

Отчет по лабораторной работе №10

Администрирование локальных сетей

Амуничников Антон, НПИбд-01-22

Содержание

1	Цель работы	4
2	Задание	5
3	Выполнение лабораторной работы	6
4	Самостоятельная работа	16
5	Выводы	22
6	Контрольные вопросы	23

Список иллюстраций

3.1	Размещение ноутбука администратора в сети other-donskaya-1 . . .	6
3.2	Задание статического ip-адреса ноутбуку admin	7
3.3	Задание gateway-адреса и адреса DNS-сервера ноутбуку admin . . .	7
3.4	Проверка работоспособности соединения ноутбука admin	8
3.5	Настройка доступа к web-серверу по порту tcp 80	9
3.6	Добавление списка управления доступом к интерфейсу	9
3.7	Проверка доступа к web-серверу через протокол HTTP	9
3.8	Проверка недоступности web-сервера через ping	10
3.9	Настройка дополнительного доступа для администратора по протоколам Telnet и FTP	10
3.10	Проверка работы ftp у администратора	11
3.11	Проверка недоступности подключения по ftp у просто пользователя	11
3.12	Настройка доступа к файловому серверу	11
3.13	Настройка доступа к почтовому серверу	12
3.14	Настройка доступа к DNS-серверу	12
3.15	Проверка доступности web-сервера по ip-адресу	12
3.16	Проверка доступности web-сервера по имени	13
3.17	Разрешение icmp-запросов	13
3.18	Просмотр строк в списке контроля доступа	13
3.19	Настройка доступа для сети Other	14
3.20	Настройка доступа администратора к сети сетевого оборудования	14
3.21	Список контроля доступа	15
4.1	Пингование устройств с dep-donskaya-aiaamunichnikov-1	16
4.2	Проверка доступности устройств с dk-donskaya-aiaamunichnikov-1 .	17
4.3	Проверка доступности устройств с dk-donskaya-aiaamunichnikov-1 .	18
4.4	Логическая область с размещенным ноутбуком admin на Павловской	19
4.5	Настройка доступов для admin-pavlovskaya	20
4.6	Список контроля доступа	20
4.7	Проверка корректности настроенного доступа	21

1 Цель работы

Освоить настройку прав доступа пользователей к ресурсам сети.

2 Задание

1. Требуется настроить следующие правила доступа:

- web-сервер: разрешить доступ всем пользователям по протоколу HTTP через порт 80 протокола TCP, а для администратора открыть доступ по протоколам Telnet и FTP;
- файловый сервер: с внутренних адресов сети доступ открыт по портам для общедоступных каталогов, с внешних — доступ по протоколу FTP;
- 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;
- DNS-сервер: открыть порт 53 протокола UDP для доступа из внутренней сети;
- разрешить icmp-сообщения, направленные в сеть серверов;
- запретить для сети Other любые запросы за пределы сети, за исключением администратора;
- 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 other-donskaya-1 (рис. 3.1) 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. 3.2), указав в качестве gateway-адреса 10.128.6.1 и адреса DNS-сервера 10.128.0.5 (рис. 3.3).

