

Настройка списков управления доступом (ACL)

Лабораторная работа № 10

Шулуужук Айраана НПИбд-02-22

Содержание

1	Цель работы	5
2	Задание	6
3	Выполнение лабораторной работы	8
4	Выводы	18
5	Контрольные вопросы	19

Список иллюстраций

3.1	присвоение статического адреса	8
3.2	шлюз и адрес DNS-сервера	9
3.3	настройка доступа к web-серверу по порту tcp 80	9
3.4	добавление списка управления доступом к интерфейсу . . .	10
3.5	проверка доступа к веб-серверу через протокол http	10
3.6	доступ для администратора по протоколам Telnet и FTP . . .	10
3.7	получение доступа по протоколу FTP	11
3.8	настройка доступа к файловому серверу	11
3.9	настройка доступа к почтовому серверу	12
3.10	настройка доступа к DNS-серверу	12
3.11	проверка доступности к web-серверу	13
3.12	разрешение icmp-запросов	13
3.13	настройка доступа для сети Other	14
3.14	настройка доступа администратора к сети сетевого оборудо- вания	14
3.15	просмотр списка контроля доступа	15
3.16	проверка корректности установленных правил доступа . . .	15
3.17	проверка корректности установленных правил доступа . . .	16
3.18	настройка доступа администратора из сети Other на Павлов- ской	17

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. 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

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

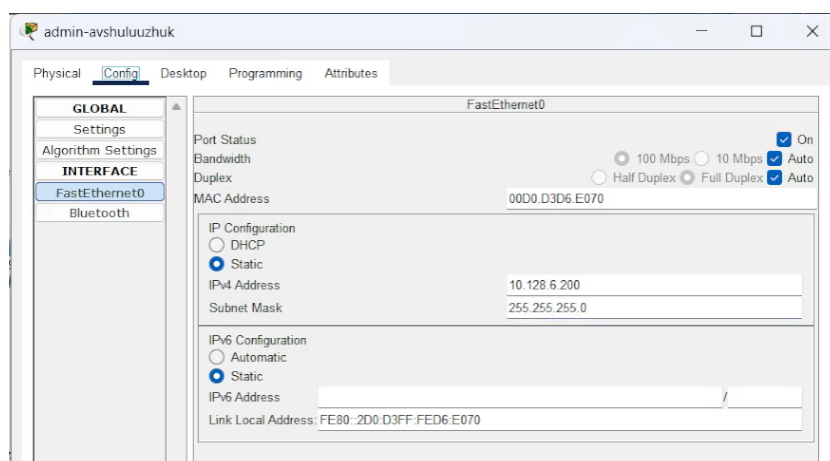


Рис. 3.1: присвоение статического адреса

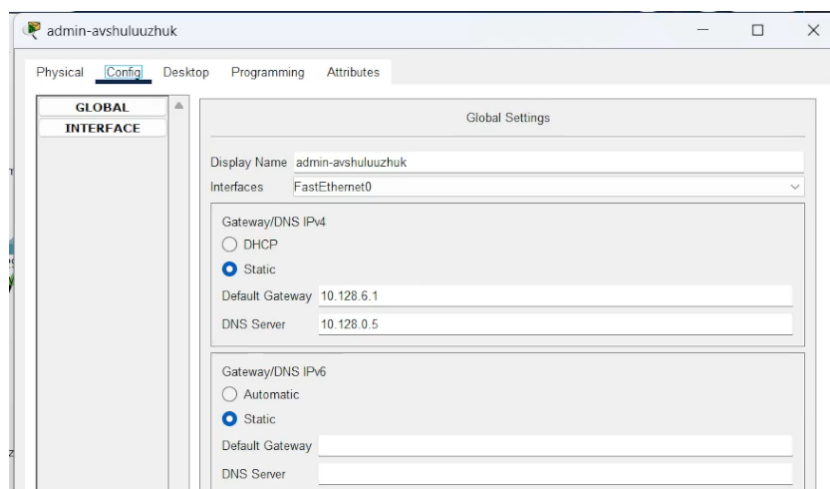


Рис. 3.2: шлюз и адрес DNS-сервера

Настроим доступ к web-серверу по порту tcp 80. Здесь: 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.(рис. 3.3)

