

# **Отчёт по лабораторной работе №10**

**Дисциплина: Администрирование локальных сетей**

**Выполнил: Танрибергенов Эльдар**

# Содержание

1	Цель работы	5
2	Задание	6
3	Выполнение лабораторной работы	7
4	Ответы на контрольные вопросы	21
5	Выводы	22

## Список иллюстраций

3.1	Размещение ноутбука администратора в сети other-donskaya-1 . .	7
3.2	Присвоение статического ip-адреса ноутбука . . . . .	8
3.3	Указание адресов шлюза и DNS-сервера . . . . .	8
3.4	Настройка доступа к web-серверу по порту http (tcp 80) . . . . .	9
3.5	Подключение списка прав доступа к интерфейсу и применение к исходящему трафику . . . . .	9
3.6	Проверка доступа к web-серверу через протокол HTTP . . . . .	10
3.7	Проверка недоступности web-сервера по команде ping . . . . .	10
3.8	Добавление разрешения устройству администратору на доступ на web-сервер по протоколам FTP и telnet . . . . .	11
3.9	Проверка доступа администратора к web-серверу по протоколу FTP	11
3.10	Проверка доступа другого устройства сети к web-серверу по протоколу FTP . . . . .	12
3.11	Настройка доступа к файловому серверу . . . . .	12
3.12	Настройка доступа к почтовому серверу . . . . .	13
3.13	Настройка доступа к DNS-серверу . . . . .	13
3.14	Проверка доступа к DNS-серверу . . . . .	13
3.15	Разрешение icmp-запросов всем узлам в сети . . . . .	14
3.16	Проверка размещения правила первым в списке . . . . .	14
3.17	Проверка доступности icmp-запросов в сети . . . . .	14
3.18	Настройка доступа для сети other . . . . .	15
3.19	Настройка доступа администратора к сети сетевого оборудования	15
3.20	Проверка доступа к web-серверу устройства из сети other . . . . .	16
3.21	Проверка доступа к сетевому оборудованию устройства из сети other	16
3.22	Проверка доступа администратора к сети сетевого оборудования	17
3.23	Проверка доступа администратора к сети сетевого оборудования	17
3.24	Размещение ноутбука администратора на Павловской . . . . .	18
3.25	Настройка интерфейса коммутатора на Павловской . . . . .	18
3.26	IP-адреса шлюза и dns-сервера ноутбука администратора на Павловской . . . . .	19
3.27	IP-адрес ноутбука администратора на Павловской . . . . .	19
3.28	Правила для администратора на Павловской в списках доступа . .	20
3.29	Проверка правильности работы правил . . . . .	20

## **Список таблиц**

# **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. Проверить правильность действия установленных правил доступа.

3. Выполнить задание для самостоятельной работы по настройке прав доступа администратора сети на Павловской.

### 3 Выполнение лабораторной работы

1. В рабочей области проекта подключил ноутбук к порту 24 коммутатора msk-donskaya-sw-4 (рис. 3.1) и присвоил 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).