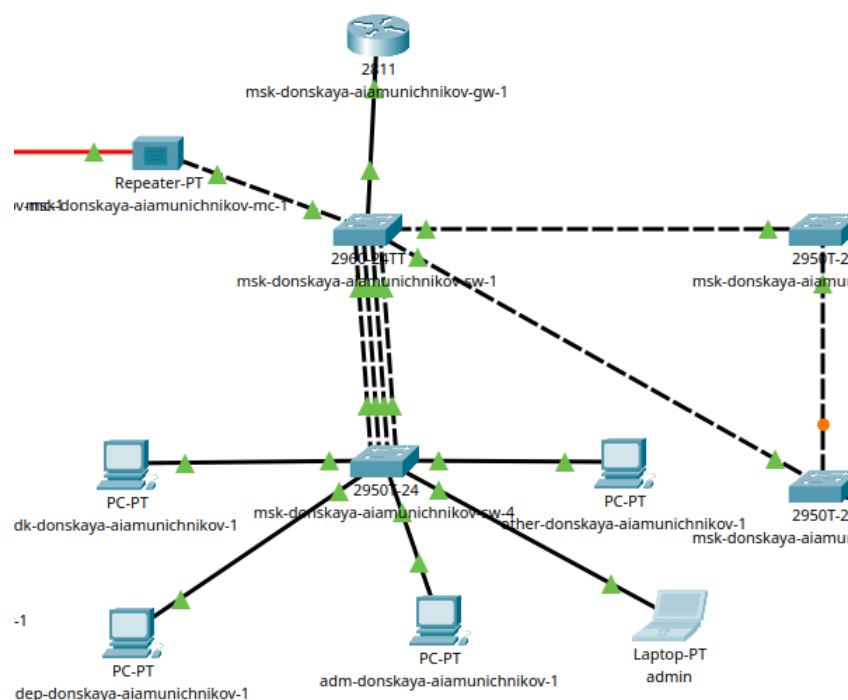


Рис. 3.1: Размещение ноутбука администратора в сети other-donskaya-1

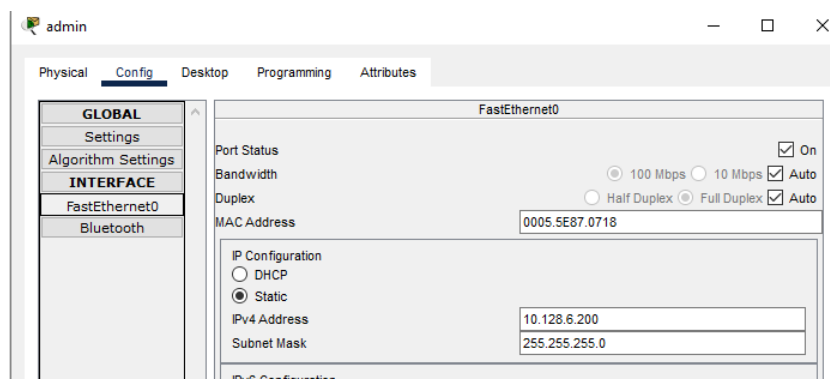


Рис. 3.2: Задание статического ip-адреса ноутбуку admin

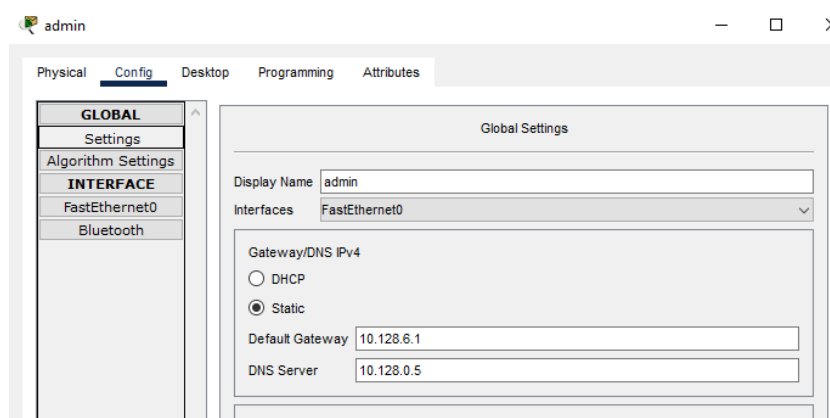


Рис. 3.3: Задание gateway-адреса и адреса DNS-сервера ноутбуку admin

Проверим, что у ноутбука корректно работает соединение через пингование разных устройств сети, например серверов (рис. 3.4).

```
Cisco Packet Tracer PC Command Line 1.0
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 = 0ms, Average = 0ms

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 = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Рис. 3.4: Проверка работоспособности соединения ноутбука admin

На оборудовании Cisco правила в списке доступа проверяются по порядку сверху вниз до первого совпадения — как только одно из правил сработало, проверка списка правил прекращается и обработка трафика происходит на основе сработавшего правила. Поэтому сначала мы надо давать разрешение (permit) на какое-то действие, а уже потом накладывать ограничения (deny).

Настроим доступ к web-серверу по порту tcp 80 (рис.3.5). Мы создаем 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, а также даем 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-aiamunichnikov-gw-01#conf t
Enter configuration commands, one per line. End with CNTL/Z.
msk-donskaya-aiamunichnikov-gw-01(config)#ip access-list extended servers-out
msk-donskaya-aiamunichnikov-gw(config-ext-nacl)#remark web
msk-donskaya-aiamunichnikov-gw(config-ext-nacl)#permit tcp any host 10.128.0.2 eq 80
msk-donskaya-aiamunichnikov-gw(config-ext-nacl)#
```

Рис. 3.5: Настройка доступа к web-серверу по порту tcp 80

Добавим список управления доступом к интерфейсу (рис.3.6). К интерфейсу f0/0.3 подключается список прав доступа servers-out и применяется к исходящему трафику (out).

```
msk-donskaya-aiamunichnikov-gw-01(config)#int f0/0.3
msk-donskaya-aiamunichnikov-gw-01(config-subif)#ip access-group servers-out out
msk-donskaya-aiamunichnikov-gw-01(config-subif)#
```

Рис. 3.6: Добавление списка управления доступом к интерфейсу

Проверим, что доступ к web-серверу есть через протокол HTTP, введя в строке браузера хоста ip-адрес web-сервера (рис.3.7). При этом команда ping будет демонстрировать недоступность web-сервера как по имени, так и по ip-адресу web-сервера (рис.3.8).

