Отчёт по лабораторной работе №10

дисциплина: Администрирование локальных сетей

Студент: Кузнецова София Вадимовна

Содержание

Список иллюстраций

Список таблиц

Цель работы

Изучить возможности протокола STP и его модификаций по обеспечению отказоустойчивости сети, агрегированию интерфейсов и перераспределению нагрузки между ними.

Выполнение лабораторной работы

Откроем проект с названием lab_PT-09.pkt и сохраним под названием lab_PT-10.pkt. После чего откроем его для дальнейшего редактирования.

Рис. 0.1: Открытие проекта lab_PT-10.pkt

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-svkuznecova-sw-4 и присвоим ему статический адрес 10.128.6.200, указав в качестве gateway-адреса 10.128.6.1 и адреса DNS-сервера 10.128.0.5. После чего пропингуем. Права доступа пользователей сети будем настраивать на маршрутизаторе msk- donskaya-svkuznecova-gw-1, поскольку именно через него проходит весь трафик сети. Ограничения можно накладывать как на входящий (in), так и на исходящий (out) трафик. По отношению к маршрутизатору накладываемые ограничения будут касаться в основном исходящего трафика. Различают стандартные (standard) и расширенные (extended) списки контроля доступа (Access Control List, ACL). Стандартные ACL проверяют только адрес источника трафика, расширенные адрес как источника, так и получателя, тип протокола и TCP/UDP порты.

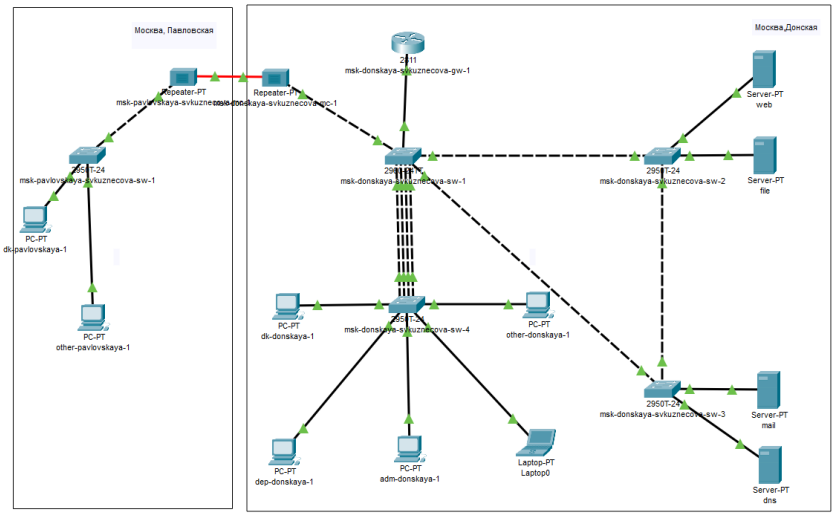

Рис. 0.2: Подсоединение ноутбука к порту 24 коммутатора msk-donskaya-svkuznecova-sw-4 и изменение названия