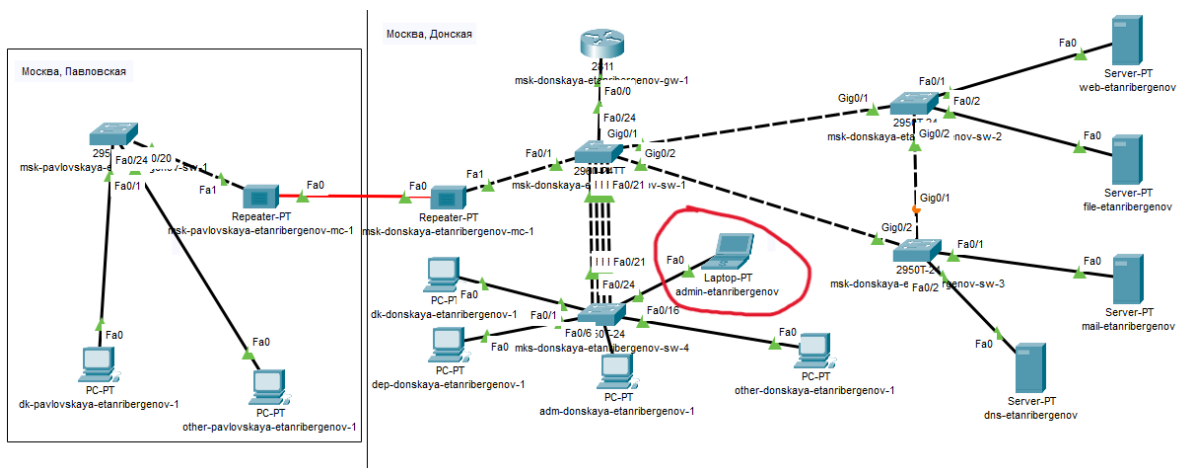


Рис. 3.1: Размещение ноутбука администратора в сети other-donskaya-1

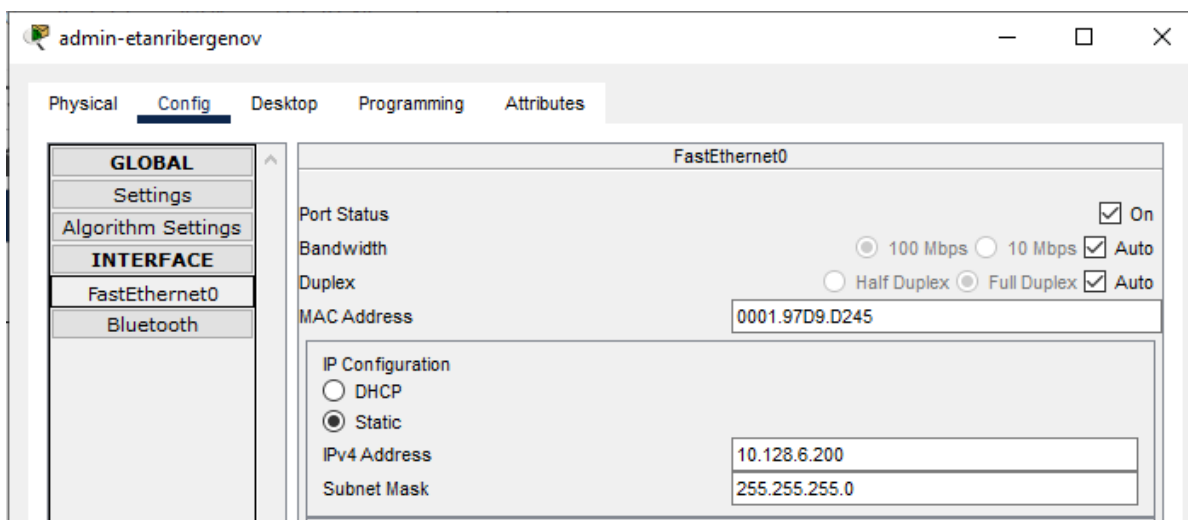


Рис. 3.2: Присвоение статического ip-адреса ноутбука

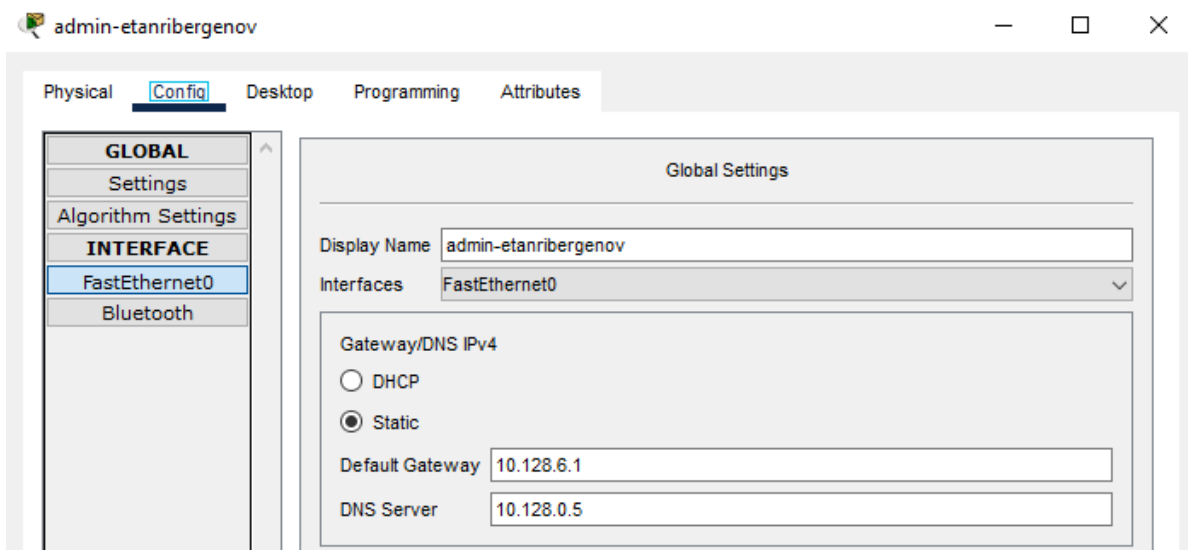


Рис. 3.3: Указание адресов шлюза и DNS-сервера

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

Создал список контроля доступа с названием servers-out (так как предполагается ограничить доступ в конкретные подсети и по отношению к маршрутизатору это будет исходящий трафик); указал (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.