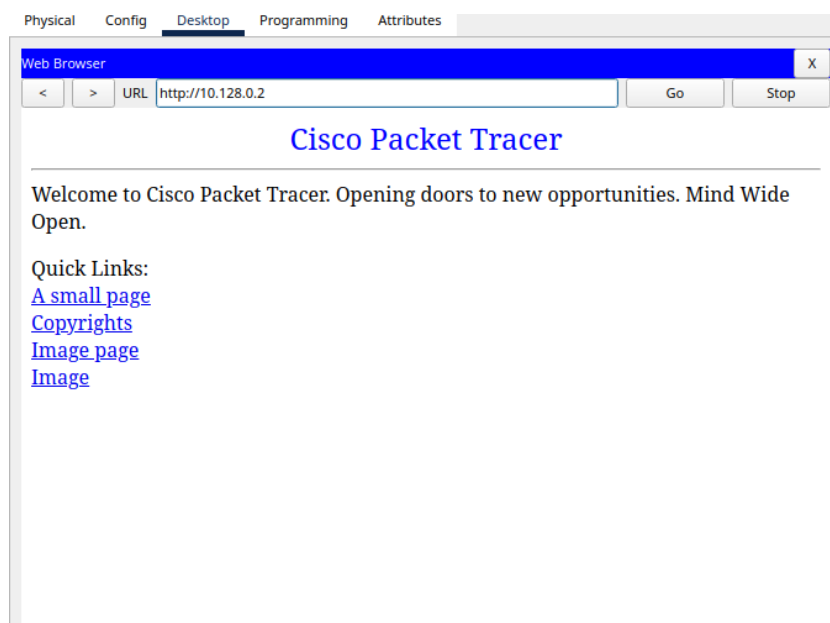
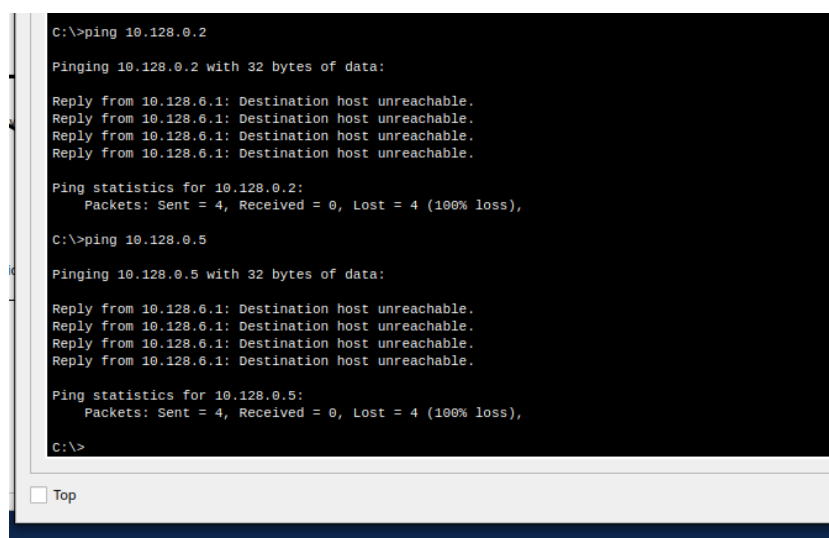


Рис. 3.7: Проверка доступа к web-серверу через протокол HTTP



```
C:\>ping 10.128.0.2

Pinging 10.128.0.2 with 32 bytes of data:

Reply from 10.128.6.1: 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:

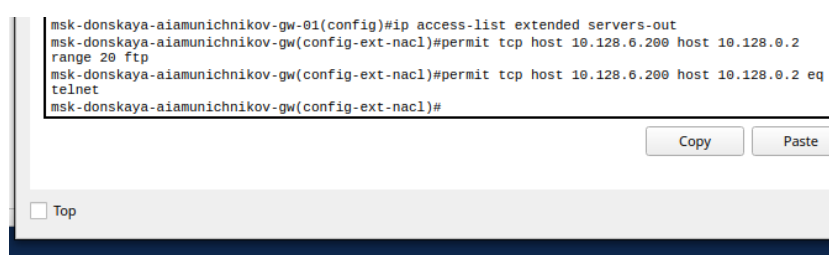
Reply from 10.128.6.1: Destination host unreachable.
Reply from 10.128.6.1: Destination host unreachable.
Reply from 10.128.6.1: Destination host unreachable.
Reply from 10.128.6.1: Destination host unreachable.

Ping statistics for 10.128.0.5:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

Рис. 3.8: Проверка недоступности web-сервера через ping

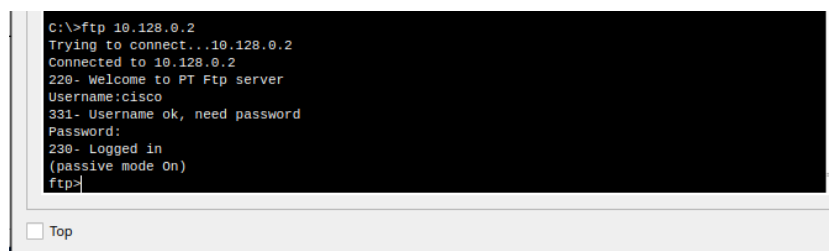
Настроим дополнительный доступ для администратора по протоколам Telnet и FTP (рис.3.9). В список контроля доступа servers-out добавлено правило, разрешающее устройству администратора с ip-адресом 10.128.6.200 доступ на web-сервер (10.128.0.2) по протоколам FTP и telnet.



