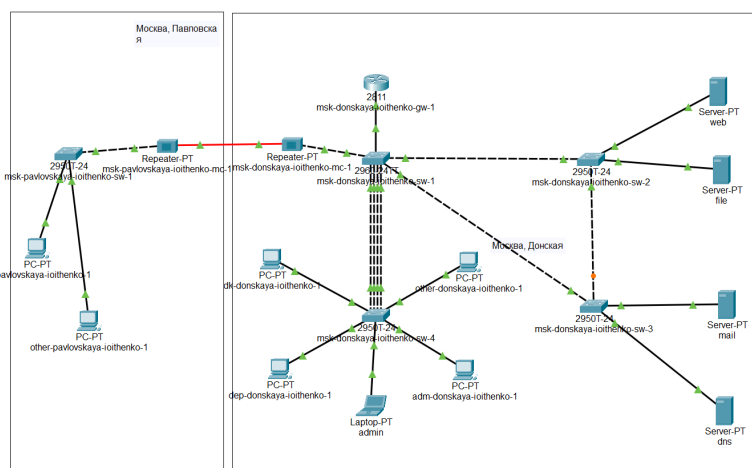


Рис. 3.1: Добавление ноутбука

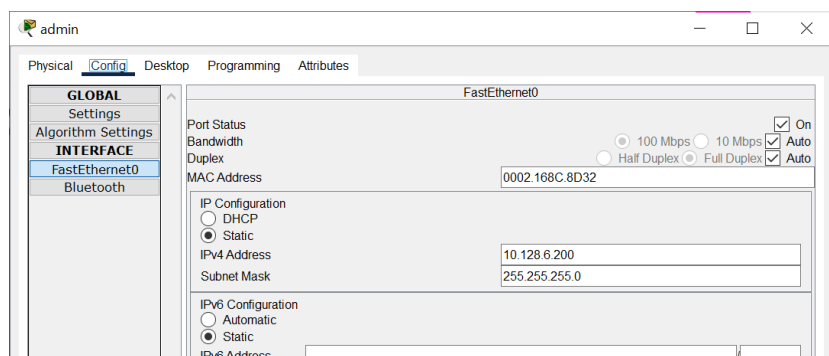


Рис. 3.2: IP

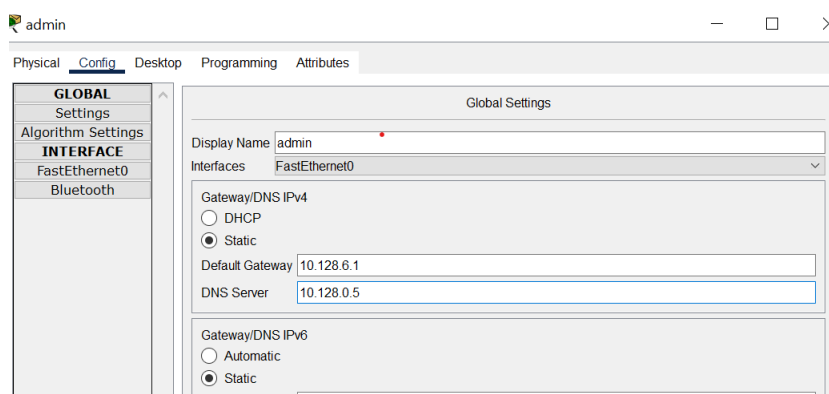


Рис. 3.3: Шлюз и адрес DNS-сервера

Проверим доступность устройств до настройки маршрутизатора (рис. 3.4).