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

Рис. 3.4: Настройка доступа к web-серверу по порту http (tcp 80)

### 3. Добавление списка управления доступом к интерфейсу:

К интерфейсу f0/0.3 подключил список прав доступа servers-out и применил к исходящему трафику (out) (рис. 3.5). Проверил, что доступ к web-серверу есть через протокол HTTP (введя в строке браузера хоста ip-адрес web-сервера) (рис. 3.6). При этом команда ping демонстрирует недоступность web-сервера как по имени, так и по ip-адресу web-сервера (рис. 3.7).

```
msk-donskaya-etanribergenov-gw-1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
msk-donskaya-etanribergenov-gw-1(config)#interface f0/0.3
msk-donskaya-etanribergenov-gw-1(config-subif)#ip access-group servers-out out
msk-donskaya-etanribergenov-gw-1(config-subif)#^Z
msk-donskaya-etanribergenov-gw-1#
%SYS-5-CONFIG_I: Configured from console by console

msk-donskaya-etanribergenov-gw-1#wr mem
Building configuration...
[OK]
```

Рис. 3.5: Подключение списка прав доступа к интерфейсу и применение к исходящему трафику



Рис. 3.6: Проверка доступа к web-серверу через протокол HTTP

```
C:\>ping 10.128.0.2

Pinging 10.128.0.2 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 10.128.0.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
C:\>ping www-etanribergenov.donskaya.rudn.edu
C:\>
```

Рис. 3.7: Проверка недоступности web-сервера по команде ping

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

В список контроля доступа servers-out добавил 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. 3.8). Убедился, что с узла с ip-адресом 10.128.6.200 есть доступ по протоколу FTP. Для этого в командной строке устройства администратора ввёл ftp 10.128.0.2, а затем по запросу имя пользователя cisco и пароль cisco (рис. 3.9).

```

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

msk-donskaya-etanribergenov-gw-1#wr mem
Building configuration...
[OK]

```

Рис. 3.8: Добавление разрешения устройству администратору на доступ на web-сервер по протоколам FTP и telnet

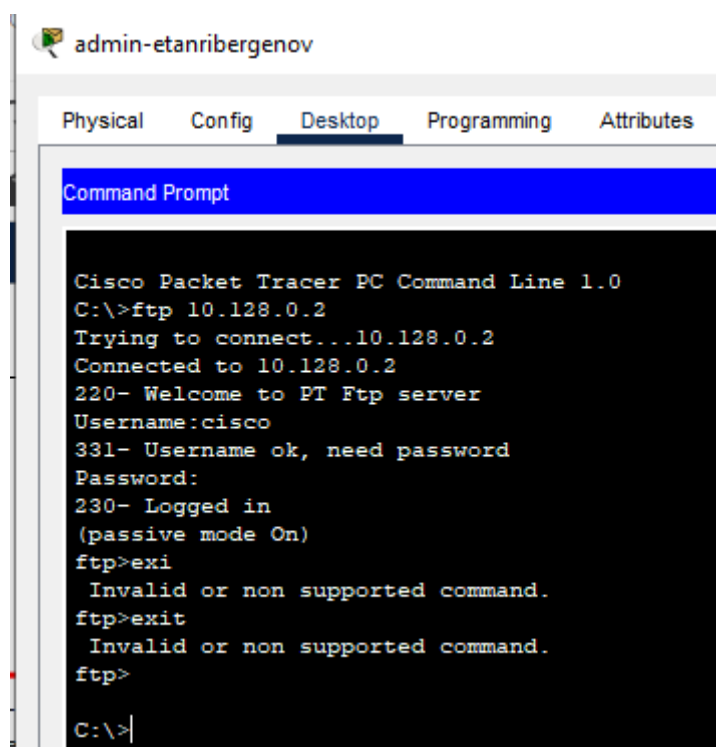


Рис. 3.9: Проверка доступа администратора к web-серверу по протоколу FTP

Попробовал провести аналогичную процедуру с другого устройства сети. Убедился, что доступ запрещён.