```
msk-donskaya-aiaamunichnikov-gw-01(config)#ip access-list extended servers-out
msk-donskaya-aiaamunichnikov-gw(config-ext-nacl)#permit tcp host 10.128.6.200 host 10.128.0.2
range 20 ftp
msk-donskaya-aiaamunichnikov-gw(config-ext-nacl)#permit tcp host 10.128.6.200 host 10.128.0.2 eq
telnet
msk-donskaya-aiaamunichnikov-gw(config-ext-nacl)#
```

Рис. 3.9: Настройка дополнительного доступа для администратора по протоколам Telnet и FTP

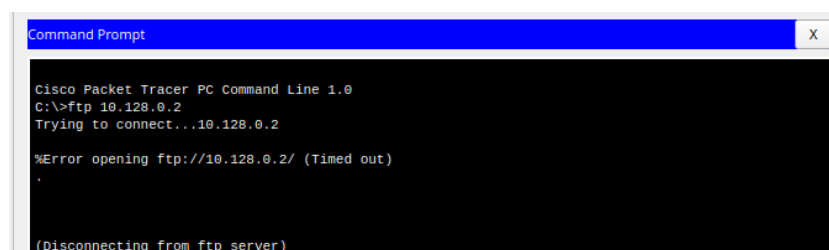
Убедимся, что с узла с ip-адресом 10.128.6.200 есть доступ по протоколу FTP (рис.3.10). Для этого в командной строке устройства администратора введем ftp 10.128.0.2, а затем по запросу имя пользователя cisco и пароль cisco, увидим, что доступ действительно есть.



```
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. 3.10: Проверка работы ftp у администратора

Попробуем провести аналогичную процедуру с другого устройства сети (рис.3.11). Увидим, что доступ запрещён.



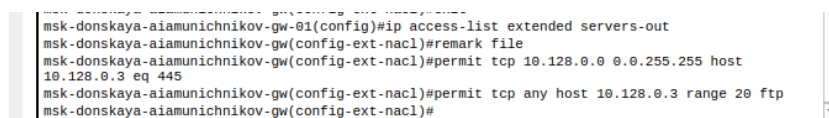
```
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>ftp 10.128.0.2
Trying to connect...10.128.0.2

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

(Disconnecting from ftp server)
```

Рис. 3.11: Проверка недоступности подключения по ftp у просто пользователя

Настроим доступ к файловому серверу (рис.3.12). 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).



```
msk-donskaya-aiaamunichnikov-gw-01(config)#ip access-list extended servers-out
msk-donskaya-aiaamunichnikov-gw(config-ext-nacl)#remark file
msk-donskaya-aiaamunichnikov-gw(config-ext-nacl)#permit tcp 10.128.0.0 0.0.255.255 host
10.128.0.3 eq 445
msk-donskaya-aiaamunichnikov-gw(config-ext-nacl)#permit tcp any host 10.128.0.3 range 20 ftp
msk-donskaya-aiaamunichnikov-gw(config-ext-nacl)#
```

Рис. 3.12: Настройка доступа к файловому серверу

Настроим доступ к почтовому серверу (рис.3.13). 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.

```
msk-donskaya-aiaamunichnikov-gw-01(config)#ip access-list extended servers-out
msk-donskaya-aiaamunichnikov-gw(config-ext-nacl)#remark mail
msk-donskaya-aiaamunichnikov-gw(config-ext-nacl)#permit tcp any host 10.128.0.4 eq smtp
msk-donskaya-aiaamunichnikov-gw(config-ext-nacl)#permit tcp any host 10.128.0.4 eq pop3
msk-donskaya-aiaamunichnikov-gw(config-ext-nacl)#exit
msk-donskaya-aiaamunichnikov-gw-01(config)#ip access-list extended servers-out
```

Рис. 3.13: Настройка доступа к почтовому серверу

Настроим доступ к DNS-серверу (рис.3.14). 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.

```
msk-donskaya-aiaamunichnikov-gw-01(config)#ip access-list extended servers-out
msk-donskaya-aiaamunichnikov-gw(config-ext-nacl)#remarkl dns
^
% Invalid input detected at '^' marker.

msk-donskaya-aiaamunichnikov-gw(config-ext-nacl)#remarkl dns
^
% Invalid input detected at '^' marker.

msk-donskaya-aiaamunichnikov-gw(config-ext-nacl)#remark dns
msk-donskaya-aiaamunichnikov-gw(config-ext-nacl)#permit udp 10.128.0.0 0.0.255.255 host
10.128.0.5 eq 53
^
% Invalid input detected at '^' marker.

msk-donskaya-aiaamunichnikov-gw(config-ext-nacl)#permit udp 10.128.0.0 0.0.255.255 host
10.128.0.5 eq 53
msk-donskaya-aiaamunichnikov-gw(config-ext-nacl)#
```

Рис. 3.14: Настройка доступа к DNS-серверу

Проверим доступность web-сервера (через браузер) не только по ip-адресу (рис.3.15), но и по имени (рис.3.16).