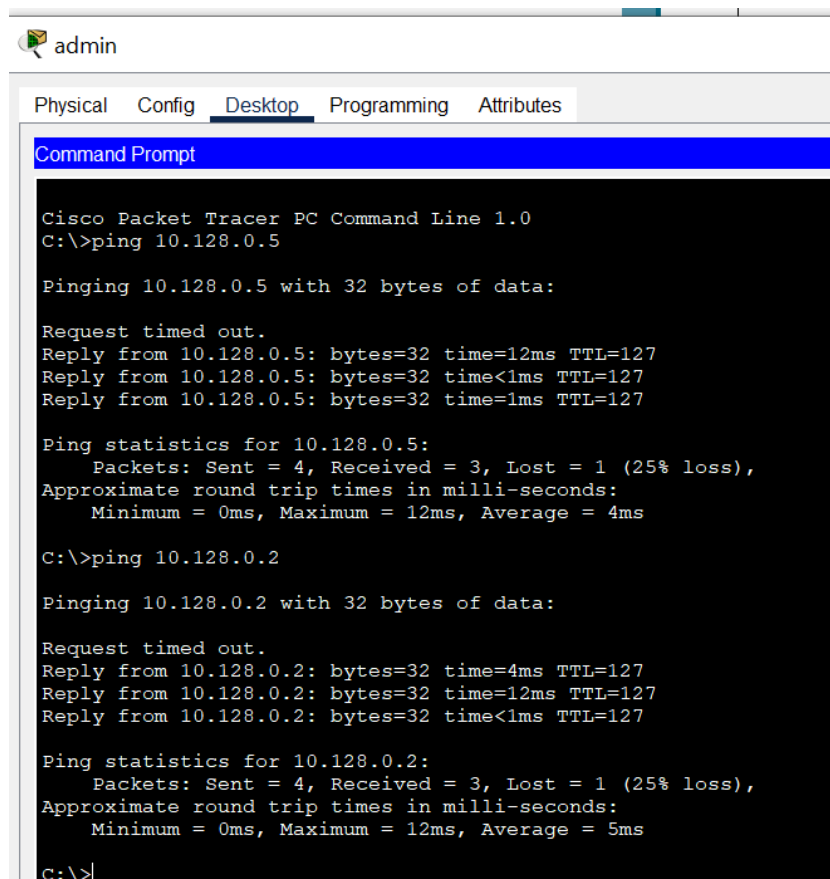


Рис. 3.4: Проверка пинга до настройки

Настроим доступа к web-серверу по порту tcp 80 (рис. 3.5).

```
msk-donskaya-ioithenko-gw-1>enable
Password:
msk-donskaya-ioithenko-gw-1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
msk-donskaya-ioithenko-gw-1(config)#ip access-list extended servers-out
msk-donskaya-ioithenko-gw-1(config-ext-nacl)#remark web
msk-donskaya-ioithenko-gw-1(config-ext-nacl)#permit tcp any host 10.128.0.2 eq 80
msk-donskaya-ioithenko-gw-1(config-ext-nacl)#^Z
msk-donskaya-ioithenko-gw-1#
%SYS-5-CONFIG_I: Configured from console by console
msk-donskaya-ioithenko-gw-1#
```

Рис. 3.5: Доступ к web-серверу по tcp 80

Добавим список управления доступом к интерфейсу (рис. 3.6).

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

Рис. 3.6: 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. 3.3).

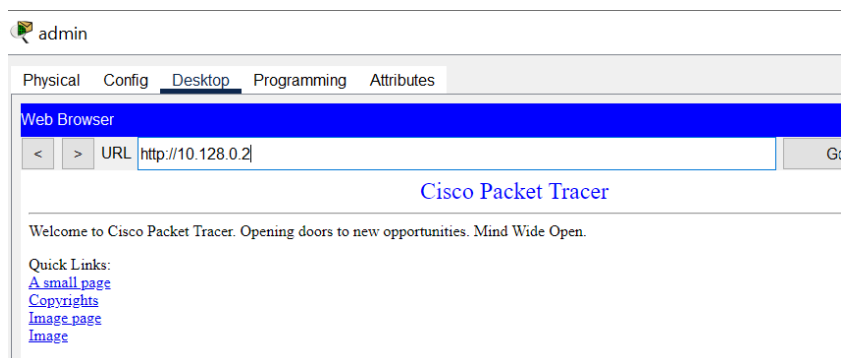


Рис. 3.7: Проверка доступа по HTTP

При этом команда ping будет демонстрировать недоступность web-сервера как по имени, так и по ip-адресу web-сервера (рис. 3.8).

```
C:\>ping 10.128.0.2

Pinging 10.128.0.2 with 32 bytes of data:

Reply from 10.128.6.1: Destination host unreachable.
Reply from 10.128.6.1: Destination host unreachable.
Reply from 10.128.6.1: Destination host unreachable.
Reply from 10.128.6.1: Destination host unreachable.

Ping statistics for 10.128.0.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 10.128.0.5

Pinging 10.128.0.5 with 32 bytes of data:

Reply from 10.128.6.1: Destination host unreachable.
Reply from 10.128.6.1: Destination host unreachable.
Reply from 10.128.6.1: Destination host unreachable.
Reply from 10.128.6.1: Destination host unreachable.

Ping statistics for 10.128.0.5:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

Рис. 3.8: Проверка пингом

Настроим дополнительный доступ для администратора по протоколам Telnet и FTP (рис. 3.9).

