

# Лабораторная работа №10

## Настройка списков управления доступом (ACL)

---

Замбалова Д.В.

Российский университет дружбы народов, Москва, Россия

## Докладчик

- Замбалова Дина Владимировна
- студентка
- Российский университет дружбы народов
- 1132226536@pfur.ru
- <https://github.com/dvzambalova>

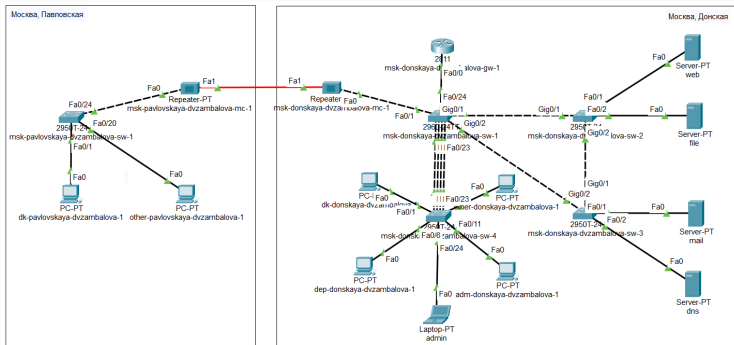
## Цель

Освоить настройку прав доступа пользователей к ресурсам сети.

## Задание

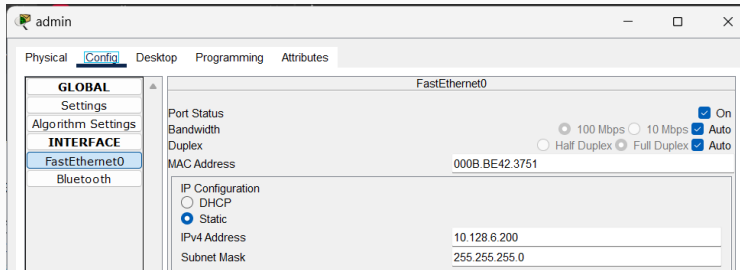
1. Требуется настроить правила доступа.
2. Требуется проверить правильность действия установленных правил доступа.
3. Требуется выполнить задание для самостоятельной работы по настройке прав доступа администратора сети на Павловской.
4. При выполнении работы необходимо учитывать соглашение об именовании.

# Выполнение лабораторной работы



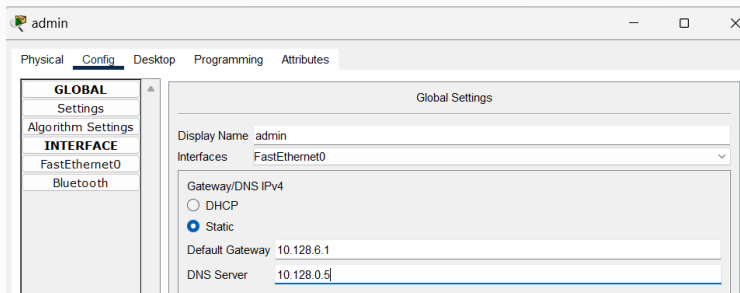
**Рис. 1:** Размещение ноутбука администратора в сети other-donskaya-1

# Выполнение лабораторной работы



**Рис. 2:** Задание статического ip-адреса ноутбуку admin

# Выполнение лабораторной работы



**Рис. 3:** Задание gateway-адреса и адреса DNS-сервера ноутбуку admin

# Выполнение лабораторной работы

```
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=2ms TTL=127
Reply from 10.128.0.2: bytes=32 time<1ms TTL=127
Reply from 10.128.0.2: bytes=32 time=10ms TTL=127
Reply from 10.128.0.2: bytes=32 time=32ms 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 = 32ms, Average = 11ms

C:\>ping 10.128.0.5

Pinging 10.128.0.5 with 32 bytes of data:

Request timed out.
Reply from 10.128.0.5: bytes=32 time<1ms 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 = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

**Рис. 4:** Проверка работоспособности соединения ноутбука admin

# Выполнение лабораторной работы

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

**Рис. 5:** Настройка доступа к web-серверу по порту tcp 80

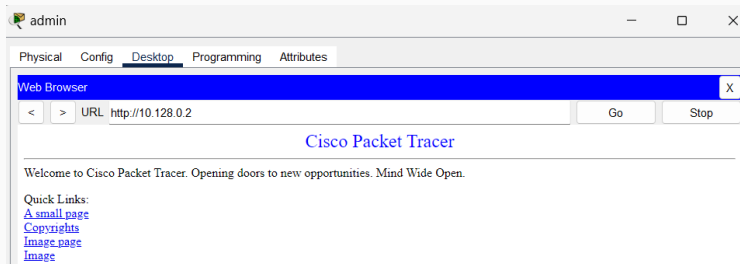


# Выполнение лабораторной работы

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

**Рис. 6:** Добавление списка управления доступом к интерфейсу

# Выполнение лабораторной работы



**Рис. 7:** Проверка доступа к web-серверу через протокол HTTP

# Выполнение лабораторной работы

