

Лабораторная работы №9

Настройка списков управления доступом (ACL)

Кузнецова С. В.

18 апреля 2025

Российский университет дружбы народов, Москва, Россия

Информация

- Кузнецова София Вадимовна
- Российский университет дружбы народов

Ход работы



Рис. 1: Создание нового проекта

Ноутбук администратора с именем admin к сети к other-donskaya-1

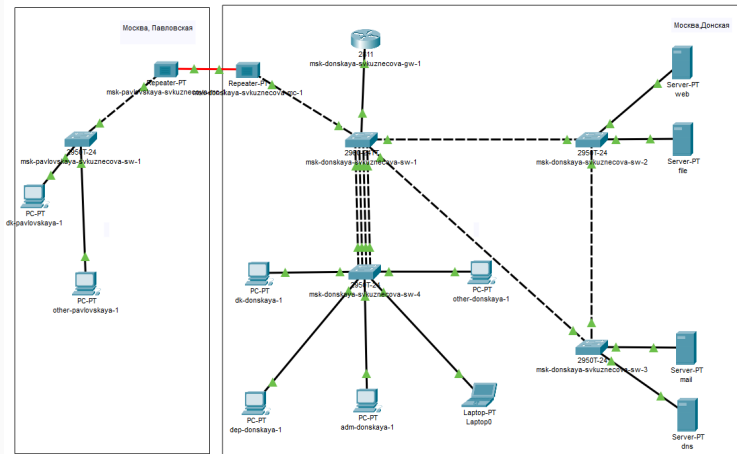


Рис. 2: Подсоединение ноутбука к порту 24 коммутатора msk-donskaya-svkuznecova-sw-4 и изменение названия

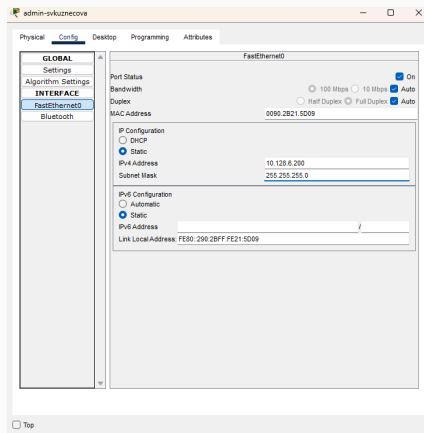
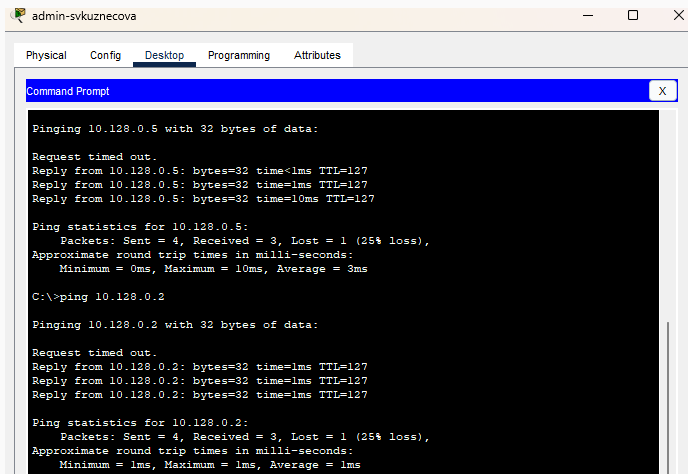


Рис. 3: Присвоение оконечному устройству статического адреса 10.128.6.200, gateway-адреса 10.128.6.1 и адреса DNS-сервера 10.128.0.5



The screenshot shows a Windows Command Prompt window with the title bar 'admin-svkuznecova'. The window has tabs for 'Physical', 'Config', 'Desktop', 'Programming', and 'Attributes', with 'Desktop' currently selected. The Command Prompt displays the following text:

```
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=10ms 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 = 10ms, Average = 3ms  
  
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=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 = 1ms, Maximum = 1ms, Average = 1ms
```