```

msk-donskaya-ioithenko-gw-1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
msk-donskaya-ioithenko-gw-1(config)#ip access-list extended servers-out
msk-donskaya-ioithenko-gw-1(config-ext-nacl)#permit tcp host 10.128.6.200 host 10.128.0.2
range 20 ftp
msk-donskaya-ioithenko-gw-1(config-ext-nacl)#permit tcp host 10.128.6.200 host 10.128.0.2 eq
telnet
msk-donskaya-ioithenko-gw-1(config-ext-nacl)#^Z
msk-donskaya-ioithenko-gw-1#
%SYS-5-CONFIG_I: Configured from console by console
msk-donskaya-ioithenko-gw-1#

```

Рис. 3.9: 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. 3.10).

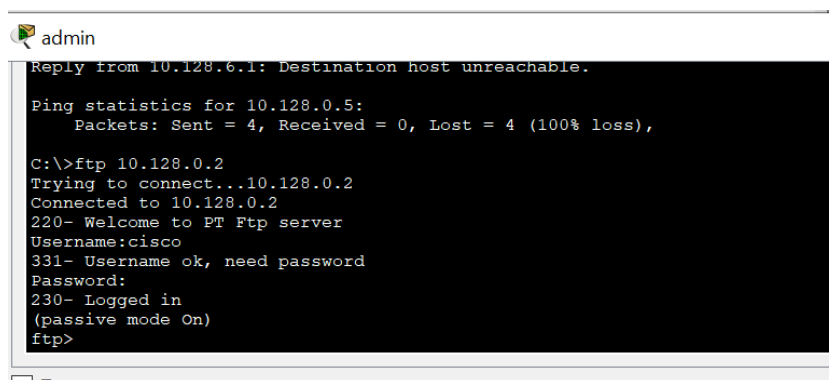


Рис. 3.10: Проверка FTP

Попробуем провести аналогичную процедуру с другого устройства сети. Убедимся, что доступ будет запрещён (рис. 3.11).

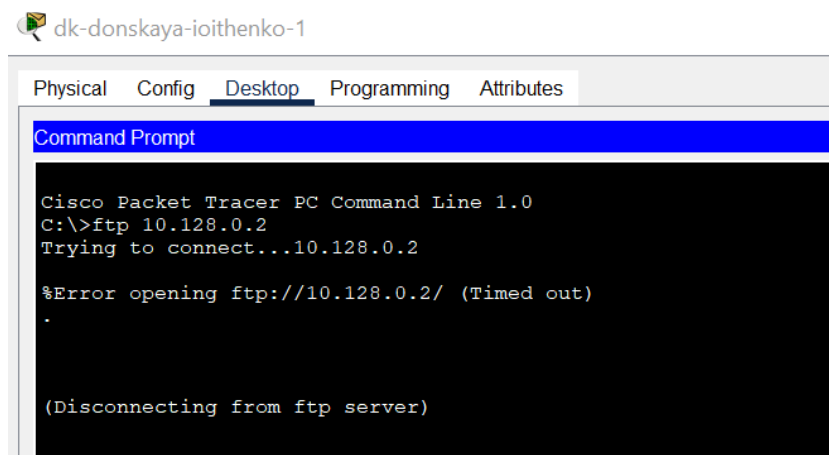


Рис. 3.11: Проверка FTP

Настроим доступ к файловому серверу. Настроим доступ к почтовому серверу, доступ к DNS-серверу. Разрешим icmp-запросы (рис. 3.12).