```
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),
```

**Рис. 8:** Проверка недоступности web-сервера через ping

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

**Рис. 9:** Настройка дополнительного доступа для администратора по протоколам Telnet и FTP

# Выполнение лабораторной работы

```
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. 10:** Проверка работы ftp у администратора

# Выполнение лабораторной работы

```
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. 11:** Проверка недоступности подключения по ftp у просто пользователя

# Выполнение лабораторной работы

```
msh-donskaya-dvzambalova-gw-1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
msh-donskaya-dvzambalova-gw-1(config)#ip access-list extended servers-out
msh-donskaya-dvzambalova-gw-1(config-ext-nacl)#remark file
msh-donskaya-dvzambalova-gw-1(config-ext-nacl)#permit tcp host 10.128.0.0 0.0.255.255 host
10.128.0.3 eq 445
                                     ^
% Invalid input detected at '^' marker.

msh-donskaya-dvzambalova-gw-1(config-ext-nacl)#permit tcp 10.128.0.0 0.0.255.255 host 10.128.0.3
eq 445
msh-donskaya-dvzambalova-gw-1(config-ext-nacl)#permit tcp any host 10.128.0.3 range 20 ftp
```

**Рис. 12:** Настройка доступа к файловому серверу

# Выполнение лабораторной работы

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

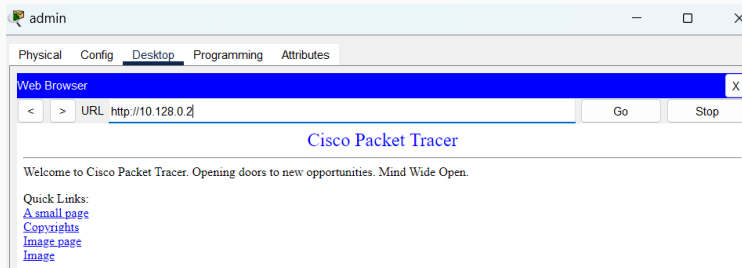
**Рис. 13:** Настройка доступа к почтовому серверу



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

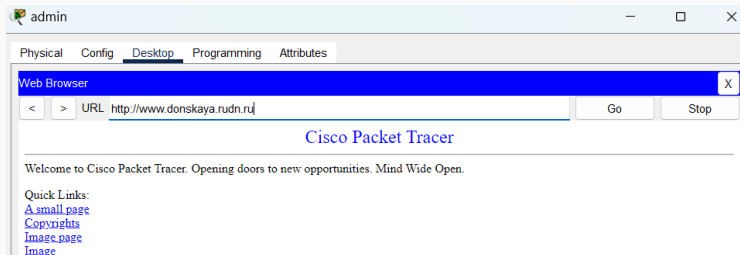
**Рис. 14:** Настройка доступа к DNS-серверу

# Выполнение лабораторной работы



**Рис. 15:** Проверка доступности web-сервера по ip-адресу

# Выполнение лабораторной работы



**Рис. 16:** Проверка доступности web-сервера по имени

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

**Рис. 17:** Разрешение icmp-запросов

# Выполнение лабораторной работы

```
msk-donskaya-dvzambalova-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 (32 match(es))
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 0.0.255.255 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 (1 match(es))
```

**Рис. 18:** Просмотр строк в списке контроля доступа

# Выполнение лабораторной работы

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

**Рис. 19:** Настройка доступа для сети Other

# Выполнение лабораторной работы

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

**Рис. 20:** Настройка доступа администратора к сети сетевого оборудования

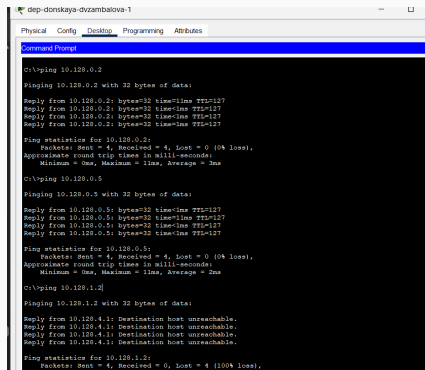
# Выполнение лабораторной работы