Рис. 4: Проверка (пингуем с admin-svkuznecova 10.128.0.2 и 10.128.0.5)

Настройка доступа к web-серверу по порту tcp 80

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

msh-donskaya-svkuznecova-gw-1#wr me
Building configuration...
[OK]
```

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

Добавление списка управления доступом к интерфейсу

```
msk-donskaya-svkuznecova-gw-1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
msk-donskaya-svkuznecova-gw-1(config)#interface f0/0.3
msk-donskaya-svkuznecova-gw-1(config-subif)#ip access group servers out out
                                     ^
% Invalid input detected at '^' marker.

msk-donskaya-svkuznecova-gw-1(config-subif)#ip access-group servers-out out
msk-donskaya-svkuznecova-gw-1(config-subif)#exit
msk-donskaya-svkuznecova-gw-1(config)#exit
msk-donskaya-svkuznecova-gw-1#
%SYS-5-CONFIG_I: Configured from console by console

msk-donskaya-svkuznecova-gw-1#wr me
Building configuration...
[OK]
```

Рис. 6: Добавление списка управления доступом к интерфейсу

```
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. 7: Проверка демонстрации недоступности web-сервера как по имени, так и по ip-адресу web-сервера.

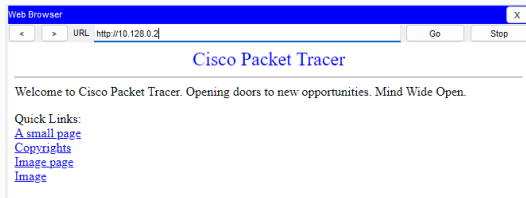


Рис. 8: Проверка доступа к web-серверу есть через протокол HTTP (введя в строке браузера хоста ip-адрес web-сервера)

Настроим дополнительный доступ для администратора по протоколам Telnet и FTP

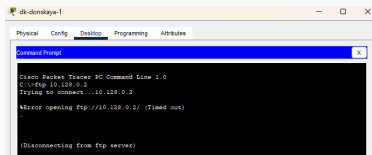
```
msk-donskaya-svkuznecova-gw-1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
msk-donskaya-svkuznecova-gw-1(config)#ip access-list extended servers-out
msk-donskaya-svkuznecova-gw-1(config-ext-nacl)#permit tcp host 10.128.6.200 host
10.128.0.2 range 20 ftp
msk-donskaya-svkuznecova-gw-1(config-ext-nacl)#permit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

msk-donskaya-svkuznecova-gw-1#wr me
Building configuration...
[OK]
```

Рис. 9: Настроим дополнительный доступ для администратора по протоколам Telnet и 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. 10: Проверка доступа с узла 10.128.6.200 по протоколу FTP



The screenshot shows a window titled 'dk-donskaya-1' with tabs for 'Physical', 'Config', 'Desktop', 'Programming', and 'Attributes'. The 'Desktop' tab is active, displaying a 'Command Prompt' window. The text in the Command Prompt is as follows:

```
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. 11: Проверка доступа с устройства dk-donskaya-1 по протоколу FTP (доступ запрещён)

Настройка доступа к файловому серверу

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

msk-donskaya-svkuznecova-gw-1#wr me
Building configuration...
[OK]
```

Рис. 12: Настройка доступа к файловому серверу

Настройка доступа к почтовому серверу

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

msk-donskaya-svkuznecova-gw-1#wr me
Building configuration...
[OK]
```

Рис. 13: Настройка доступа к почтовому серверу

Настройка доступа к DNS-серверу

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

msk-donskaya-svkuznecova-gv-1#vr me
Building configuration...
[OK]
```