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

Рис. 3.3: настройка доступа к web-серверу по порту tcp 80

Добавим список управления доступом к интерфейсу. Здесь: к интерфейсу f0/0.3 подключается список прав доступа servers-out и применяется к исходящему трафику (out) (рис. 3.4)

```

msk-donskaya-avshuluuzhuk-gw-1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
msk-donskaya-avshuluuzhuk-gw-1(config)#interface f0/0.3
msk-donskaya-avshuluuzhuk-gw-1(config-subif)#ip access-group servers-out out
msk-donskaya-avshuluuzhuk-gw-1(config-subif)#^Z
msk-donskaya-avshuluuzhuk-gw-1#
%SYS-5-CONFIG_I: Configured from console by console
wr m
Building configuration...
[OK]
msk-donskaya-avshuluuzhuk-gw-1#

```

Рис. 3.4: добавление списка управления доступом к интерфейсу

Можно проверить, что доступ к web-серверу есть через протокол HTTP (введя в строке браузера хоста ip-адрес web-сервера). При этом команда ping будет демонстрировать недоступность web-сервера как по имени, так и по ip-адресу web-сервера (рис. 3.5)

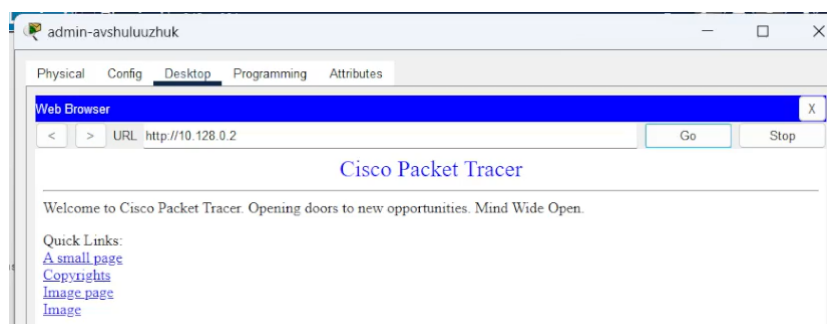


Рис. 3.5: проверка доступа к веб-серверу через протокол http

Дополнительный доступ для администратора по протоколам Telnet и FTP. Здесь: 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 (рис. 3.6)

```

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

```

Рис. 3.6: доступ для администратора по протоколам 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. 3.7)