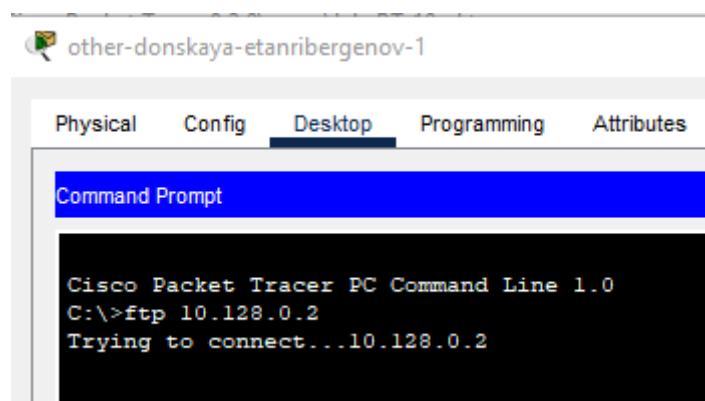


Рис. 3.10: Проверка доступа другого устройства сети к web-серверу по протоколу FTP

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

В списке контроля доступа `servers-out` указал (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`).

```
msk-donskaya-etanribergenov-gw-1(config)#ip access-list extended servers-out
msk-donskaya-etanribergenov-gw(config-ext-nacl)#remark file
msk-donskaya-etanribergenov-gw(config-ext-nacl)#permit tcp 10.128.0.0 0.0.255.255 host 10.128.0.3
eq 445
msk-donskaya-etanribergenov-gw(config-ext-nacl)#permit tcp any host 10.128.0.3 range 20 ftp
msk-donskaya-etanribergenov-gw(config-ext-nacl)#
```

Рис. 3.11: Настройка доступа к файловому серверу

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

В списке контроля доступа `servers-out` указал (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.

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

Рис. 3.12: Настройка доступа к почтовому серверу

## 7. Настройка доступа к DNS-серверу:

В списке контроля доступа servers-out указал (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. 3.13). Проверил доступность web-сервера (через браузер) по имени (рис. 3.14).

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

Рис. 3.13: Настройка доступа к DNS-серверу

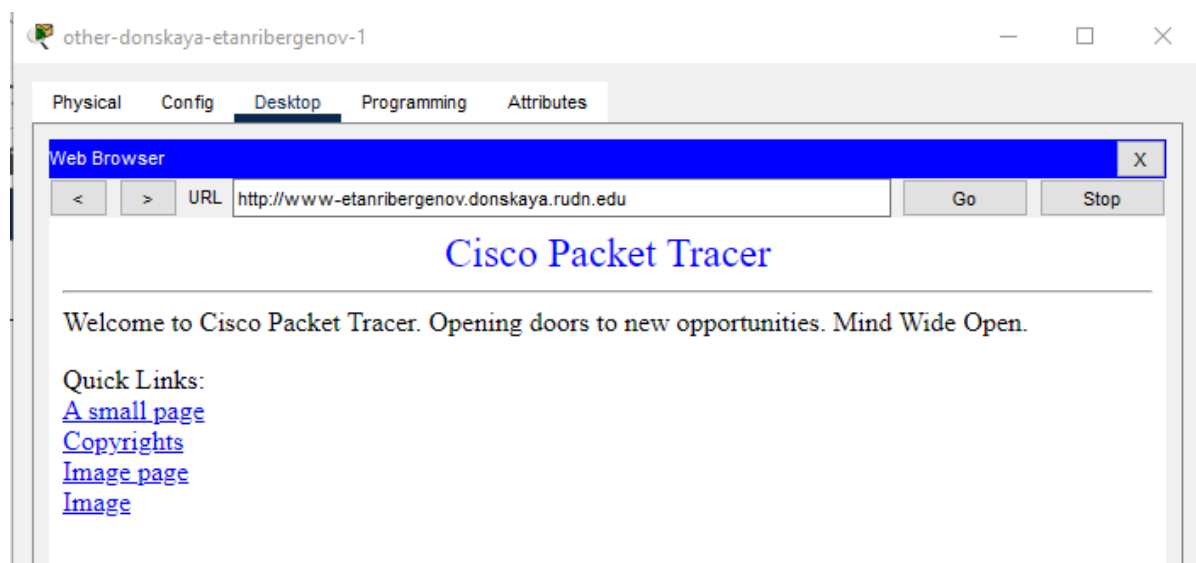


Рис. 3.14: Проверка доступа к DNS-серверу

## 8. Разрешение icstr-запросов:

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

Рис. 3.15: Разрешение істр-запросов всем узлам в сети

Явно указал порядок размещения правил — правило разрешения для істр-запросов добавил в начало списка контроля доступа (рис. 3.16).

```
msk-donskaya-etanribergenov-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 (28 match(es))
20 permit tcp host 10.128.6.200 host 10.128.0.2 range 20 ftp (7 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 (3 match(es))
msk-donskaya-etanribergenov-gw-1#
```