```
msk-donskaya-ioithenko-gw-1(config)#ip access-list extended servers-out
msk-donskaya-ioithenko-gw-1(config-ext-nacl)#remark file
msk-donskaya-ioithenko-gw-1(config-ext-nacl)#permit tcp 10.128.0.0 0.0.255.255 host 10.128.0.3
eq 445
msk-donskaya-ioithenko-gw-1(config-ext-nacl)#permit tcp any host 10.128.0.3 range 20 ftp
msk-donskaya-ioithenko-gw-1(config-ext-nacl)#^Z
msk-donskaya-ioithenko-gw-1#
%SYS-5-CONFIG_I: Configured from console by console

msk-donskaya-ioithenko-gw-1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
msk-donskaya-ioithenko-gw-1(config)#ip access-list extended servers-out
msk-donskaya-ioithenko-gw-1(config-ext-nacl)#remark mail
msk-donskaya-ioithenko-gw-1(config-ext-nacl)#permit tcp any host 10.128.0.4 eq smtp
msk-donskaya-ioithenko-gw-1(config-ext-nacl)#permit tcp any host 10.128.0.4 eq pop3
msk-donskaya-ioithenko-gw-1(config-ext-nacl)#^Z
msk-donskaya-ioithenko-gw-1#
%SYS-5-CONFIG_I: Configured from console by console

msk-donskaya-ioithenko-gw-1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
msk-donskaya-ioithenko-gw-1(config)#ip access-list extended servers-out
msk-donskaya-ioithenko-gw-1(config-ext-nacl)#remark dns
msk-donskaya-ioithenko-gw-1(config-ext-nacl)#permit udp 10.128.0.0 0.0.255.255 host 10.128.0.5
eq 53
msk-donskaya-ioithenko-gw-1(config-ext-nacl)#^Z
msk-donskaya-ioithenko-gw-1#
%SYS-5-CONFIG_I: Configured from console by console

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

Рис. 3.12: 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. 3.13).

```
msk-donskaya-ioithenko-gw-1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
msk-donskaya-ioithenko-gw-1(config)#ip access-list extended other-in
msk-donskaya-ioithenko-gw-1(config-ext-nacl)#remark admin
msk-donskaya-ioithenko-gw-1(config-ext-nacl)#permit ip host 10.128.6.200 any
msk-donskaya-ioithenko-gw-1(config-ext-nacl)#exit
msk-donskaya-ioithenko-gw-1(config)#interface f0/0.104
^
% Invalid input detected at '^' marker.

msk-donskaya-ioithenko-gw-1(config)#interface f0/0.104
msk-donskaya-ioithenko-gw-1(config-subif)#ip access group other in in
^
% Invalid input detected at '^' marker.

msk-donskaya-ioithenko-gw-1(config-subif)#ip access-group other-in in
msk-donskaya-ioithenko-gw-1(config-subif)#
```