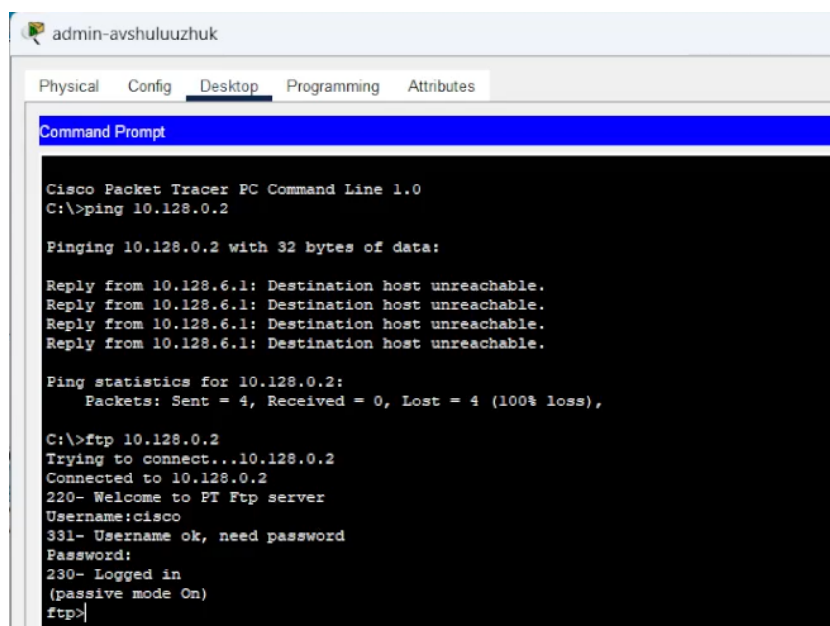


Рис. 3.7: получение доступа по протоколу FTP

Настройка доступа к файловому серверу. Здесь: 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) (рис. 3.8)

```
msk-donskaya-avshuluuzhuk-gw-1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
msk-donskaya-avshuluuzhuk-gw-1(config)#ip access-list extended servers-out
msk-donskaya-avshuluuzhuk-gw-1(config-ext-nacl)#remark file
msk-donskaya-avshuluuzhuk-gw-1(config-ext-nacl)#permit tcp 10.128.0.0 0.0.255.255 host 10.128.0.3
eq 445
msk-donskaya-avshuluuzhuk-gw-1(config-ext-nacl)#permit tcp any host 10.128.0.3 range 20 ftp
msk-donskaya-avshuluuzhuk-gw-1(config-ext-nacl)#^Z
msk-donskaya-avshuluuzhuk-gw-1#
^SYS-5-CONFIG_I: Configured from console by console
wr m
Building configuration...
[OK]
msk-donskaya-avshuluuzhuk-gw-1#
```

Рис. 3.8: настройка доступа к файловому серверу

Настройка доступа к почтовому серверу. 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 (рис. 3.9)

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

Рис. 3.9: настройка доступа к почтовому серверу

Настройка доступа к DNS-серверу. 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 (рис. 3.10)

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

Рис. 3.10: настройка доступа к DNS-серверу

Проверим доступность web-сервера (через браузер) не только по ip-адресу, но и по имени (рис. 3.11)

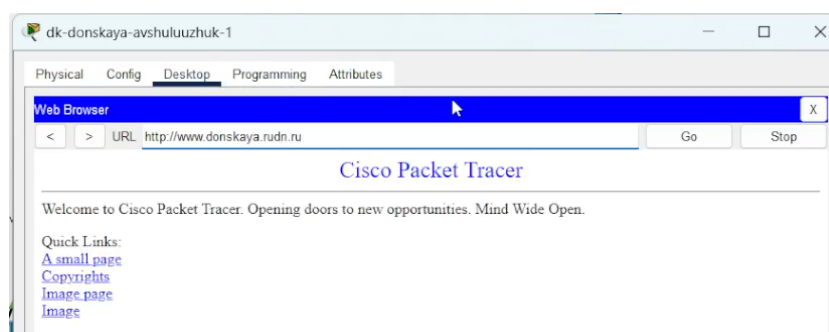


Рис. 3.11: проверка доступности к web-серверу

Разрешение icmp-запросов. Здесь демонстрируется явное управление порядком размещения правил — правило разрешения для icmp-запросов добавляется в начало списка контроля доступа (рис. 3.12)

```
msk-donskaya-avshuluuzhuk-gw-1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
msk-donskaya-avshuluuzhuk-gw-1(config)#ip access-list extended servers-out
msk-donskaya-avshuluuzhuk-gw-1(config-ext-nacl)#1 permit icmp any any
msk-donskaya-avshuluuzhuk-gw-1(config-ext-nacl)#^Z
msk-donskaya-avshuluuzhuk-gw-1#
%SYS-5-CONFIG_I: Configured from console by console
wr m
Building configuration...
[OK]
msk-donskaya-avshuluuzhuk-gw-1#
```