Рис. 3.16: Проверка размещения правила первым в списке

Проверил, что істр-запросы доступны (рис. 3.17).

```
C:\>ping www-etanribergenov.donskaya.rudn.edu

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=9ms 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 = 9ms, Average = 2ms

C:\>
```

Рис. 3.17: Проверка доступности істр-запросов в сети

9. Настройка доступа для сети Other (наложил ограничение на исходящий из сети Other трафик, который по отношению к маршрутизатору 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).

```
msk-donskaya-etanribergenov-gw-1(config)#ip access-list extended other-in
msk-donskaya-etanribergenov-gw-1(config-ext-nacl)#remark admin
msk-donskaya-etanribergenov-gw-1(config-ext-nacl)#permit ip host 10.128.6.200 any
msk-donskaya-etanribergenov-gw-1(config-ext-nacl)#exit
msk-donskaya-etanribergenov-gw-1(config)#
msk-donskaya-etanribergenov-gw-1(config)#interface f0/0.104
msk-donskaya-etanribergenov-gw-1(config-subif)#ip access-group other-in in
msk-donskaya-etanribergenov-gw-1(config-subif)#
```

Рис. 3.18: Настройка доступа для сети other

#### 10. Настройка доступа администратора к сети сетевого оборудования:

В списке контроля доступа management-out указал (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).

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

Рис. 3.19: Настройка доступа администратора к сети сетевого оборудования

#### 11. Проверил корректность установленных правил доступа, попытавшись получить доступ по различным протоколам с разных устройств сети к подсети серверов и подсети сетевого оборудования.

Проверил правильность работы установленных правил доступа, попытавшись получить доступ с устройства из сети other. Убедился, что доступ запрещён.

К серверу:

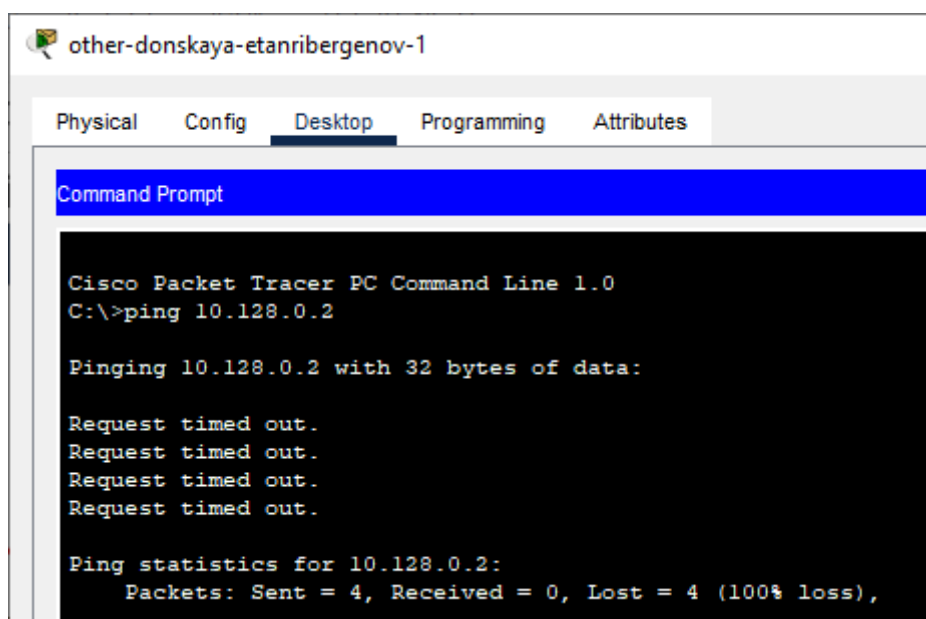


Рис. 3.20: Проверка доступа к web-серверу устройства из сети other

К сетевому оборудованию:

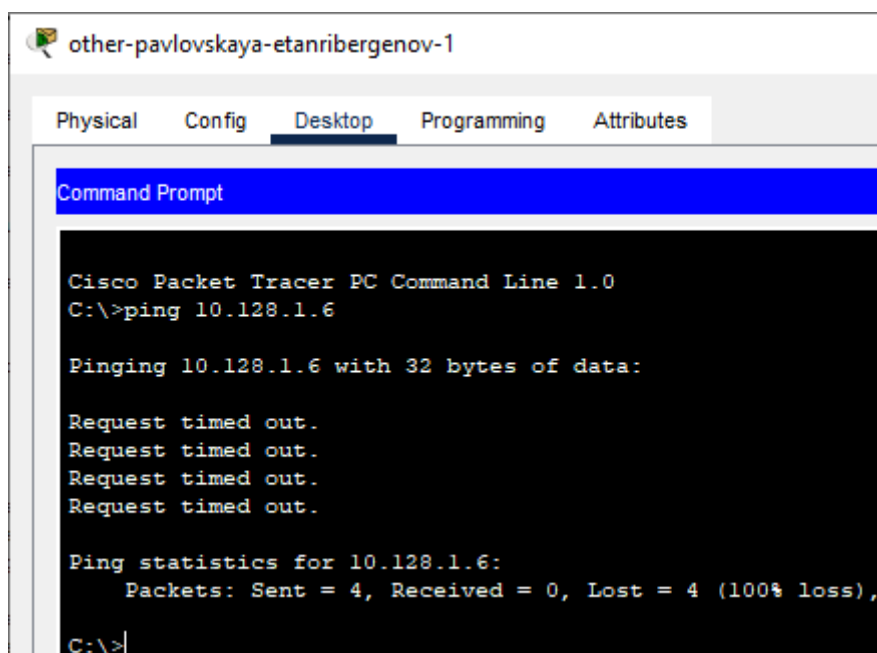


Рис. 3.21: Проверка доступа к сетевому оборудованию устройства из сети other

Проверил правильность работы установленных правил доступа, попытыв-



шись получить доступ с устройства администратора. Убедился, что доступ разрешён.

К серверу:

```
C:\>ping www-etanribergenov.donskaya.rudn.edu

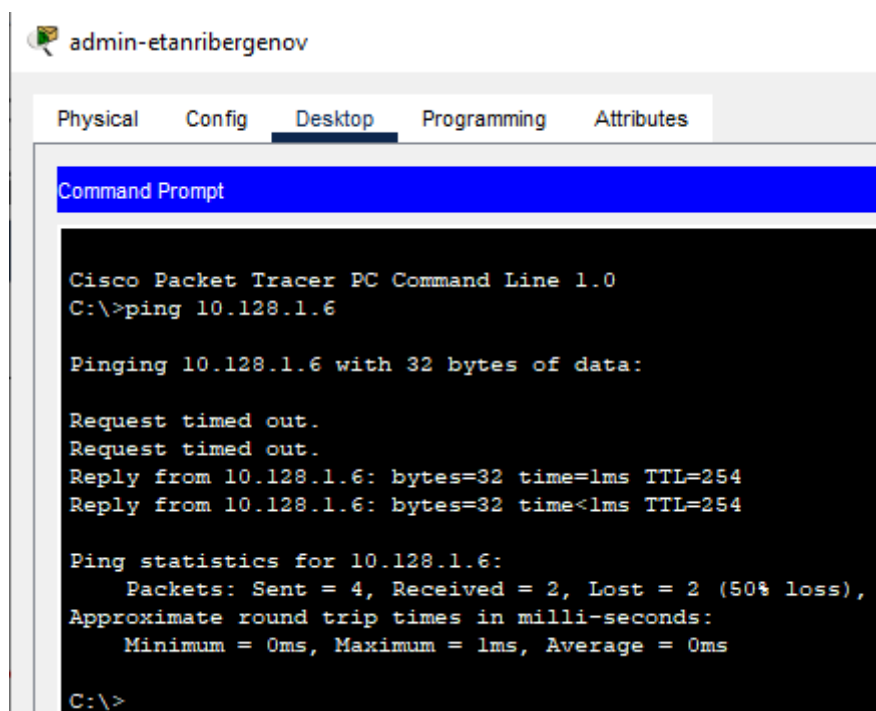
Pinging 10.128.0.2 with 32 bytes of data:

Request timed out.
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 = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Рис. 3.22: Проверка доступа администратора к сети сетевого оборудования

К сетевому оборудованию:



```
admin-etanribergenov

Physical  Config  Desktop  Programming  Attributes

Command Prompt

Cisco Packet Tracer PC Command Line 1.0
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. 3.23: Проверка доступа администратора к сети сетевого оборудования

12. Разрешил администратору из сети Other на Павловской действия, аналогичные действиям администратора сети Other на Донской.