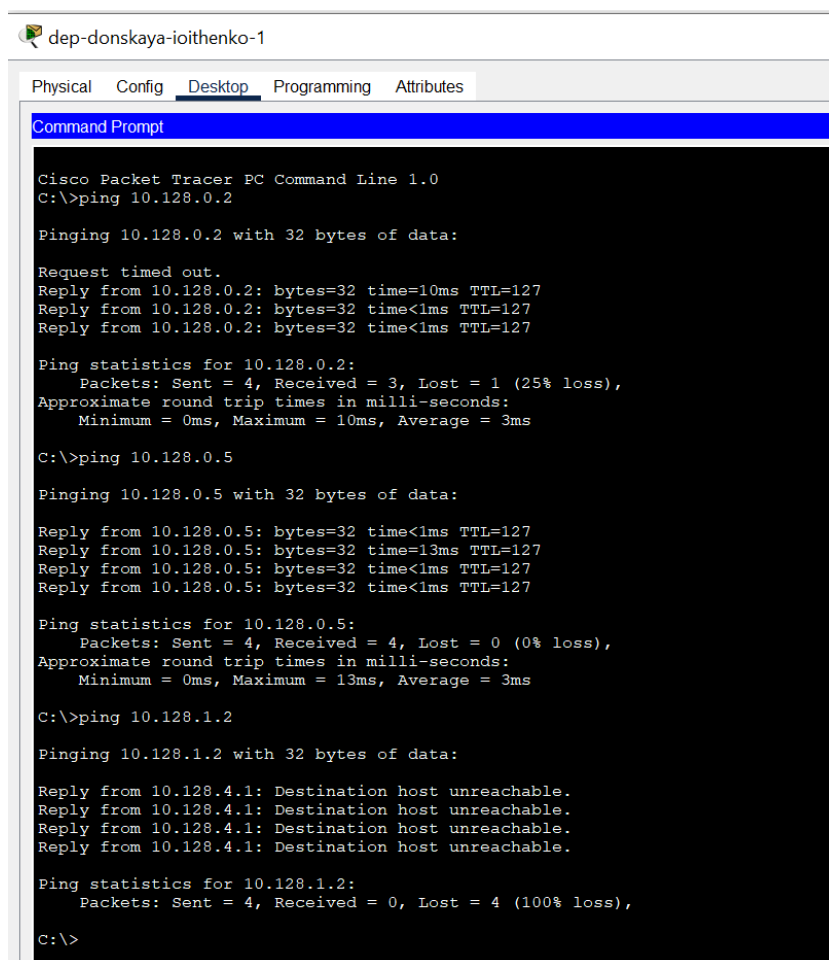
Рис. 3.13: Доступ для сети Other

Настроим доступ администратора к сети сетевого оборудования (рис. 3.14).

```
msk-donskaya-ioithenko-gw-1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
msk-donskaya-ioithenko-gw-1(config)#ip access-list extended management-out
msk-donskaya-ioithenko-gw-1(config-ext-nacl)#remark admin
msk-donskaya-ioithenko-gw-1(config-ext-nacl)#permit ip host 10.128.6.200 10.128.1.0 0.0.255.255
msk-donskaya-ioithenko-gw-1(config-ext-nacl)#exit
msk-donskaya-ioithenko-gw-1(config)#interface f0/0.2
msk-donskaya-ioithenko-gw-1(config-subif)#ip access-group management-out out
msk-donskaya-ioithenko-gw-1(config-subif)#^Z
msk-donskaya-ioithenko-gw-1#
%SYS-5-CONFIG_I: Configured from console by console
```

Рис. 3.14: 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 пропиnguем разные устройства. Увидим, что серверы и другие конечные устройства пингуются, однако к сетевому оборудованию доступа нет, как и должно быть. (рис. 3.15).



```
dep-donskaya-ioithenko-1
Physical Config Desktop Programming Attributes
