

Лабораторная Работа №10

Настройка списков управления доступом (ACL)

Козлов В.П.

Российский университет дружбы народов им. Патриса Лумумбы, Москва, Россия

- Козлов Всеволод Павлович
- НФИбд-02-22
- Российский университет дружбы народов
- [1132226428@pfur.ru]

Выполнение лабораторной работы

Освоить настройку прав доступа пользователей к ресурсам сети

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;

Подключил ноутбук администратора

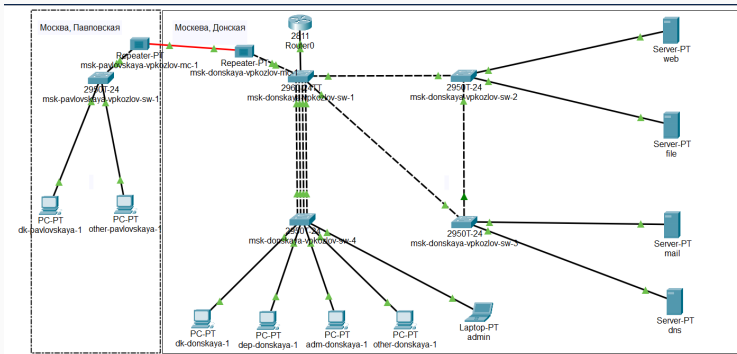


Figure 1: Ноутбук администратора

Настроил конфигурацию ноутбука администратора

The image shows two overlapping network configuration windows. The top window is titled 'FastEthernet0' and contains the following fields: 'Display Name' with the value 'admin', 'Interfaces' with the value 'FastEthernet0', a 'Gateway/DNS IPv4' section with 'DHCP' unselected and 'Static' selected, 'Default Gateway' with the value '10.128.6.1', and 'DNS Server' with the value '10.128.0.5'. The bottom window is titled 'IP Configuration' and contains: 'IP Configuration' section with 'DHCP' unselected and 'Static' selected, 'IPv4 Address' with the value '10.128.6.200', and 'Subnet Mask' with the value '255.255.255.0'.

Display Name	admin
Interfaces	FastEthernet0
Gateway/DNS IPv4	
<input type="radio"/> DHCP	
<input checked="" type="radio"/> Static	
Default Gateway	10.128.6.1
DNS Server	10.128.0.5

IP Configuration	
<input type="radio"/> DHCP	
<input checked="" type="radio"/> Static	
IPv4 Address	10.128.6.200
Subnet Mask	255.255.255.0

Figure 2: Конфигурация ноутбука администратора

Проверка работоспособности соединения ноутбука admin

```
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=23ms 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 = 23ms, Average = 7ms

C:\>ipconfig

FastEthernet0 Connection: (default port)

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address...: FE80::2D0:FFFF:FE19:93DC
    IPv6 Address...: ::
    IPv4 Address...: 10.128.6.200
    Subnet Mask...: 255.255.255.0
    Default Gateway...: ::
                        10.128.6.1
```

Figure 3: Проверка работоспособности соединения ноутбука admin

Настройка доступа к web-серверу по порту tcp 80

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

Figure 4: Настройка доступа к web-серверу по порту tcp 80

Добавление списка управления доступом к интерфейсу

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

Figure 5: Добавление списка управления доступом к интерфейсу

Проверка недоступности web-сервера через ping

```
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:\>
```

Figure 6: Недоступность web-сервера через ping

Дополнительный доступ для администратора по протоколам Telnet и FTP

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

Figure 7: Дополнительный доступ для администратора по протоколам Telnet и FTP

Попытка подключения по FTP

```
C:\>  
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>
```

Figure 8: Попытка подключения по FTP

Настройка доступа к файловому серверу

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

Figure 9: Настройка доступа к файловому серверу

Настройка доступа к почтовому серверу

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

Figure 10: Настройка доступа к почтовому серверу

Настройка доступа к DNS-серверу

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

mik-donskaya-vpkozlov-gw-1(config)#ip access-list extended servers-out
mik-donskaya-vpkozlov-gw-1(config-ext-nacl)#remark dns
mik-donskaya-vpkozlov-gw-1(config-ext-nacl)#permit udp 10.128.0.0 0.0.255.255 host 10.128.0.5 eq
53
mik-donskaya-vpkozlov-gw-1(config-ext-nacl)#exit
mik-donskaya-vpkozlov-gw-1(config)#exit
mik-donskaya-vpkozlov-gw-1#
%SYS-5-CONFIG_I: Configured from console by console
write memory
Building configuration...
[OK]
mik-donskaya-vpkozlov-gw-1#
```

Figure 11: Настройка доступа к DNS-серверу

Проверил доступность web-сервера в браузере

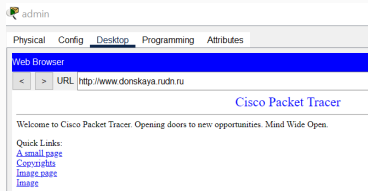


Figure 12: Доступность web-сервера в браузере

Разрешение icmp-запросов

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

Figure 13: Разрешение icmp-запросов

Посмотрел правила в списке контроля доступа