Рис. 3.12: разрешение icmp-запросов

Настройка доступа для сети Other (требуется наложить ограничение на исходящий из сети Other трафик, который по отношению к маршрутизатору msk-donskaya-gw-1 является входящим трафиком). Здесь: 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). (рис. 3.13)

```

msk-donskaya-avshuluuzhuk-gw-1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
msk-donskaya-avshuluuzhuk-gw-1(config)#ip access-list extended other-in
msk-donskaya-avshuluuzhuk-gw-1(config-ext-nacl)#remark admin
msk-donskaya-avshuluuzhuk-gw-1(config-ext-nacl)#permit ip host 10.128.6.200 any
msk-donskaya-avshuluuzhuk-gw-1(config-ext-nacl)#exit
msk-donskaya-avshuluuzhuk-gw-1(config)#interface f0/0.104
msk-donskaya-avshuluuzhuk-gw-1(config-subif)#ip access-group other-in in
msk-donskaya-avshuluuzhuk-gw-1(config-subif)#^Z
msk-donskaya-avshuluuzhuk-gw-1#
%SYS-5-CONFIG_I: Configured from console by console
wr m
Building configuration...
[OK]

```

Рис. 3.13: настройка доступа для сети Other

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) (рис. 3.14)

```

msk-donskaya-avshuluuzhuk-gw-1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
msk-donskaya-avshuluuzhuk-gw-1(config)#ip access-list extended management-out
msk-donskaya-avshuluuzhuk-gw-1(config-ext-nacl)#remark admin
msk-donskaya-avshuluuzhuk-gw-1(config-ext-nacl)#permit ip host 10.128.6.200 10.128.1.0 0.0.0.255
msk-donskaya-avshuluuzhuk-gw-1(config-ext-nacl)#exit
msk-donskaya-avshuluuzhuk-gw-1(config)#interface f0/0.2
msk-donskaya-avshuluuzhuk-gw-1(config-subif)#ip access-group management-out out
msk-donskaya-avshuluuzhuk-gw-1(config-subif)#^Z
msk-donskaya-avshuluuzhuk-gw-1#
%SYS-5-CONFIG_I: Configured from console by console
wr m
Building configuration...
[OK]
msk-donskaya-avshuluuzhuk-gw-1#

```

Рис. 3.14: настройка доступа администратора к сети сетевого оборудования

Номера строк правил в списке контроля доступа можно посмотреть с помощью команды show access – lists (рис. 3.15)

```
msk-donskaya-avshuluuzhuk-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 (53 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 (9 match(es))
Extended IP access list other-in
10 permit ip host 10.128.6.200 any
Extended IP access list management-out
10 permit ip host 10.128.6.200 10.128.1.0 0.0.0.255
msk-donskaya-avshuluuzhuk-gw-1#
```

Рис. 3.15: просмотр списка контроля доступа

Проверим корректность установленных правил доступа, попытавшись получить доступ по различным протоколам с разных устройств сети к подсети серверов и подсети сетевого оборудования (рис. 3.16) (рис. 3.17)

