

Отчёт по лабораторной работе №10

Администрирование локальных сетей

Бансимба Клодели Дъегра, НПИбд-02-22

Содержание

1	Цель работы	6
2	Выполнение лабораторной работы	7
3	Выводы	26
4	Ответы на контрольные вопросы:	27

Список иллюстраций

2.1	Открытие проекта lab_PT-10.pkt	7
2.2	Подсоединение ноутбука к порту 24 коммутатора msk-donskaya-claudely-sw-4 и изменение названия.	8
2.3	Присвоение оконечному устройству статического адреса 10.128.6.200, gateway-адреса 10.128.6.1 и адреса DNS-сервера 10.128.0.5.	8
2.4	Присвоение оконечному устройству статического адреса 10.128.6.200, gateway-адреса 10.128.6.1 и адреса DNS-сервера 10.128.0.5.	9
2.5	Настройка доступа к web-серверу по порту tcp 80 (создан список контроля доступа с названием servers-out; указано, что ограничения предназначены для работы с web-сервером; дано разрешение доступа по протоколу TCP всем пользователям сети на доступ к web-серверу, имеющему адрес 10.128.0.2, через порт 80).	10
2.6	Добавление списка управления доступом к интерфейсу (к интерфейсу f0/0.3 подключается список прав доступа serversout и применяется к исходящему трафику).	11
2.7	Проверка демонстрации недоступности web-сервера при использовании команды ping по ip-адресу web-сервера.	12
2.8	Проверка доступа к web-серверу через протокол HTTP (ввод в строке браузера хоста ip-адреса web-сервера).	12
2.9	Настройка дополнительного доступа для администратора по протоколам Telnet и FTP (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).	13
2.10	Проверка доступа с узла с ip-адресом 10.128.6.200 по протоколу FTP.	14
2.11	Проверка доступа с устройства dk-donskaya-1 по протоколу FTP (доступ запрещён).	14
2.12	Настройка доступа к файловому серверу (в списке контроля доступа servers-out указано, что следующие ограничения предназначены для работы с file-сервером; всем узлам внутренней сети (10.128.0.0) разрешён доступ по протоколу SMB к каталогам общего пользования; любым узлам разрешён доступ к file-серверу по протоколу FTP (запись 0.0.255.255 — обратная маска).	15

2.13	Настройка доступа к почтовому серверу (в списке контроля доступа servers-out указано, что следующие ограничения предназначены для работы с почтовым сервером; всем разрешён доступ к почтовому серверу по протоколам POP3 и SMTP).	16
2.14	Настройка доступа к DNS-серверу (в списке контроля доступа servers-out указано, что следующие ограничения предназначены для работы с DNS-сервером; всем узлам внутренней сети разрешён доступ к DNS-серверу через UDP-порт 53)	17
2.15	Проверка доступности web-сервера (через браузер) по имени. . . .	17
2.16	Разрешение icmp-запросов (демонстрируется явное управление порядком размещения правил — правило разрешения для icmp-запросов добавляется в начало списка контроля доступ).	18
2.17	Просмотр номеров строк правил в списке контроля доступа.	19
2.18	Настройка доступа для сети Other (в списке контроля доступа other-in указано, что следующие правила относятся к администратору сети; разрешение устройству с адресом 10.128.6.200 на любые действия; подключение к интерфейсу f0/0.104 списка прав доступа other-in и применение к входящему трафику).	20
2.19	Настройка доступа администратора к сети сетевого оборудования (в списке контроля доступа management-out указано, что устройству администратора с адресом 10.128.6.200 разрешён доступ к сети сетевого оборудования (10.128.1.0); к интерфейсу f0/0.2 подключён список прав доступа management-out и применено к исходящему трафику)	21
2.20	Проверка корректности установленных правил доступа с оконечного устройства admin-claudely.	22
2.21	Проверка корректности установленных правил доступа с оконечного устройства other-donskaya-1.	23
2.22	Разрешение администратору из сети Other на Павловской действия, аналогичные действиям администратора сети Other на Донской. . .	24
2.23	Проверка разрешений администратора из сети Other на Павловской. .	25

Список таблиц

1 Цель работы

Освоить настройку прав доступа пользователей к ресурсам сети.

2 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. fig. 2.1).