Рис. 14: Настройка доступа к DNS-серверу

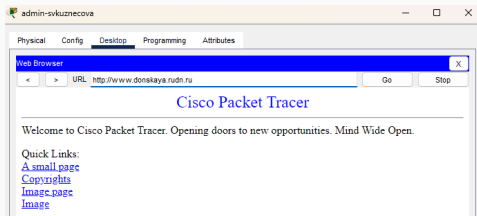


Рис. 15: Проверка доступности web-сервера(через браузер) по имени

Разрешим іср-запросов

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

msk-donskaya-svkuznecova-gw-1#wr me
Building configuration...
[OK]
```

Рис. 16: Разрешим іср-запросов

```
msk-donskaya-svkuznecova-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 (10 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 (1 match(es))
Extended IP access list other-in
```

Рис. 17: Просмотр номеров строк правил в списке контроля доступа

Настройка доступа для сети Other

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

msk-donskaya-svkuznecova-gw-1(config-subif)#ip access-group other-in in
msk-donskaya-svkuznecova-gw-1(config-subif)#exit
msk-donskaya-svkuznecova-gw-1(config)#exit
msk-donskaya-svkuznecova-gw-1#
%SYS-5-CONFIG_I: Configured from console by console

msk-donskaya-svkuznecova-gw-1#wr me
Building configuration...
[OK]
```

Рис. 18: Настройка доступа для сети Other

Настройка доступа администратора к сети сетевого оборудования

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

msk-donskaya-svkuznecova-gw-1#wr me
Building configuration...
[OK]
```

Рис. 19: Настройка доступа администратора к сети сетевого оборудования

Проверим корректность

```
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 = 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 = 1ms, Average = 0ms

C:\>ping 10.128.0.3

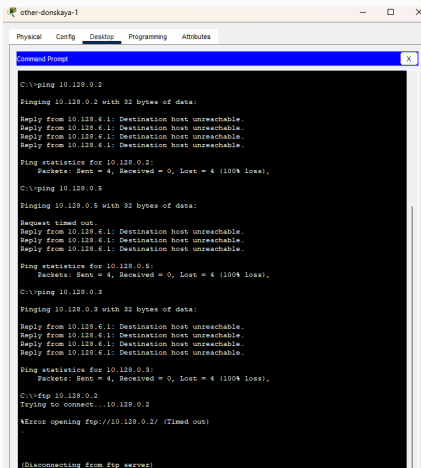
Pinging 10.128.0.3 with 32 bytes of data:

Request timed out.
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=10ms TTL=127

Ping statistics for 10.128.0.3:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 10ms, Average = 3ms
```

Рис. 20: Проверка корректности установленных правил доступа с оконечного устройства admin-svkuznecova.

Проверим корректность



```
other-donskaya-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 10.128.6.1: 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:

Request timed out.
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:\>ping 10.128.0.3

Pinging 10.128.0.3 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 10.128.0.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

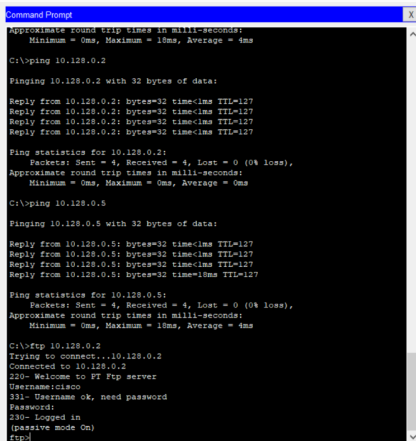
C:\>ftp 10.128.0.2
Trying to connect...10.128.0.2

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

(Disconnecting from ftp server)
```

Рис. 21: Проверка корректности установленных правил доступа с оконечного устройства other-donskaya-1.

Разрешим администратору из сети Other на Павловской действия, аналогичные действиям администратора сети Other на Донской



```
Command Prompt
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 16ms, Average = 4ms

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 10.128.0.5

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=18ms 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 = 18ms, Average = 4ms

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

Рис. 22: Проверка разрешений администратора из сети Other на Павловской.

Выводы

В ходе выполнения лабораторной работы мы освоили настройку прав доступа пользователей к ресурсам сети.

Спасибо за внимание!