```
!  
ip access-list extended servers-out  
remark web  
permit icmp any any  
permit tcp any host 10.128.0.2  
permit tcp host 10.128.6.200 host 10.128.0.2 range 20 ftp  
permit tcp host 10.128.6.200 host 10.128.0.2 eq telnet  
remark file  
permit tcp 10.128.0.0 0.0.255.255 host 10.128.0.3 eq 445  
permit tcp any host 10.128.0.3 range 20 ftp  
remark mail  
permit tcp any host 10.128.0.4 eq smtp  
permit tcp any host 10.128.0.4 eq pop3  
remark dns  
permit udp 10.128.0.0 0.0.255.255 host 10.128.0.5 eq domain  
permit tcp any host 10.128.0.2 eq www  
ip access-list extended servers-in  
remark admin  
permit ip host 10.128.6.200 any  
ip access-list extended management-out  
remark admin  
permit ip host 10.128.6.200 10.128.1.0 0.0.0.255  
!
```

**Рис. 21:** Список контроля доступа



# Самостоятельная работа



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

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 = 1ms, 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=1ms 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 = 1ms, Average = 3ms

C:\>ping 10.128.1.2

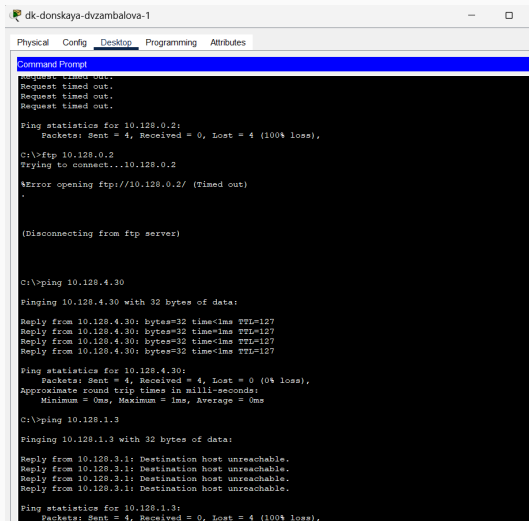
Pinging 10.128.1.2 with 32 bytes of data:

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),
```

**Рис. 22:** Пингование устройств с dep-donskaya-dvzambalova-1

# Самостоятельная работа



```
dk-donskaya-dvzambalova-1
Physical Config Desktop Programming Attributes
Command Prompt
Request timed out.
Request timed out.
Request timed out.
Request timed out.

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

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 10.128.4.30

Pinging 10.128.4.30 with 32 bytes of data:

Reply from 10.128.4.30: bytes=32 time<1ms TTL=127
Reply from 10.128.4.30: bytes=32 time<1ms TTL=127
Reply from 10.128.4.30: bytes=32 time<1ms TTL=127
Reply from 10.128.4.30: bytes=32 time<1ms TTL=127

Ping statistics for 10.128.4.30:
    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

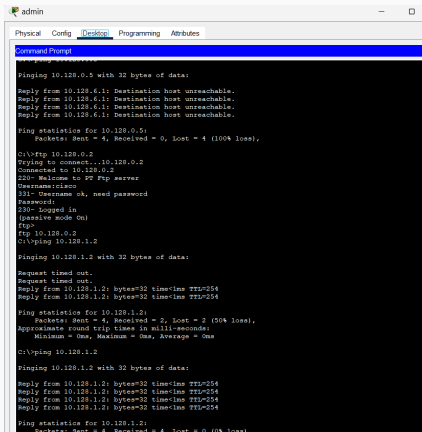
Pinging 10.128.1.3 with 32 bytes of data:

Reply from 10.128.3.1: 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),
```

**Рис. 23:** Проверка доступности устройств с dk-donskaya-dvzambalova-1

# Самостоятельная работа



```
admin
Physical Config Desktop Programming Attributes

Command Prompt

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:\>ftp 10.128.0.2
Trying to connect...10.128.0.2
Connected to 10.128.0.2
220- Welcome to 52 Ftp server
Username: cisco
331- Username ok, need password
Password:
230- Logged in
(passive mode on)
ftp>
ftp 10.128.0.2
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

C:\>ping 10.128.1.2

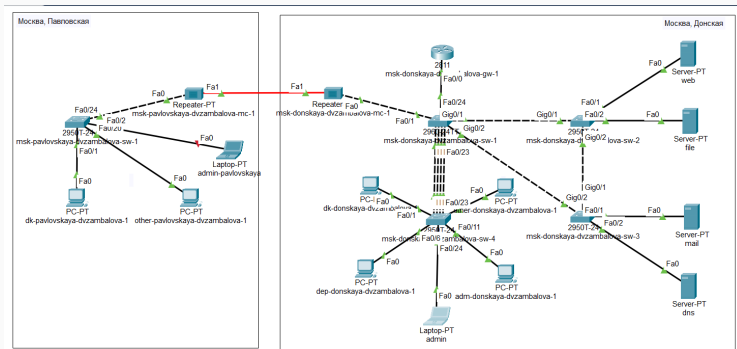
Pinging 10.128.1.2 with 32 bytes of data:

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),
```