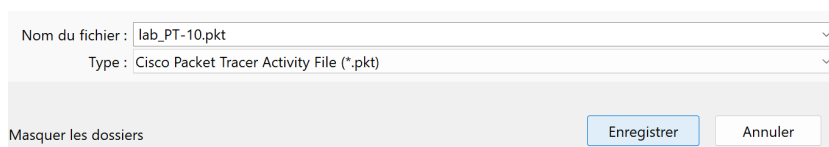


Рис. 2.1: Открытие проекта lab_PT-10.pkt

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-claudely-sw-4 (Рис. 1.2) 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 (Рис. 1.3). После чего пропингуем (Рис. 1.4). Права доступа пользователей сети будем настраивать на маршрутизаторе msk-donskaya-claudely-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.

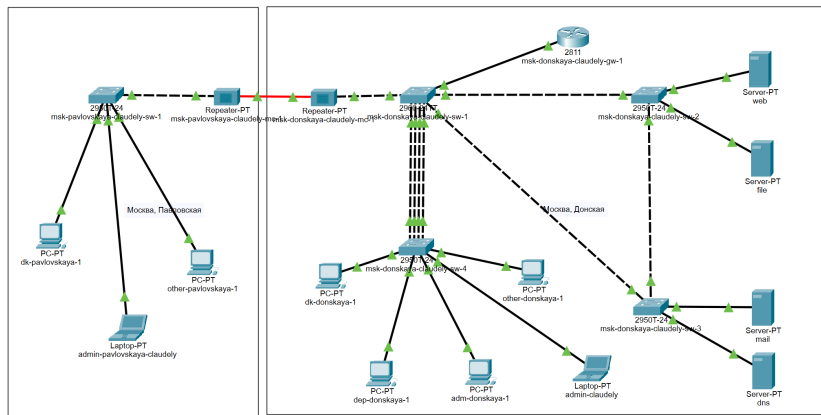


Рис. 2.2: Подсоединение ноутбука к порту 24 коммутатора msk-donskaya-claudely-sw-4 и изменение названия.

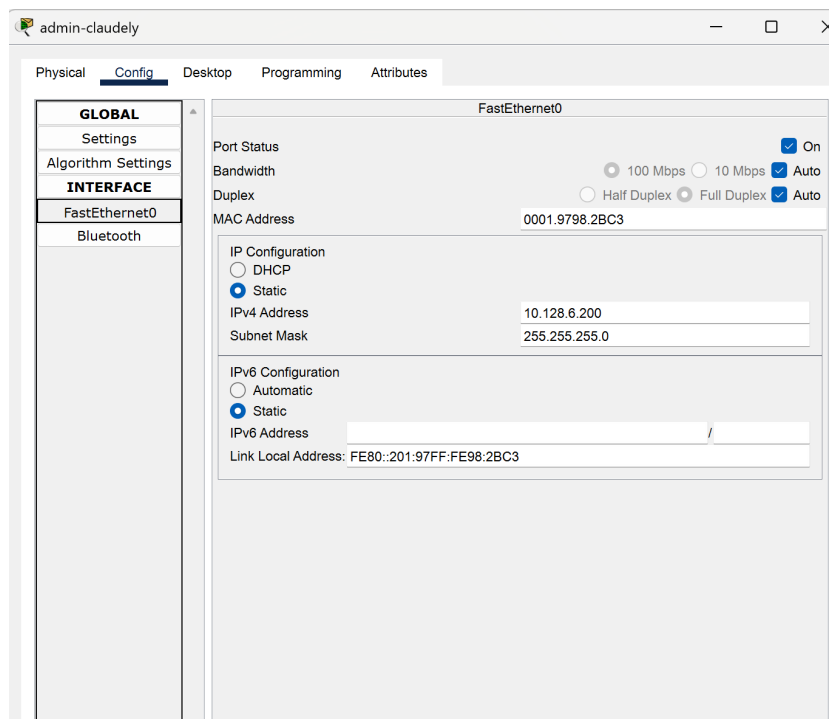


Рис. 2.3: Присвоение оконечному устройству статического адреса 10.128.6.200, gateway-адреса 10.128.6.1 и адреса DNS-сервера 10.128.0.5.