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 10.128.0.2

Pinging 10.128.0.2 with 32 bytes of data:

Request timed out.
Reply from 10.128.0.2: bytes=32 time=10ms 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 = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 10ms, Average = 3ms

C:\>ping 10.128.0.5

Pinging 10.128.0.5 with 32 bytes of data:

Reply from 10.128.0.5: bytes=32 time<1ms TTL=127
Reply from 10.128.0.5: bytes=32 time=13ms TTL=127
Reply from 10.128.0.5: bytes=32 time<1ms TTL=127
Reply from 10.128.0.5: bytes=32 time<1ms TTL=127

Ping statistics for 10.128.0.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 13ms, Average = 3ms

C:\>ping 10.128.1.2

Pinging 10.128.1.2 with 32 bytes of data:

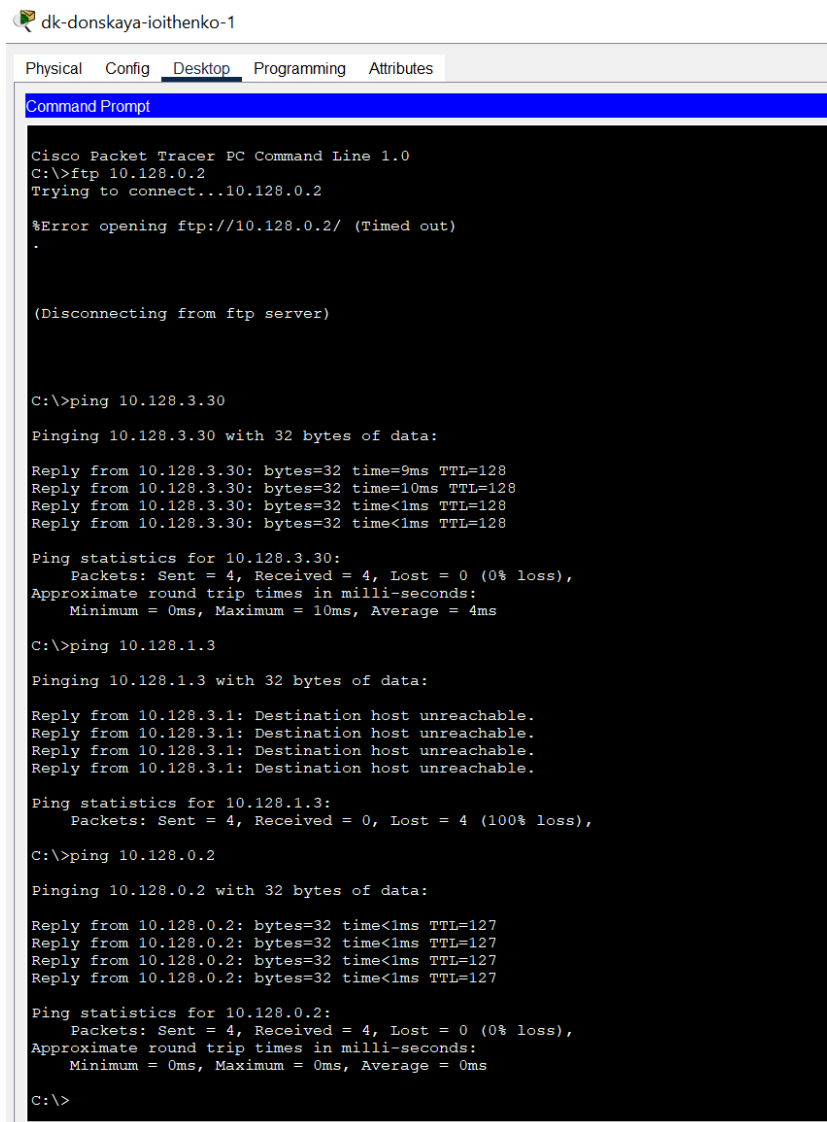
Reply from 10.128.4.1: Destination host unreachable.
Reply from 10.128.4.1: Destination host unreachable.
Reply from 10.128.4.1: Destination host unreachable.
Reply from 10.128.4.1: Destination host unreachable.

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

C:\>
```