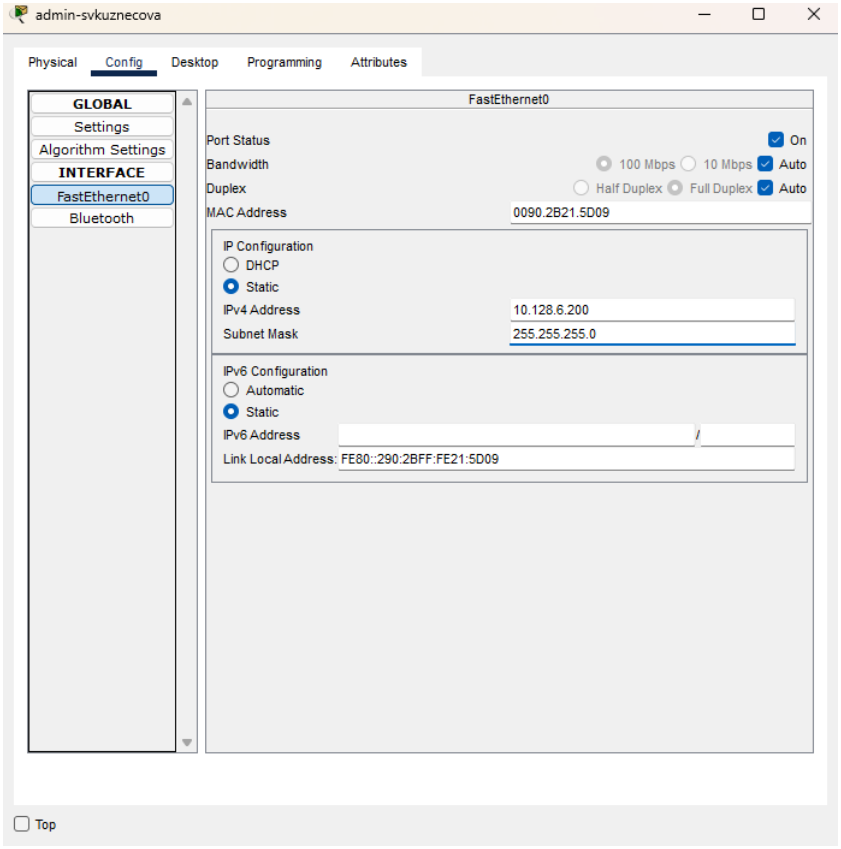

Рис. 0.3: Присвоение оконечному устройству статического адреса 10.128.6.200, gateway-адреса 10.128.6.1 и адреса DNS-сервера 10.128.0.5

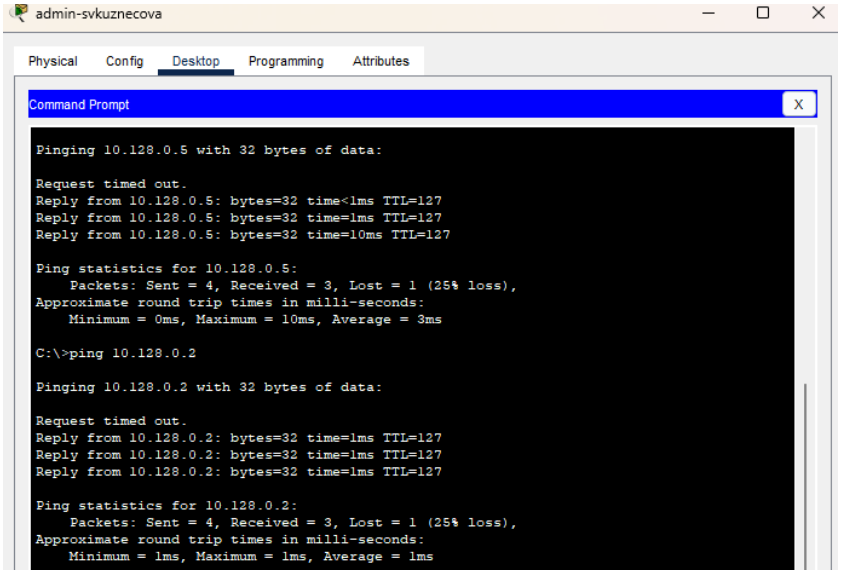

Рис. 0.4: Проверка (пингуем с admin-svkuznecova 10.128.0.2 и 10.128.0.5)

Далее настроим доступ к web-серверу по порту tcp 80. Здесь: 1. Создадим список контроля доступа с названием servers-out (так как предполагается ограничить доступ в конкретные подсети и по отношению к маршрутизатору это будет исходящий трафик); 2. Укажем (в качестве комментария-напоминания remark web), что ограничения предназначены для работы с web-сервером; 3. Дадим 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-svkuznecova-gw-1>en
Password:
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 web
msk-donskaya-svkuznecova-gw-1(config-ext-nacl)#permit tcp any host 10.128.0.2 eq 80
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. 0.5: Настройка доступа к web-серверу по порту tcp 80

Добавление списка управления доступом к интерфейсу. Здесь: - К интерфейсу f0/0.3 подключаем список прав доступа serversout и примяем к исходящему трафику