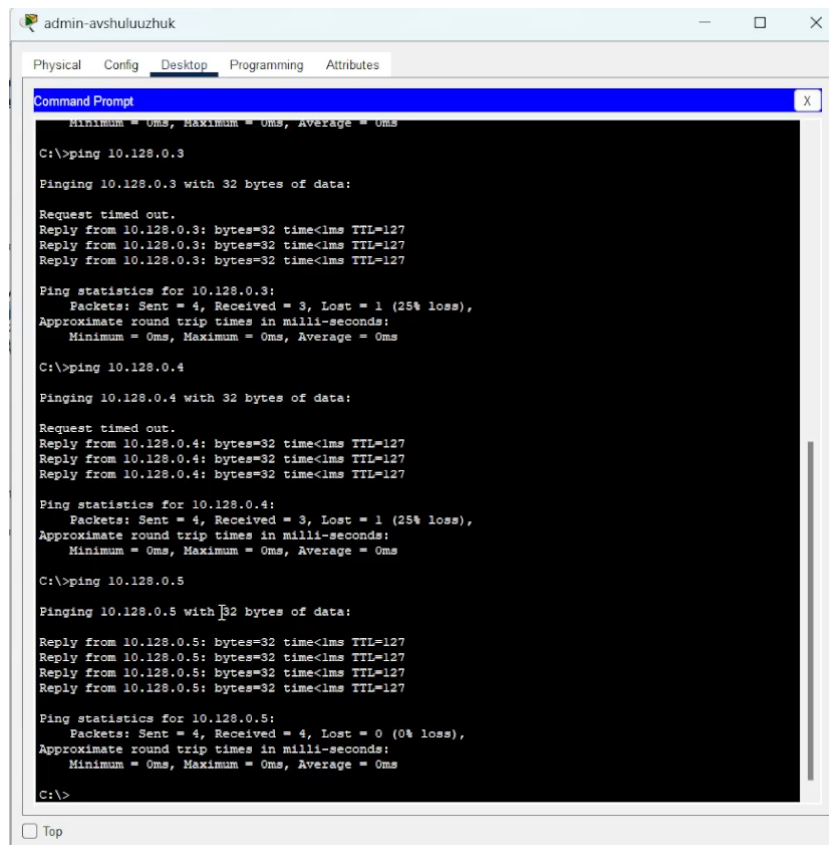
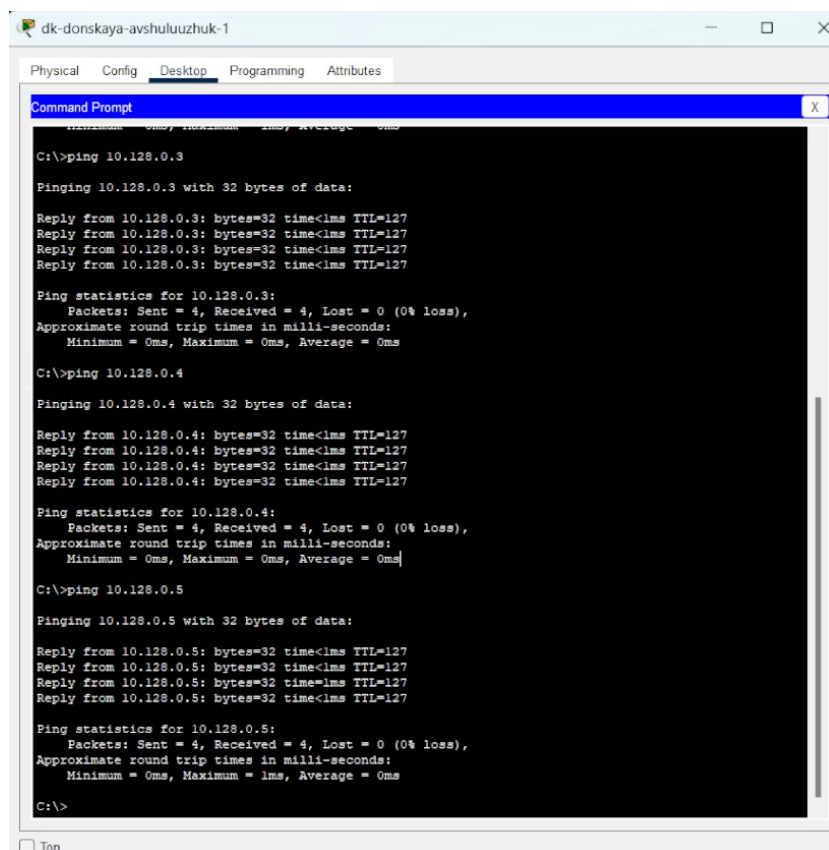


Рис. 3.16: проверка корректности установленных правил доступа



```
dk-donskaya-avshuluuzhuk-1
Physical Config Desktop Programming Attributes
Command Prompt
C:\>ping 10.128.0.3

Pinging 10.128.0.3 with 32 bytes of data:

Reply from 10.128.0.3: bytes=32 time<1ms TTL=127
Reply from 10.128.0.3: bytes=32 time<1ms TTL=127
Reply from 10.128.0.3: bytes=32 time<1ms TTL=127
Reply from 10.128.0.3: bytes=32 time<1ms TTL=127

Ping statistics for 10.128.0.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 10.128.0.4

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<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:\>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 = 0ms

C:\>
```