```
msk-donskaya-vpkozlov-gw-1#  
msk-donskaya-vpkozlov-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 (5 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))  
msk-donskaya-vpkozlov-gw-1#
```

Figure 14: Правила в списке контроля доступа

Проверил пингование

```
C:\>
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=16ms 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 = 16ms, Average = 4ms

C:\>ping www.donskaya.rudn.ru

Pinging 10.128.0.2 with 32 bytes of data:

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
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 = 10ms, Average = 2ms

C:\>
```

Figure 15: Проверка пингования

Настройка доступа для сети Other

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

msk-donskaya-vpkozlov-gw-1(config)#ip access-list extended other-in
msk-donskaya-vpkozlov-gw-1(config-ext-nacl)#ed other in
^
% Invalid input detected at '^' marker.

msk-donskaya-vpkozlov-gw-1(config-ext-nacl)#mskdonskaya gw 1(config extnacl)#r
^
% Invalid input detected at '^' marker.

msk-donskaya-vpkozlov-gw-1(config-ext-nacl)#ed other in
^
% Invalid input detected at '^' marker.

msk-donskaya-vpkozlov-gw-1(config-ext-nacl)#remark admin
msk-donskaya-vpkozlov-gw-1(config-ext-nacl)#permit ip host 10.128.6.200 any
msk-donskaya-vpkozlov-gw-1(config-ext-nacl)#exit
msk-donskaya-vpkozlov-gw-1(config)#interface f0/0.104
msk-donskaya-vpkozlov-gw-1(config-subif)#ip access group other in in
^
% Invalid input detected at '^' marker.

msk-donskaya-vpkozlov-gw-1(config-subif)#ip access-group other-in in
msk-donskaya-vpkozlov-gw-1(config-subif)#exit
msk-donskaya-vpkozlov-gw-1(config)#exit
msk-donskaya-vpkozlov-gw-1#
%SYS-5-CONFIG_I: Configured from console by console
write memory
Building configuration...
[OK]
msk-donskaya-vpkozlov-gw-1#
```

Figure 16: Настройка доступа для сети Other

Самостоятельная работа

Пингование с устройства dep-donskaya-vpkozlov-1

```
C:\>
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<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 10.128.1.2

Pinging 10.128.1.2 with 32 bytes of data:

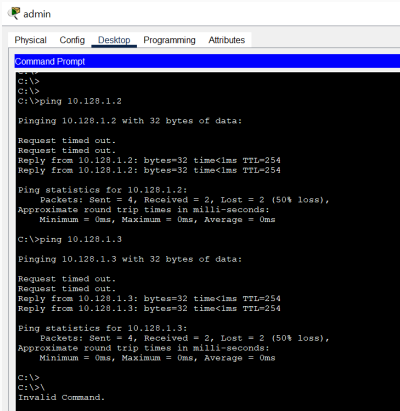
Reply from 10.128.4.1: Destination host unreachable.
Reply from 10.128.4.1: Destination host unreachable.
Reply from 10.128.4.1: Destination host unreachable.
Reply from 10.128.4.1: Destination host unreachable.

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

C:\>
```

Figure 17: Пингование с устройства dep-donskaya-vpkozlov-1

Пингование с устройства dk-donskaya-vpkozlov-1



```
admin
Physical Config Desktop Programming Attributes
Command Prompt
C:\>
C:\>
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 10.128.1.3

Pinging 10.128.1.3 with 32 bytes of data:

Request timed out.
Request timed out.
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 = 2, Lost = 2 (50% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
C:\>\
Invalid Command.
```