(out). Проверим, 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.

```
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. 0.6: 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. 0.7: Проверка демонстрации недоступности web-сервера как по имени, так и по ip-адресу web-сервера.

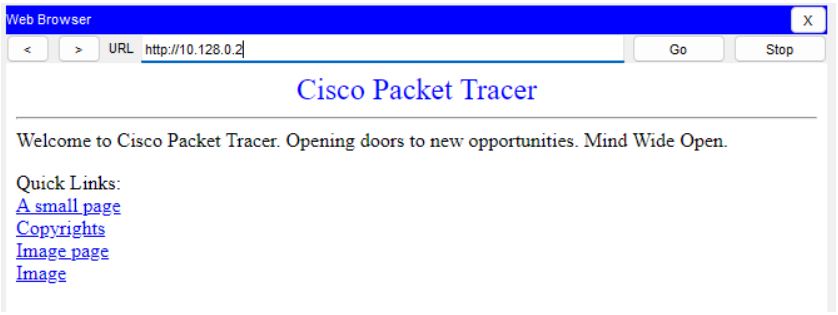

Рис. 0.8: Проверка доступа к web-серверу есть через протокол HTTP (введя в строке браузера хоста ip-адрес web-сервера)

Настроим дополнительный доступ для администратора по протоколам Telnet и FTP. Здесь: - В список контроля доступа servers-out добавим правило, разрешающее устройству администратора с ip-адресом 10.128.6.200 доступ на web-сервер (10.128.0.2) по протоколам FTP и telnet. Убедимся, что с узла с ip-адресом 10.128.6.200 есть доступ по протоколу FTP. Для этого в командной строке устройства администратора введём ftp 10.128.0.2, а затем по запросу имя пользователя cisco и пароль cisco. Попробуем провести аналогичную процедуру с другого устройства сети. Попробуем убедиться, что доступ будет запрещён.

```
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. 0.9: Настроим дополнительный доступ для администратора по протоколам Telnet и FTP

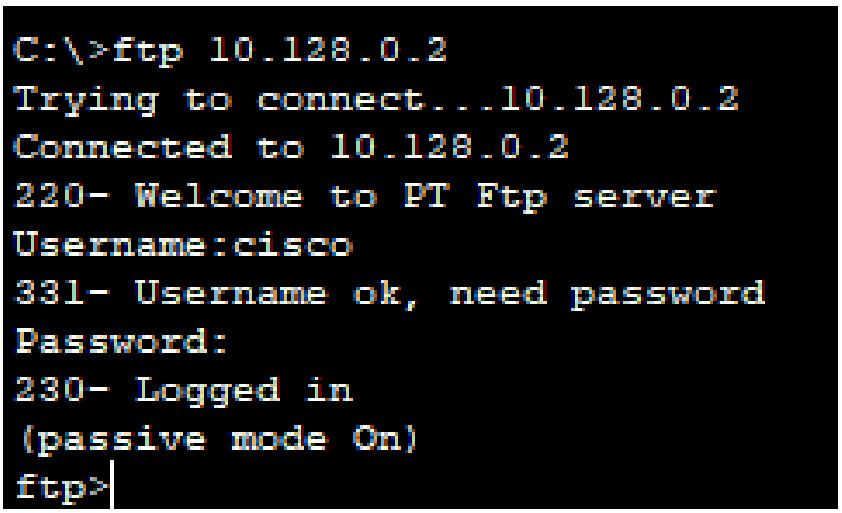

Рис. 0.10: Проверка доступа с узла 10.128.6.200 по протоколу FEP

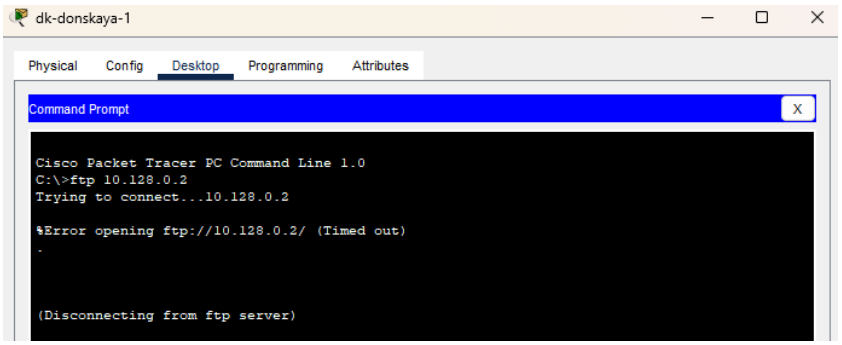

Рис. 0.11: Проверка доступа с устройства dk-donskaya-1 по протоколу FTP (доступ запрещён)

Настроим доступа к файловому серверу. Здесь: 1. В списке контроля доступа servers-out укажем (в качестве комментария-напоминания remark file), что следующие ограничения предназначены для работы с file-сервером; 2. Всем узлам внутренней сети (10.128.0.0) разрешим доступ по протоколу SMB (работает через порт 445 протокола TCP) к каталогам общего пользования; 3. Любым узлам разрешим доступ к file-серверу по протоколу FTP. Запись 0.0.255.255 — обратная маска (wildcard mask).

```
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. 0.12: Настройка доступа к файловому серверу

Теперь настроим доступа к почтовому серверу. Здесь: 1. В списке контроля доступа servers-out укажем (в качестве комментария-напоминания remark mail), что следующие ограничения предназначены для работы с почтовым сервером; 2. Всем разрешим доступ к почтовому серверу по протоколам POP3 и SMTP.