Рис. 3.17: проверка корректности установленных правил доступа

Разрешим администратору из сети Other на Павловской действия, аналогичные действиям администратора сети Other на Донской (рис. 3.18)


```
msk-donskaya-avshuluuzhuk-gw-1
Physical Config CLI Attributes
IOS Command Line Interface

Password:
msk-donskaya-avshuluuzhuk-gw-1>
msk-donskaya-avshuluuzhuk-gw-1>en
Password:
msk-donskaya-avshuluuzhuk-gw-1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
msk-donskaya-avshuluuzhuk-gw-1(config)#ip access-list extended servers-out
msk-donskaya-avshuluuzhuk-gw-1(config-ext-nacl)#permit tcp host 10.128.6.201 host 10.128.0.2 range
20 ftp
msk-donskaya-avshuluuzhuk-gw-1(config-ext-nacl)#permit tcp host 10.128.6.201 host 10.128.0.2 eq
telnet
msk-donskaya-avshuluuzhuk-gw-1(config-ext-nacl)#^Z
msk-donskaya-avshuluuzhuk-gw-1#
%SYS-5-CONFIG_I: Configured from console by console
wr m
Building configuration...
[OK]
msk-donskaya-avshuluuzhuk-gw-1#conf
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
msk-donskaya-avshuluuzhuk-gw-1(config)#ip access-list extended other-in
msk-donskaya-avshuluuzhuk-gw-1(config-ext-nacl)#permit ip host 10.128.6.201 any
msk-donskaya-avshuluuzhuk-gw-1(config-ext-nacl)#^Z
msk-donskaya-avshuluuzhuk-gw-1#
%SYS-5-CONFIG_I: Configured from console by console
wr m
Building configuration...
[OK]
msk-donskaya-avshuluuzhuk-gw-1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
msk-donskaya-avshuluuzhuk-gw-1(config)#ip access-list extended management-out
msk-donskaya-avshuluuzhuk-gw-1(config-ext-nacl)#permit ip host 10.128.6.201 10.128.1.0 0.0.0.255
msk-donskaya-avshuluuzhuk-gw-1(config-ext-nacl)#exit
msk-donskaya-avshuluuzhuk-gw-1(config)#^Z
msk-donskaya-avshuluuzhuk-gw-1#
%SYS-5-CONFIG_I: Configured from console by console
wr m
Building configuration...
[OK]
msk-donskaya-avshuluuzhuk-gw-1#
```

Рис. 3.18: настройка доступа администратора из сети Other на Павловской

4 Выводы

В результате выполнения лабораторной работы было освоено настройка прав доступа пользователей к ресурсам сети.

5 Контрольные вопросы

1. Как задать действие правила для конкретного протокола? Чтобы задать действие правила для конкретного протокола, необходимо указать его в настройках правила. Например, если вы используете iptables (в Linux), вы можете сделать это следующим образом. Здесь -p tcp указывает, что правило применяется только к TCP-протоколу.
2. Как задать действие правила сразу для нескольких портов? Для задания действия правила для нескольких портов можно использовать перечисление или диапазон портов. Например, в iptables вы можете использовать -m multiport:

```
iptables -A INPUT -p tcp -m multiport -dports 80,443 -j ACCEPT
```

Либо задать диапазон:

```
iptables -A INPUT -p tcp -dport 1000:2000 -j ACCEPT
```

3. Как узнать номер правила в списке прав доступа? Чтобы узнать номер правила в списке прав доступа, можно использовать команду, которая отображает все правила с номерами, например, в iptables:

```
iptables -L -line-numbers
```

Это выведет список правил с номерами строк.

4. Каким образом можно изменить порядок применения правил в списке контроля доступа? Порядок применения правил обычно определяется их расположением в списке. В iptables для изменения порядка

необходимо удалить правило и затем добавить его снова, либо использовать команды, которые позволяют задать правила в определенных позициях. Например

`iptables -D INPUT 2` # Удалить правило номер 2
`iptables -I INPUT 1` # Вставить правило на первую позицию