Разместил ноутбук администратора на территории Павловская и соединил с 23 портом коммутатора msk-pavlovskaya-etanribergenov-sw-1:

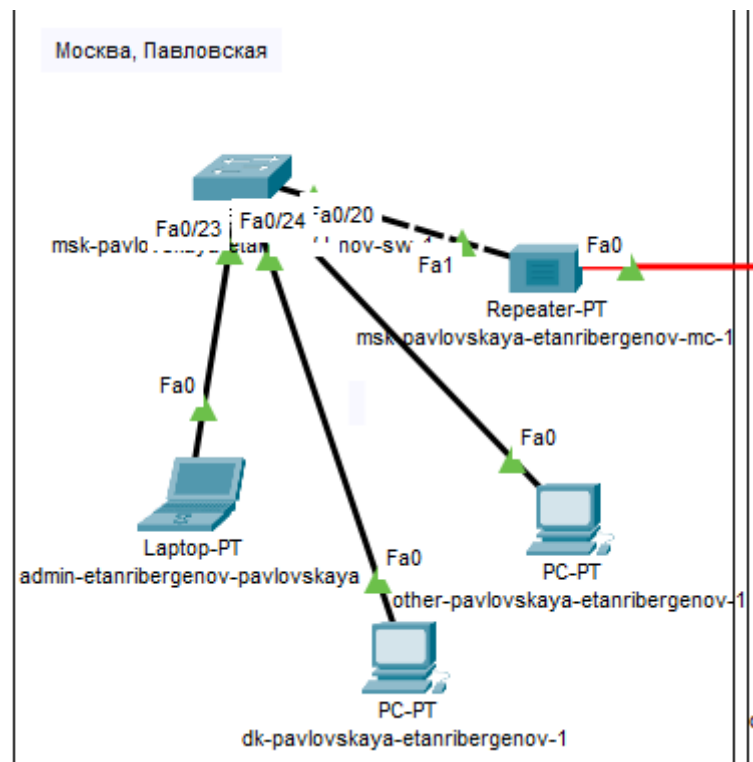


Рис. 3.24: Размещение ноутбука администратора на Павловской

Настроил интерфейс f0/23: задал ему принадлежность к vlan 104 (сеть other):

```
interface FastEthernet0/23
  switchport access vlan 104
  switchport mode access
  !
```

Рис. 3.25: Настройка интерфейса коммутатора на Павловской

Задал адреса шлюза и dns-сервера, а также его собственный статический ip-адрес:

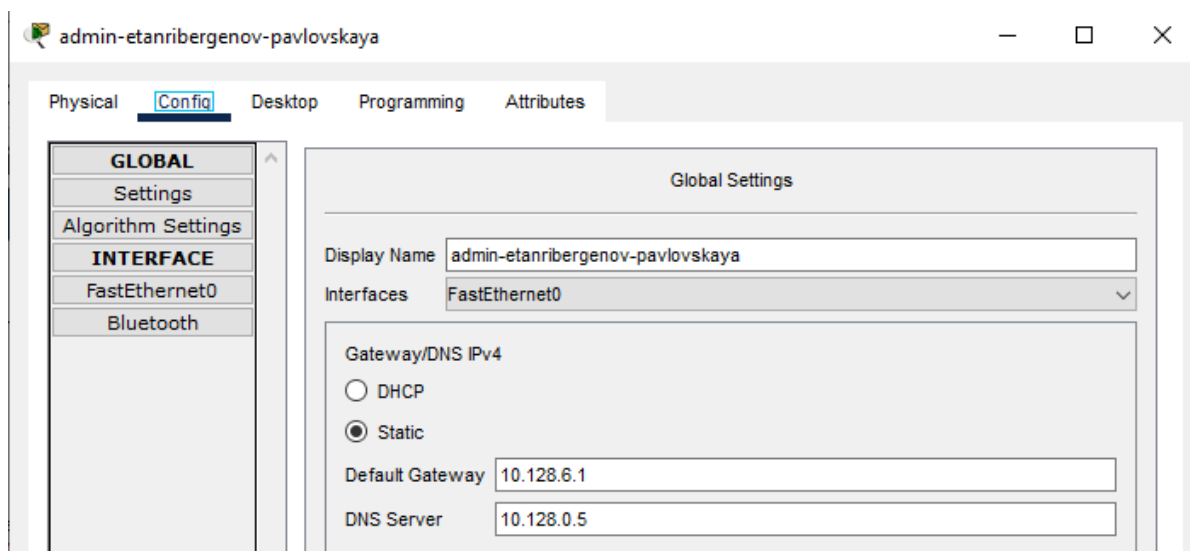


Рис. 3.26: IP-адреса шлюза и dns-сервера ноутбука администратора на Павловской

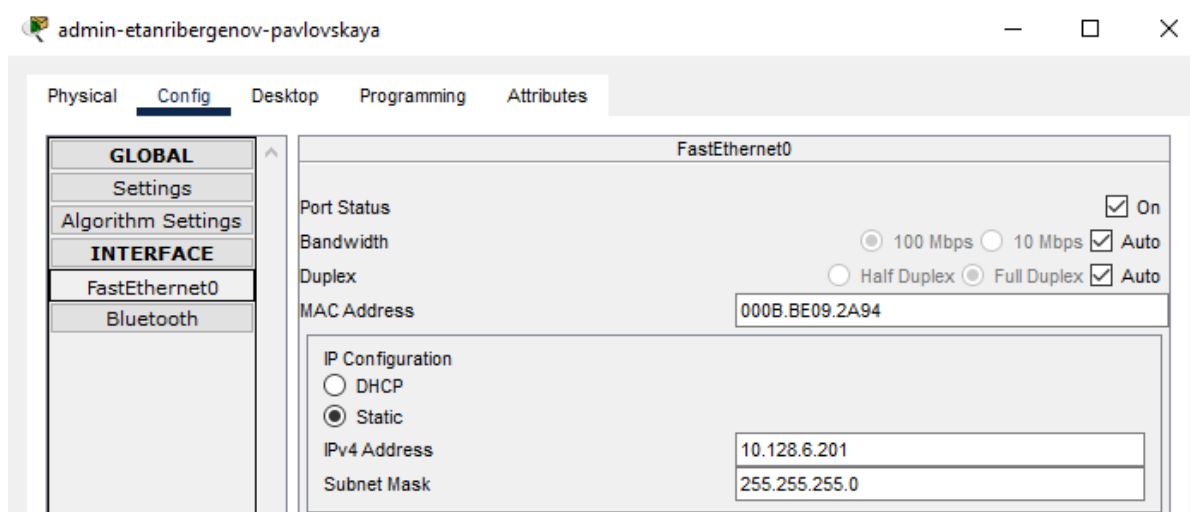


Рис. 3.27: IP-адрес ноутбука администратора на Павловской

Добавил правила (доступ по всем протоколам ко всем узлам сети и сетевому оборудованию) в списки доступа для узла администратора на Павловской:

```

ip access-list extended other-in
 remark admin
 permit ip host 10.128.6.200 any
 permit ip host 10.128.6.201 any
ip access-list extended management-out
 remark admin
 permit ip host 10.128.6.200 10.128.1.0 0.0.0.255
 permit ip host 10.128.6.201 10.128.1.0 0.0.0.255
!
```

Рис. 3.28: Правила для администратора на Павловской в списках доступа

Проверка доступа узла администратора на Павловской к остальным узлам сети и сетевому оборудованию:

```

C:\>ping mail-etanribergenov.donskaya.rudn.edu

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<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 = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
C:\>ping 10.128.1.6

Pinging 10.128.1.6 with 32 bytes of data:

Reply from 10.128.1.6: bytes=32 time<1ms TTL=254
Reply from 10.128.1.6: bytes=32 time=1ms TTL=254
Reply from 10.128.1.6: bytes=32 time<1ms TTL=254
Reply from 10.128.1.6: bytes=32 time=15ms TTL=254

Ping statistics for 10.128.1.6:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 15ms, Average = 4ms
```

Рис. 3.29: Проверка правильности работы правил

## 4 Ответы на контрольные вопросы

1. Команда *permit* *<протокол>* *<кому>* *<куда>* *<порт>* задаёт правило для конкретного протокола.
2. Чтобы задать действие правила сразу для нескольких портов, можно написать сразу несколько протоколов.
3. Команда *show access-lists* выводит списки доступа с их порядковыми номерами.
4. Добавив перед правилом (перед словом *permit/deny*) число, можно изменить порядок применения правил в списке контроля доступа.

## **5 Выводы**

Я освоил настройку прав доступа пользователей к ресурсам сети.