Рис. 3.15: Проверка доступа

Откроем терминал dk-donskaya-dmbelicheva-1 и пропиnguем разные устройства. Увидим, что серверы и другие конечные устройства пингуются, однако к сетевому оборудованию доступа нет, как и должно быть. Также попробуем подключиться к web-серверу по ftp, доступ закрыт (рис. 3.16).



The screenshot shows a Cisco Packet Tracer PC Command Line 1.0 window with tabs for Physical, Config, Desktop, Programming, and Attributes. The Desktop tab is active, displaying a Command Prompt. The user has attempted to connect to 10.128.0.2 via ftp, which failed with a 'Timed out' error. Subsequently, the user performed ping tests to three different IP addresses: 10.128.3.30, 10.128.1.3, and 10.128.0.2. The ping to 10.128.3.30 was successful, while the ping to 10.128.1.3 failed with 100% loss. The ping to 10.128.0.2 was also successful.

```
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)

C:\>ping 10.128.3.30

Pinging 10.128.3.30 with 32 bytes of data:

Reply from 10.128.3.30: bytes=32 time=9ms TTL=128
Reply from 10.128.3.30: bytes=32 time=10ms TTL=128
Reply from 10.128.3.30: bytes=32 time<1ms TTL=128
Reply from 10.128.3.30: bytes=32 time<1ms TTL=128

Ping statistics for 10.128.3.30:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 10ms, Average = 4ms

C:\>ping 10.128.1.3

Pinging 10.128.1.3 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 10.128.1.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 10.128.0.2

Pinging 10.128.0.2 with 32 bytes of data:

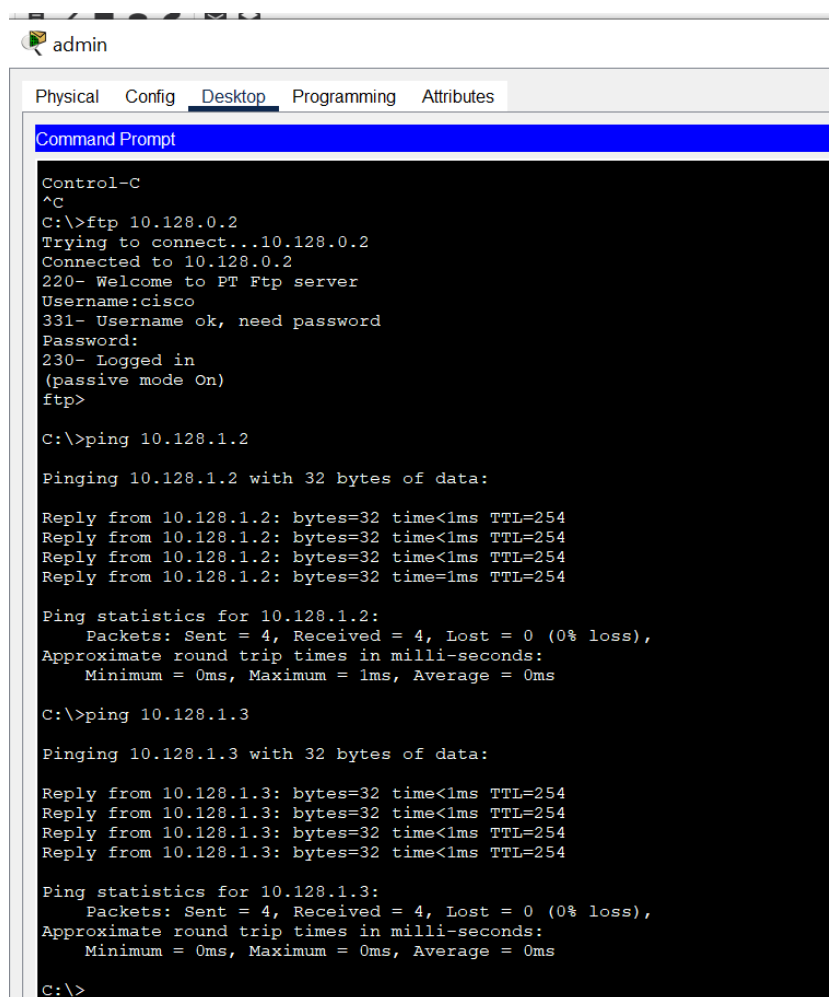
Reply from 10.128.0.2: bytes=32 time<1ms TTL=127
Reply from 10.128.0.2: bytes=32 time<1ms TTL=127
Reply from 10.128.0.2: bytes=32 time<1ms TTL=127
Reply from 10.128.0.2: bytes=32 time<1ms TTL=127

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:\>
```

Рис. 3.16: Проверка доступа

Теперь проверим корректность настроенного доступа с admin. Есть доступ к серверу по ftp, а также успешно пингуется сетевое оборудование (рис. 3.17).



```
admin
Physical Config Desktop Programming Attributes
Command Prompt
Control-C
^C
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 10.128.1.2
Pinging 10.128.1.2 with 32 bytes of data:
Reply from 10.128.1.2: bytes=32 time<1ms TTL=254
Reply from 10.128.1.2: bytes=32 time<1ms TTL=254
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 = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
C:\>ping 10.128.1.3
Pinging 10.128.1.3 with 32 bytes of data:
Reply from 10.128.1.3: bytes=32 time<1ms TTL=254
Reply from 10.128.1.3: bytes=32 time<1ms TTL=254
Reply from 10.128.1.3: bytes=32 time<1ms TTL=254
Reply from 10.128.1.3: bytes=32 time<1ms TTL=254
Ping statistics for 10.128.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>
```

Рис. 3.17: Проверка доступа

Разместим еще один ноутбук admin на Павловской (рис. 3.18).