```
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. 0.13: Настройка доступа к почтовому серверу

Настройим доступа к DNS-серверу. Здесь: 1. В списке контроля доступа servers-out укажем (в качестве комментария-напоминания remark dns), что следующие ограничения пред назначены для работы с DNS-сервером; 2. Всем узлам внутренней сети разрешим доступ к DNS-серверу через UDP-порт 53.

```
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 dns
msk-donskaya-svkuznecova-gw-1(config-ext-nacl)#permit udp 10.128.0.0 0.0.255.255 host
10.128.0.5 eq 53
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. 0.14: Настройка доступа к DNS-серверу

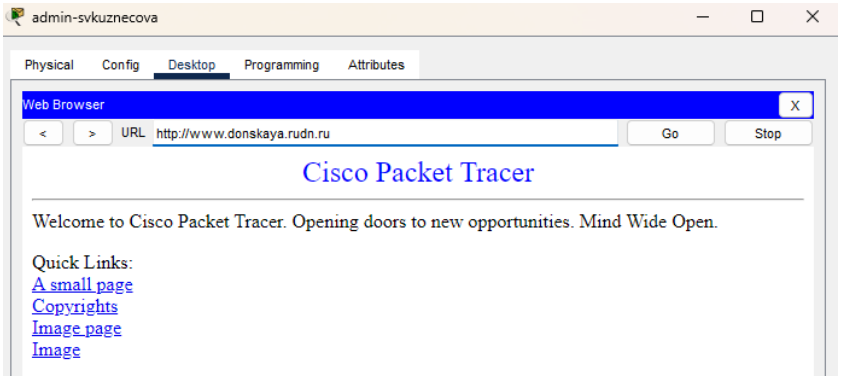

Рис. 0.15: Проверка доступности web-сервера(через браузер) по имени

Разрешим icmp-запросов. Здесь: - Демонстрируем явное управление порядком размещения правил правило разрешения для icmp-запросов добавляется в начало списка контроля доступа. Посмотрим номера строк правил в списке контроля доступа.

```
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. 0.16: Разрешим icmp-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. 0.17: Просмотр номеров строк правил в списке контроля доступа

Теперь настроим 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): 1. В списке контроля доступа other-in укажем, что следующие правила относятся к администратору сети; 2. Даём разрешение устройству с адресом 10.128.6.200 на любые действия (any); 3. К интерфейсу f0/0.104 подключаем список прав доступа other-in и применяеем к входящему трафику (in).

```
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-gorup 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. 0.18: Настройка доступа для сети Other

Настроим доступ администратора к сети сетевого оборудования.Здесь: 1. 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); 2. К интерфейсу f0/0.2 подключаем список прав доступа management-out и применяем к исходящему трафику (out).

```
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. 0.19: Настройка доступа администратора к сети сетевого оборудования