**Рис. 24:** Проверка доступности устройств с dk-donskaya-dvzambalova-1

# Самостоятельная работа



**Рис. 25:** Логическая область с размещенным ноутбуком admin на Павловской

# Самостоятельная работа

```
msk-donskaya-dvzambalova-gw-1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
msk-donskaya-dvzambalova-gw-1(config)#ip access list extended servers out
                                     ^
% Invalid input detected at '^' marker.

msk-donskaya-dvzambalova-gw-1(config)#ip access-list extended servers-out
msk-donskaya-dvzambalova-gw-1(config-ext-nacl)#permit tcp host 10.128.6.201 host 10.128.0.2 range
20 ftp
msk-donskaya-dvzambalova-gw-1(config-ext-nacl)#permit tcp host 10.128.6.201 host 10.128.0.2 eq
telnet
msk-donskaya-dvzambalova-gw-1(config-ext-nacl)#^Z
msk-donskaya-dvzambalova-gw-1#
%SYS-5-CONFIG_I: Configured from console by console

msk-donskaya-dvzambalova-gw-1#wr m
Building configuration...
[OK]
msk-donskaya-dvzambalova-gw-1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
msk-donskaya-dvzambalova-gw-1(config)#ip access-list extended other-in
msk-donskaya-dvzambalova-gw-1(config-ext-nacl)#remark admin
msk-donskaya-dvzambalova-gw-1(config-ext-nacl)#permit ip host 10.128.6.201 any
msk-donskaya-dvzambalova-gw-1(config-ext-nacl)#exit
msk-donskaya-dvzambalova-gw-1(config)#interface f0/0.104
msk-donskaya-dvzambalova-gw-1(config-subif)#ip access group other in in
                                     ^
% Invalid input detected at '^' marker.

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

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

**Рис. 26:** Настройка доступов для admin-pavlovskaya

```
msk-donskaya-dvzambalova-gw-1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
msk-donskaya-dvzambalova-gw-1(config)#ip access-list extended management-out
msk-donskaya-dvzambalova-gw-1(config-ext-nacl)#remark admin
msk-donskaya-dvzambalova-gw-1(config-ext-nacl)##permit ip host 10.128.6.201 10.128.1.0 0.0.0.255
^
% Invalid input detected at '^' marker.

msk-donskaya-dvzambalova-gw-1(config-ext-nacl)#permit ip host 10.128.6.201 10.128.1.0 0.0.0.255
msk-donskaya-dvzambalova-gw-1(config-ext-nacl)#exit
msk-donskaya-dvzambalova-gw-1(config)#interface f0/0.2
msk-donskaya-dvzambalova-gw-1(config-subif)#ip access-group management-out out
```

**Рис. 27:** Настройка доступов для admin-pavlovskaya

# Самостоятельная работа

```
ip access-list extended servers-out
remark web
permit icmp any any
permit tcp any host 10.128.0.2
permit tcp host 10.128.6.200 host 10.128.0.2 range 20 ftp
permit tcp host 10.128.6.200 host 10.128.0.2 eq telnet
remark file
permit tcp 10.128.0.0 0.0.255.255 host 10.128.0.3 eq 445
permit tcp any host 10.128.0.3 range 20 ftp
remark mail
permit tcp any host 10.128.0.4 eq smtp
permit tcp any host 10.128.0.4 eq pop3
remark dns
permit udp 10.128.0.0 0.0.255.255 host 10.128.0.5 eq domain
permit tcp host 10.128.6.201 host 10.128.0.2 range 20 ftp
permit tcp host 10.128.6.201 host 10.128.0.2 eq telnet
ip access-list extended servers-in
remark admin
permit ip host 10.128.6.200 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
ip access-list extended other-in
remark admin
permit ip host 10.128.6.201 any
```

**Рис. 28:** Список контроля доступа

В процессе выполнения данной лабораторной работы я освоила настройку прав доступа пользователей к ресурсам сети.



**Спасибо за внимание!**