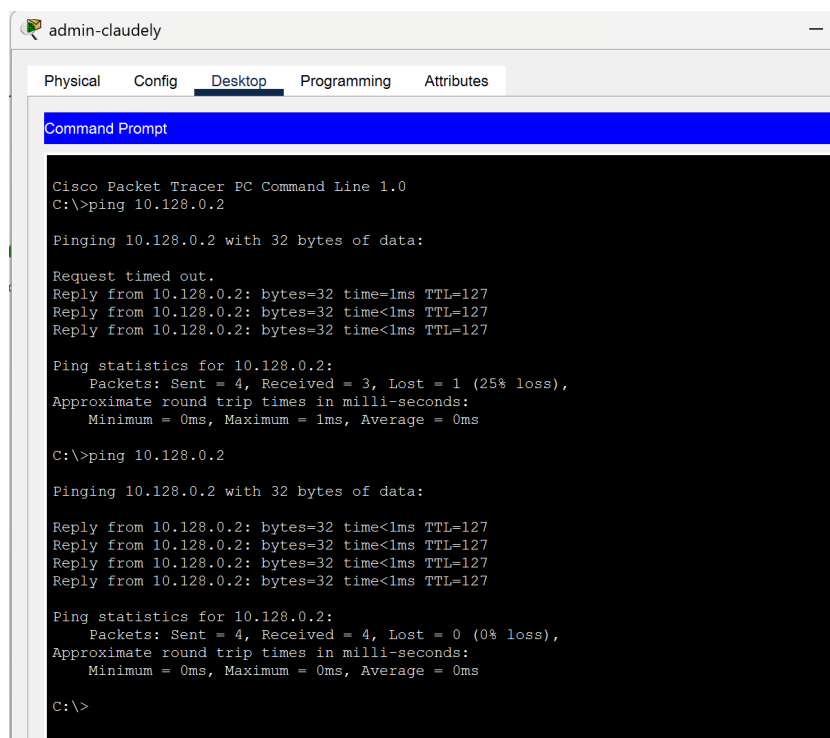
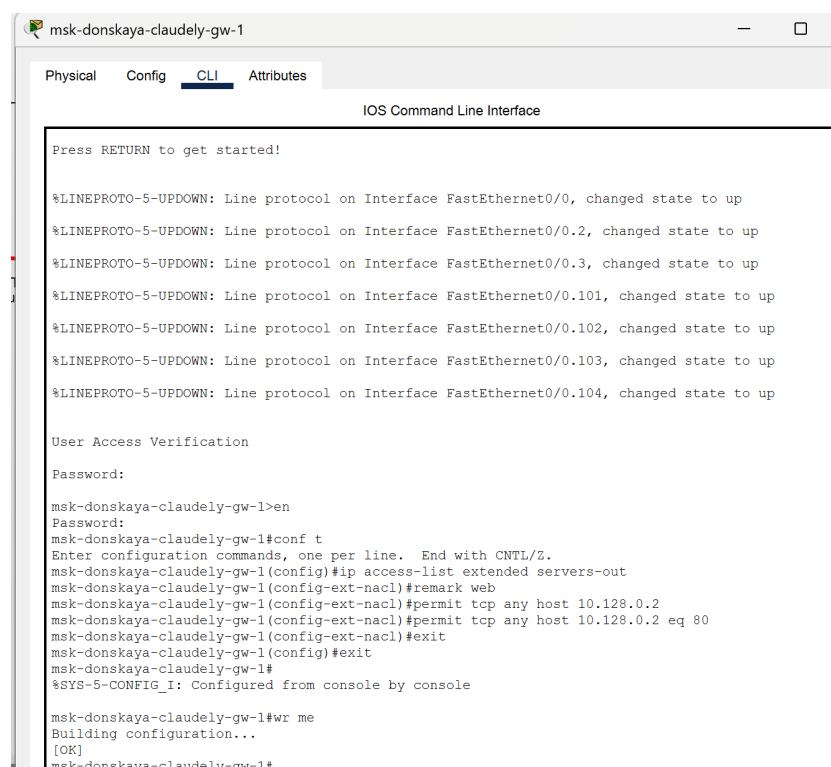


Рис. 2.4: Присвоение оконечному устройству статического адреса 10.128.6.200, gateway-адреса 10.128.6.1 и адреса DNS-сервера 10.128.0.5.

Далее настроим доступ к web-серверу по порту tcp 80. Здесь (Рис. 1.5): 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-claudely-gw-1
Physical Config CLI Attributes
IOS Command Line Interface

Press RETURN to get started!

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.2, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.3, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.101, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.102, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.103, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.104, changed state to up

User Access Verification

Password:

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

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

Рис. 2.5: Настройка доступа к web-серверу по порту tcp 80 (создан список контроля доступа с названием servers-out; указано, что ограничения предназначены для работы с web-сервером; дано разрешение доступа по протоколу TCP всем пользователям сети на доступ к web-серверу, имеющему адрес 10.128.0.2, через порт 80).