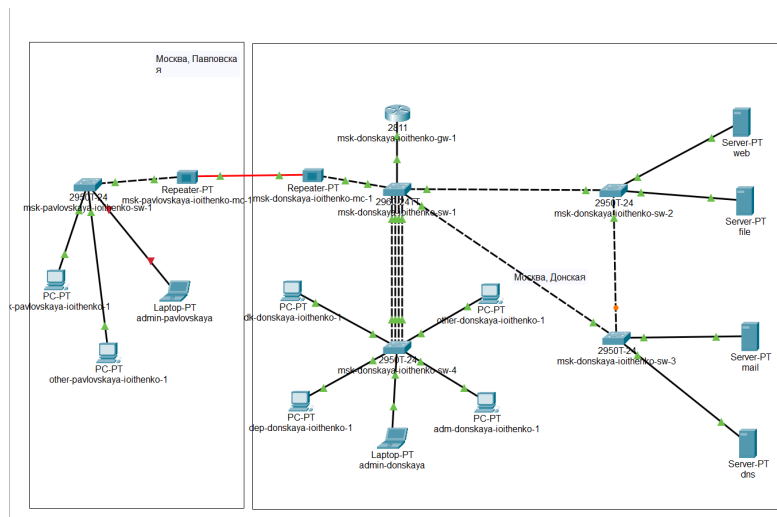


Рис. 3.18: Размещение устройства

Разрешим администратору из сети Other на Павловской действия, аналогичные действиям администратора сети Other на Донской (рис. 3.19).

```
msk-donskaya-ioithenko-gw-1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
msk-donskaya-ioithenko-gw-1(config)#ip access-list extended servers-out
msk-donskaya-ioithenko-gw-1(config-ext-nacl)#permit tcp host 10.128.6.201 host 10.128.0.2 range
20 ftp
msk-donskaya-ioithenko-gw-1(config-ext-nacl)#permit tcp host 10.128.6.201 host 10.128.0.2 eq
telnet
msk-donskaya-ioithenko-gw-1(config-ext-nacl)#exit
msk-donskaya-ioithenko-gw-1(config)#ip access-list extended other-in
msk-donskaya-ioithenko-gw-1(config-ext-nacl)#remark admin
msk-donskaya-ioithenko-gw-1(config-ext-nacl)#permit ip host 10.128.6.201 any
msk-donskaya-ioithenko-gw-1(config-ext-nacl)#exit
msk-donskaya-ioithenko-gw-1(config)#interface f0/0.104
msk-donskaya-ioithenko-gw-1(config-subif)#ip access-group other-in in
msk-donskaya-ioithenko-gw-1(config-subif)#exit
msk-donskaya-ioithenko-gw-1(config)#ip access-list extended management-out
msk-donskaya-ioithenko-gw-1(config-ext-nacl)#remark admin
msk-donskaya-ioithenko-gw-1(config-ext-nacl)#permit ip host 10.128.6.201 10.128.1.0 0.0.0.255
msk-donskaya-ioithenko-gw-1(config-ext-nacl)#exit
msk-donskaya-ioithenko-gw-1(config)#interface f0/0.2
msk-donskaya-ioithenko-gw-1(config-subif)#ip access-group management-out out
msk-donskaya-ioithenko-gw-1(config-subif)#^Z
%SYS-5-CONFIG_I: Configured from console by console
msk-donskaya-ioithenko-gw-1#
```

Рис. 3.19: Правила

Посмотрим список правил в нашей сети. После выполнения была изменена обратная маска в правилах для их корректной работы (рис. 3.20).



```

msk-donskaya-ioithenko-gw-1#show access-lists
Extended IP access list servers-out
 1 permit icmp any any
10 permit tcp any host 10.128.0.2 eq www
20 permit tcp host 10.128.6.200 host 10.128.0.2 range 20 ftp
30 permit tcp host 10.128.6.200 host 10.128.0.2 eq telnet
40 permit tcp 10.128.0.0 0.0.0.255 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 0.0.0.255 host 10.128.0.5 eq domain
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 10.128.0.0 0.0.0.255
20 permit ip host 10.128.6.201 10.128.1.0 0.0.0.255
msk-donskaya-ioithenko-gw-1#

```

Рис. 3.20: Список правил

Проверим работу устройства администратора (рис. 3.21).

```

admin-pavlovskaya
Physical Config Desktop Programming Attributes
Command Prompt
C:\>ping -n 2 10.128.3.30

Pinging 10.128.3.30 with 32 bytes of data:

Reply from 10.128.3.30: bytes=32 time<1ms TTL=127
Reply from 10.128.3.30: bytes=32 time<1ms TTL=127

Ping statistics for 10.128.3.30:
    Packets: Sent = 2, Received = 2, 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<1ms TTL=254
Reply from 10.128.1.2: bytes=32 time<1ms TTL=254
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 = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

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)

```

Рис. 3.21: 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`.

2. Как задать действие правила сразу для нескольких портов?

Для этого нужна команда `interface range`.

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?

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.