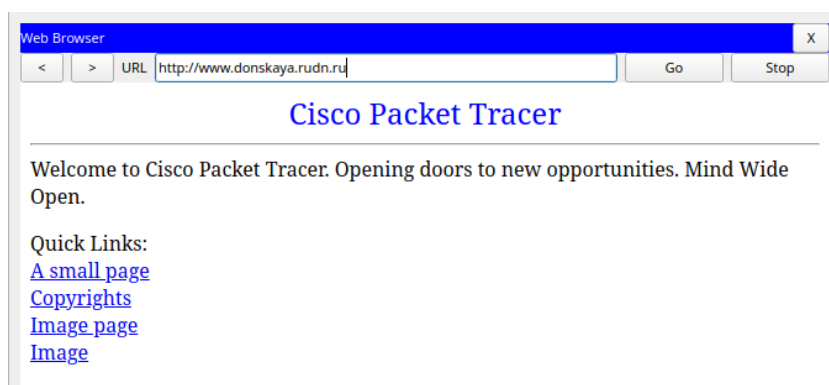


Рис. 3.15: Проверка доступности web-сервера по ip-адресу

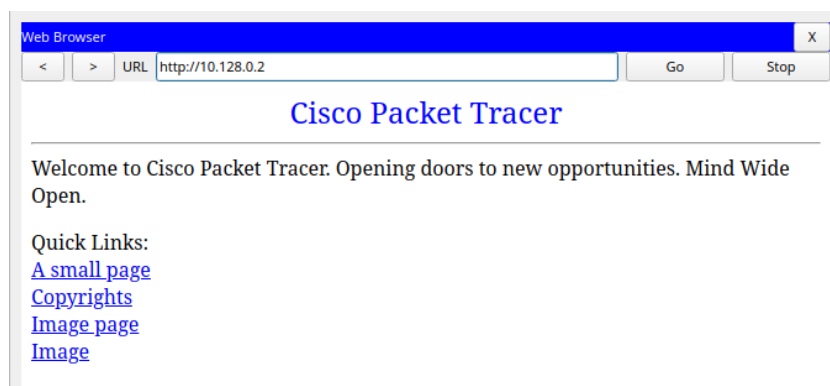


Рис. 3.16: Проверка доступности web-сервера по имени

Разрешим icmp-запросы (рис.3.17).

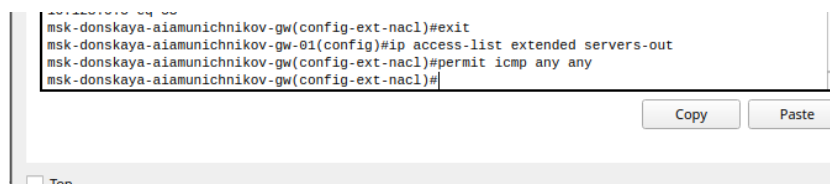


Рис. 3.17: Разрешение icmp-запросов

Посмотрим номера строк правил в списке контроля доступа (рис.3.18).

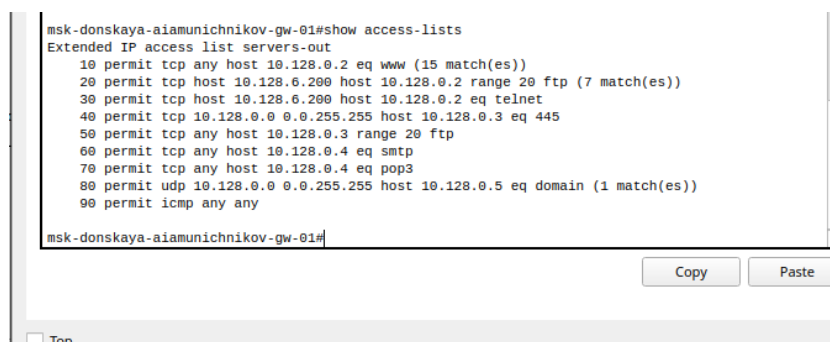
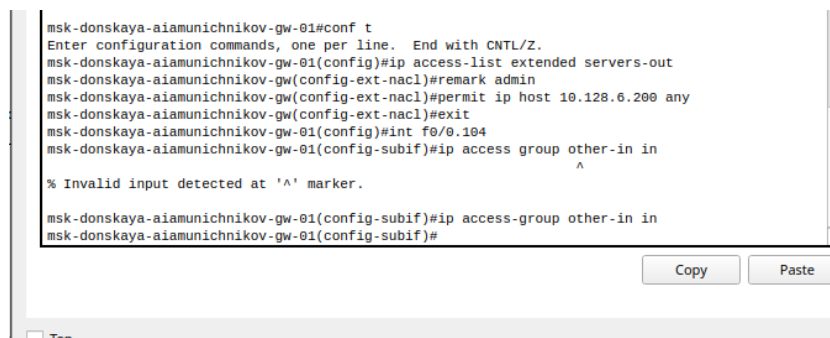


Рис. 3.18: Просмотр строк в списке контроля доступа

Настроим доступ для сети Other (рис.3.19). Наложим ограничение на исходящий из сети Other трафик, который по отношению к маршрутизатору msk-donskaya-gw-1 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).

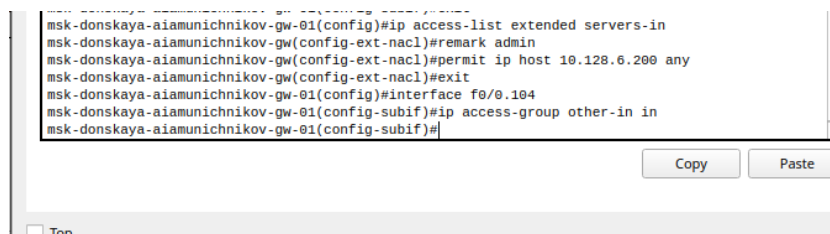


```
msk-donskaya-aiaamunichnikov-gw-01#conf t
Enter configuration commands, one per line. End with CNTL/Z.
msk-donskaya-aiaamunichnikov-gw-01(config)#ip access-list extended servers-out
msk-donskaya-aiaamunichnikov-gw-01(config-ext-nacl)#remark admin
msk-donskaya-aiaamunichnikov-gw-01(config-ext-nacl)#permit ip host 10.128.6.200 any
msk-donskaya-aiaamunichnikov-gw-01(config-ext-nacl)#exit
msk-donskaya-aiaamunichnikov-gw-01(config)#int f0/0.104
msk-donskaya-aiaamunichnikov-gw-01(config-subif)#ip access group other-in in
^
% Invalid input detected at '^' marker.

msk-donskaya-aiaamunichnikov-gw-01(config-subif)#ip access-group other-in in
msk-donskaya-aiaamunichnikov-gw-01(config-subif)#
```