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

```
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. 0.20: Проверка корректности установленных правил доступа с оконечного устройства admin-svkuznecova.

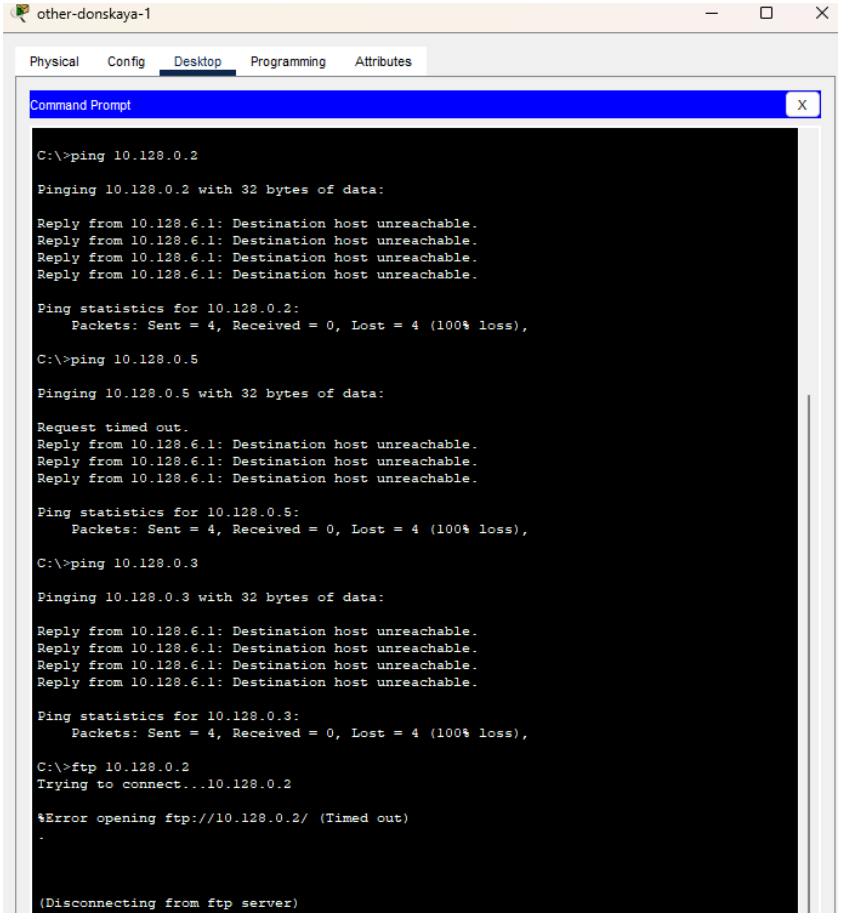

Рис. 0.21: Проверка корректности установленных правил доступа с оконечного устройства other-donskaya-1.

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

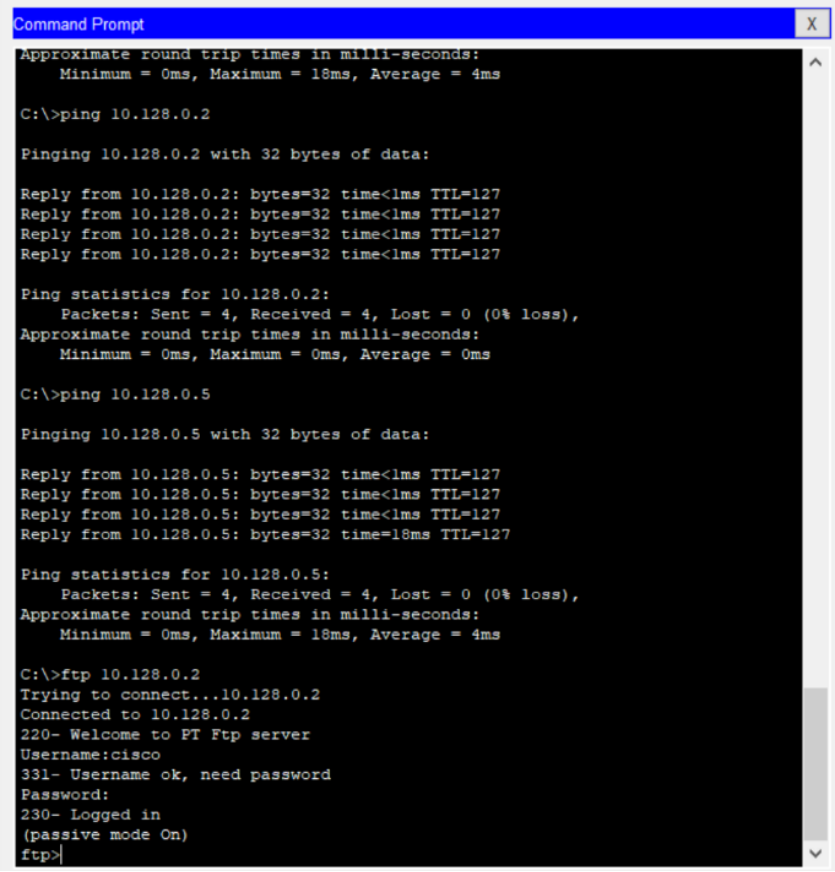

Рис. 0.22: Проверка разрешений администратора из сети Other на Павловской.

Выводы

В ходе выполнения лабораторной работы мы освоили настройку прав доступа польНастройка доступа к web-серверу по порту tcp 80зователей к ресурсам сети.

Ответы на контрольные вопросы

1. Как задать действие правила для конкретного протокола? – permit...
2. Как задать действие правила сразу для нескольких портов? - ...range...
3. Как узнать номер правила в списке прав доступа? – show access-lists
4. Каким образом можно изменить порядок применения правил в списке контроля доступа? – ip access-list resequence...