Figure 18: Пингование с устройства dk-donskaya-vpkozlov-1

Размещение ноутбука admin на Павловской

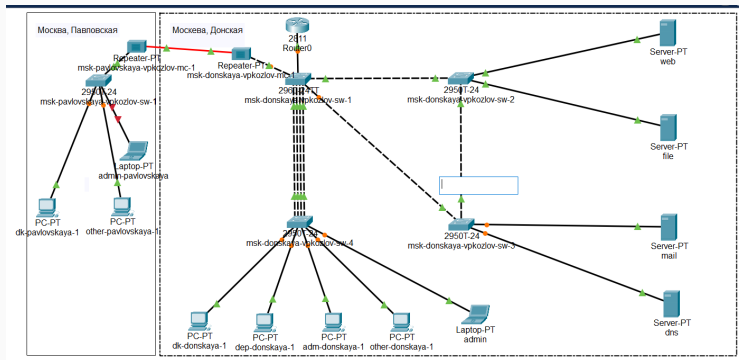


Figure 19: Размещение ноутбука admin на Павловской

Настройка доступа для admin-pavlovskaya

```
msk-donskaya-vpkozlov-gw-1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
msk-donskaya-vpkozlov-gw-1(config)#ip access-list extended servers-out
msk-donskaya-vpkozlov-gw-1(config-ext-nacl)#permit tcp host 10.128.6.201 host 10.128.0.2 range
20 ftp
msk-donskaya-vpkozlov-gw-1(config-ext-nacl)#permit tcp host 10.128.6.201 host 10.128.0.2 eq
telnet
msk-donskaya-vpkozlov-gw-1(config-ext-nacl)#exit
msk-donskaya-vpkozlov-gw-1(config)#exit
msk-donskaya-vpkozlov-gw-1#
%SYS-5-CONFIG_I: Configured from console by console
write memory
Building configuration...
[OK]
msk-donskaya-vpkozlov-gw-1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
msk-donskaya-vpkozlov-gw-1(config)#ip access-list extended other-in
msk-donskaya-vpkozlov-gw-1(config-ext-nacl)#remark admin
msk-donskaya-vpkozlov-gw-1(config-ext-nacl)#permit ip host 10.128.6.201 any
msk-donskaya-vpkozlov-gw-1(config-ext-nacl)#exit
msk-donskaya-vpkozlov-gw-1(config)#int f0/0.104
msk-donskaya-vpkozlov-gw-1(config-subif)#ip access-group other-in in
^
% Invalid input detected at '^' marker.

msk-donskaya-vpkozlov-gw-1(config-subif)#ip access-group other-in in
msk-donskaya-vpkozlov-gw-1(config-subif)#exit
msk-donskaya-vpkozlov-gw-1(config)#exit
msk-donskaya-vpkozlov-gw-1#
%SYS-5-CONFIG_I: Configured from console by console
write memory
Building configuration...
[OK]
msk-donskaya-vpkozlov-gw-1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
msk-donskaya-vpkozlov-gw-1(config)#ip access list extended management-out
^
% Invalid input detected at '^' marker.

msk-donskaya-vpkozlov-gw-1(config)#ip access-list extended management-out
msk-donskaya-vpkozlov-gw-1(config-ext-nacl)#remark admin
msk-donskaya-vpkozlov-gw-1(config-ext-nacl)#permit ip host 10.128.6.201 10.128.1.0 0.0.0.255
msk-donskaya-vpkozlov-gw-1(config-ext-nacl)#exit
msk-donskaya-vpkozlov-gw-1(config)#int f0/0.2
```

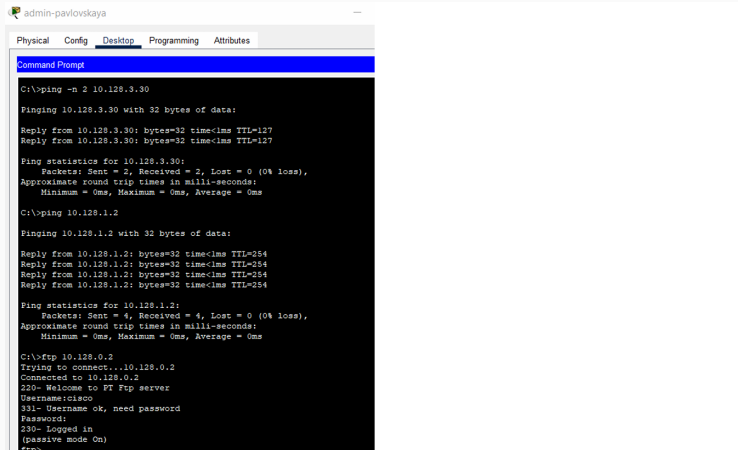
Figure 20: Настройка доступа для admin-pavlovskaya

Список контроля доступа

```
ip access-list extended servers-out
remark web
permit icmp any any
permit tcp any host 10.128.0.2 eq www
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 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 10.128.6.200 any
permit ip host 10.128.6.201 any
!
```

Figure 21: Список контроля доступа

Проверка корректности настроенного доступа



The screenshot shows a Cisco Packet Tracer console window for a device named 'admin-pavlovskaya'. The window has tabs for 'Physical', 'Config', 'Desktop', 'Programming', and 'Attributes', with 'Desktop' currently selected. The console displays the output of several commands:

```
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)
ftp>
```

Figure 22: Проверка корректности настроенного доступа

Освоил настройку прав доступа пользователей к ресурсам сети