Рис. 3.19: Настройка доступа для сети Other

Настроим доступ администратора к сети сетевого оборудования (рис.3.20). 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).



```
msk-donskaya-aiaamunichnikov-gw-01(config)#ip access-list extended servers-in
msk-donskaya-aiaamunichnikov-gw-01(config-ext-nacl)#remark admin
msk-donskaya-aiaamunichnikov-gw-01(config-ext-nacl)#permit ip host 10.128.6.200 any
msk-donskaya-aiaamunichnikov-gw-01(config-ext-nacl)#exit
msk-donskaya-aiaamunichnikov-gw-01(config)#interface f0/0.104
msk-donskaya-aiaamunichnikov-gw-01(config-subif)#ip access-group other-in in
msk-donskaya-aiaamunichnikov-gw-01(config-subif)#
```

Рис. 3.20: Настройка доступа администратора к сети сетевого оборудования

Проверим получившийся список контроля доступа (рис.3.21).

```
msk-donskaya-aiaamunichnikov-gw-01(config)#ip access-list extended management-out
msk-donskaya-aiaamunichnikov-gw-01(config-ext-nacl)#remark admin
msk-donskaya-aiaamunichnikov-gw-01(config-ext-nacl)#permit ip host 10.128.6.200 10.128.1.0
0.0.0.255
msk-donskaya-aiaamunichnikov-gw-01(config-ext-nacl)#exit
msk-donskaya-aiaamunichnikov-gw-01(config)#interface 0/0.2
^
% Invalid input detected at '^' marker.

msk-donskaya-aiaamunichnikov-gw-01(config)#
msk-donskaya-aiaamunichnikov-gw-01(config)#interface f0/0.2
msk-donskaya-aiaamunichnikov-gw-01(config-subif)#ip access-group management-out out
msk-donskaya-aiaamunichnikov-gw-01(config-subif)#
```

Copy Paste

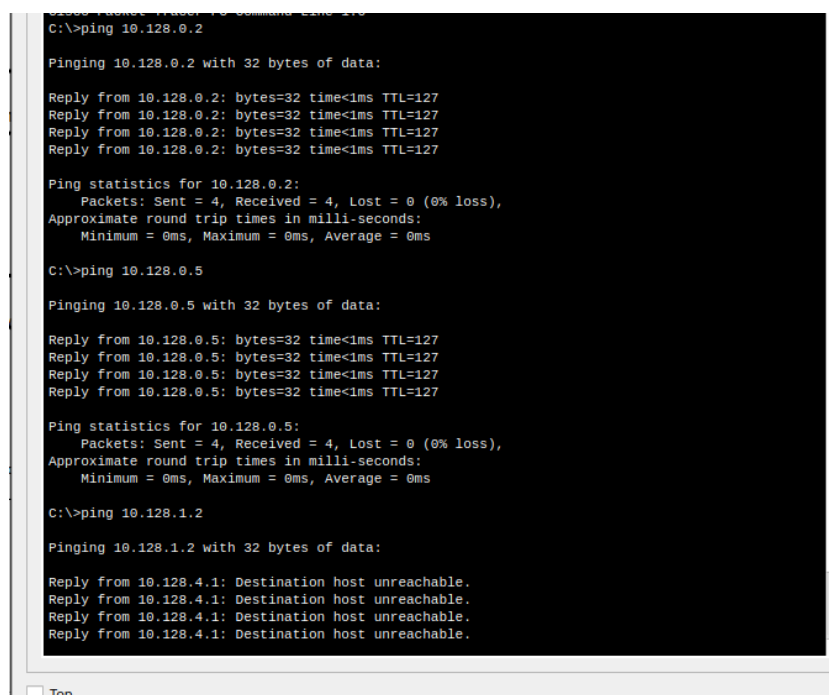
☐ Top

Рис. 3.21: Список контроля доступа

4 Самостоятельная работа

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

Откроем терминал `dep-donskaya-a1amunichnikov-1` и пропингуем разные устройства (рис.4.1). Увидим, что серверы и другие конечные устройства пингуются, однако к сетевому оборудованию доступа нет, как и должно быть.



```
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.
```

Рис. 4.1: Пингование устройств с `dep-donskaya-a1amunichnikov-1`

Откроем терминал `dk-donskaya-a1amunichnikov-1` и пропингуем разные устройства (рис.4.2). Увидим, что серверы и другие конечные устройства пингуются,

однако к сетевому оборудованию доступа нет, как и должно быть. Также попробуем подключиться к web-серверу по ftp, доступ закрыт.

```
Request timed out.

Ping statistics for 10.128.1.12:
    Packets: Sent = 2, Received = 0, Lost = 2 (100% loss),

Control-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=20ms 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 = 20ms, Average = 10ms

C:\>ping 10.128.1.2

Pinging 10.128.1.2 with 32 bytes of data:

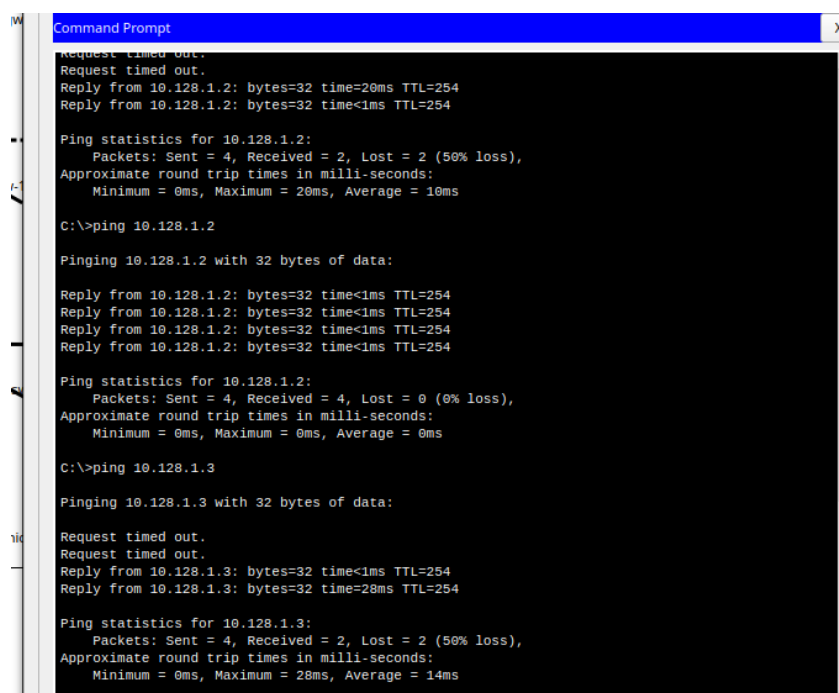
Reply from 10.128.1.2: bytes=32 time<1ms TTL=254
Reply from 10.128.1.2: bytes=32 time<1ms TTL=254
Reply from 10.128.1.2: bytes=32 time<1ms TTL=254
Reply from 10.128.1.2: bytes=32 time<1ms TTL=254

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:\>ping 10.128.1.3
```

Рис. 4.2: Проверка доступности устройств с dk-donskaya-aiaamunichnikov-1

Теперь проверим корректность настроенного доступа с admin (рис.4.3). Есть доступ к серверу по ftp, а также успешно пингуется сетевое оборудование.



```
Request timed out.
Request timed out.
Reply from 10.128.1.2: bytes=32 time=20ms 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 = 20ms, Average = 10ms

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:\>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=28ms 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 = 28ms, Average = 14ms
```

Рис. 4.3: Проверка доступности устройств с dk-donskaya-aiaamunichnikov-1

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

Разместим в рабочей области ноутбук admin-pavlovskaya на Павловской (рис.4.4).

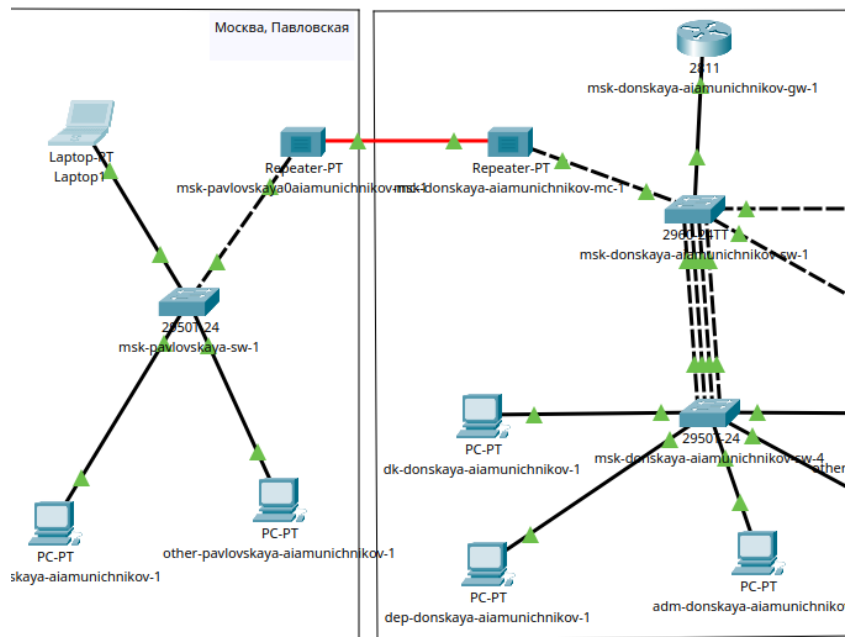


Рис. 4.4: Логическая область с размещенным ноутбуком admin на Павловской

Настроим доступ для администратора на Павловской по протоколам Telnet и FTP, дадим разрешение устройству с адресом 10.128.6.201 на любые действия (any), настроим доступ администратора к сети сетевого оборудования (рис.4.5).

```

IOS Command Line Interface

msk-donskaya-aiamunichnikov-gw-01#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
msk-donskaya-aiamunichnikov-gw-01(config)#ip access-list extended servers-out
msk-donskaya-aiamunichnikov-gw-01(config-ext-nacl)#permit tcp host 10.128.6.201 host 10.128.0.2
range 20 ftp
msk-donskaya-aiamunichnikov-gw-01(config-ext-nacl)#permit tcp host 10.128.6.201 host 10.128.0.2 eq
telnet
msk-donskaya-aiamunichnikov-gw-01(config-ext-nacl)#exit
msk-donskaya-aiamunichnikov-gw-01(config)#ip access-list extended other-in
msk-donskaya-aiamunichnikov-gw-01(config-ext-nacl)#remarkl admin
^
% Invalid input detected at '^' marker.

msk-donskaya-aiamunichnikov-gw-01(config-ext-nacl)#
msk-donskaya-aiamunichnikov-gw-01(config-ext-nacl)#remark admin
msk-donskaya-aiamunichnikov-gw-01(config-ext-nacl)#permit ip host 10.128.6.201 any
msk-donskaya-aiamunichnikov-gw-01(config-ext-nacl)#exit
msk-donskaya-aiamunichnikov-gw-01(config)#int f0/0.104
msk-donskaya-aiamunichnikov-gw-01(config-subif)#ip access-group other-in in
msk-donskaya-aiamunichnikov-gw-01(config-subif)#exit
msk-donskaya-aiamunichnikov-gw-01(config)#ip access-list extended management-out
msk-donskaya-aiamunichnikov-gw-01(config-ext-nacl)#remark admin
msk-donskaya-aiamunichnikov-gw-01(config-ext-nacl)#permit ip host 10.128.6.201 10.128.1.0
0.0.0.255
msk-donskaya-aiamunichnikov-gw-01(config-ext-nacl)#exit
msk-donskaya-aiamunichnikov-gw-01(config)#ip access-list management-out out
^
% Invalid input detected at '^' marker.

msk-donskaya-aiamunichnikov-gw-01(config)#int f0/0.2
msk-donskaya-aiamunichnikov-gw-01(config-subif)#ip access-list management-out out
^
% Invalid input detected at '^' marker.

msk-donskaya-aiamunichnikov-gw-01(config-subif)#ip access-group management-out out
msk-donskaya-aiamunichnikov-gw-01(config-subif)#

```

Рис. 4.5: Настройка доступов для admin-pavlovskaya

Проверим получившийся список контроля доступа (рис.4.6).

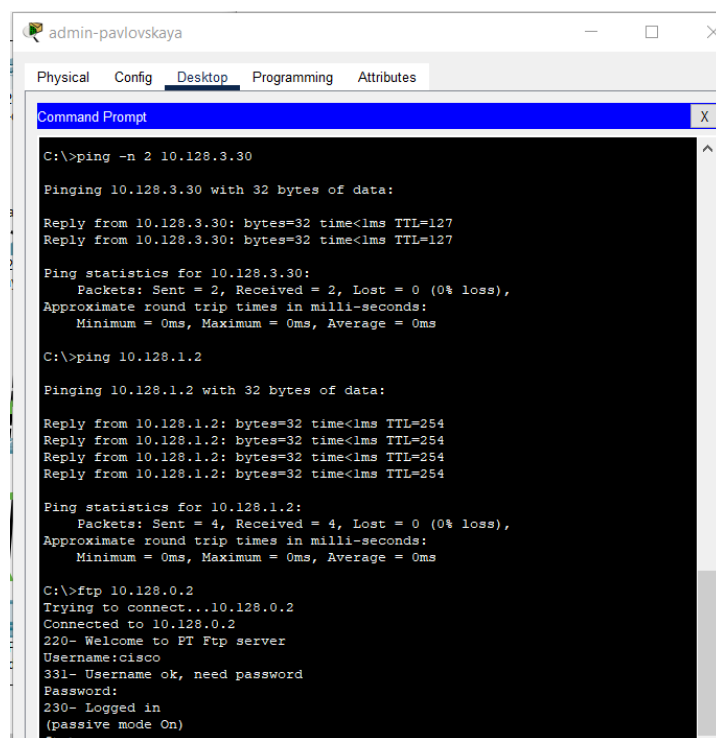
```

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
!

```

Рис. 4.6: Список контроля доступа

Проверим, что наша настройка доступов работает корректно (рис.4.7).



The screenshot shows a Cisco Packet Tracer window titled 'admin-pavlovskaya'. It has tabs for 'Physical', 'Config', 'Desktop', 'Programming', and 'Attributes'. The 'Desktop' tab is active, displaying a 'Command Prompt' window. The Command Prompt shows the following commands and outputs:

```
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 FT Ftp server
Username:cisco
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>
```

Рис. 4.7: Проверка корректности настроенного доступа

5 Выводы

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

6 Контрольные вопросы

1. Как задать действие правила для конкретного протокола?

Например, `permit tcp any host 10.128.0.4 eq pop3`.

2. Как задать действие правила сразу для нескольких портов?

Для этого нужна команда `interface range`.

3. Как узнать номер правила в списке прав доступа?

С помощью команды `show access-lists`.

4. Каким образом можно изменить порядок применения правил в списке контроля доступа?

Команда `access-list <номер в списке> permit`.