Добавим список управления доступом к интерфейсу. Здесь (Рис. 1.6): • К интерфейсу f0/0.3 подключаем список прав доступа serversout и применяем 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)

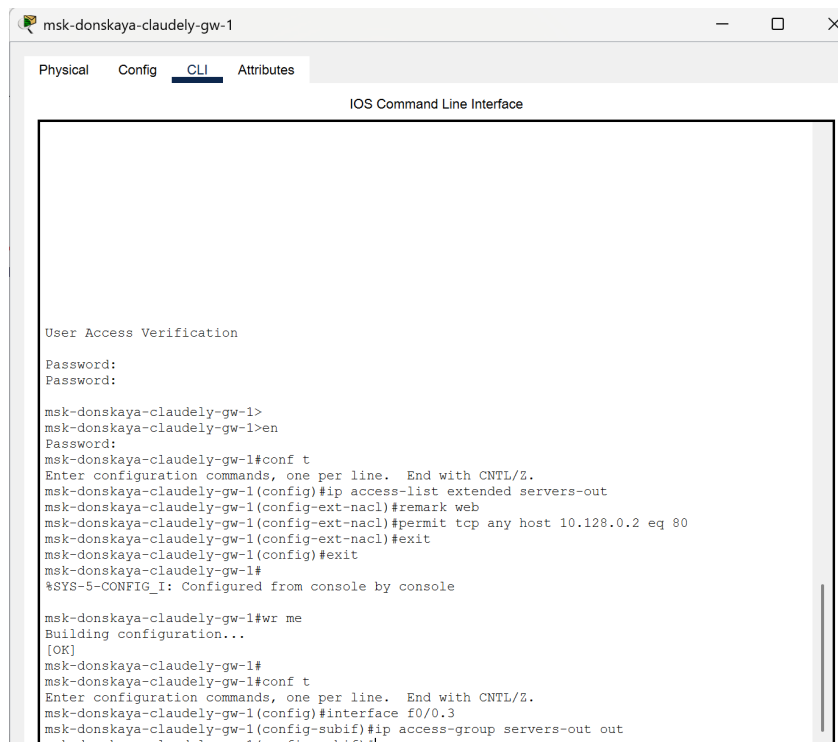


Рис. 2.6: Добавление списка управления доступом к интерфейсу (к интерфейсу f0/0.3 подключается список прав доступа serversout и применяется к исходящему трафику).

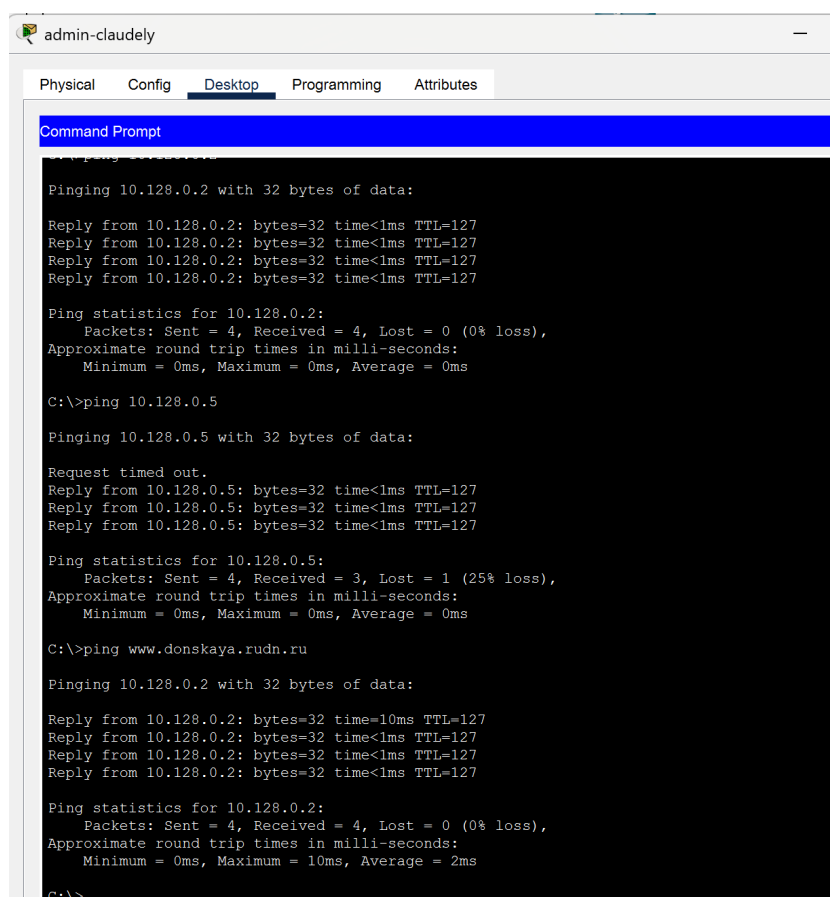


Рис. 2.7: Проверка демонстрации недоступности web-сервера при использовании команды ping по ip-адресу web-сервера.

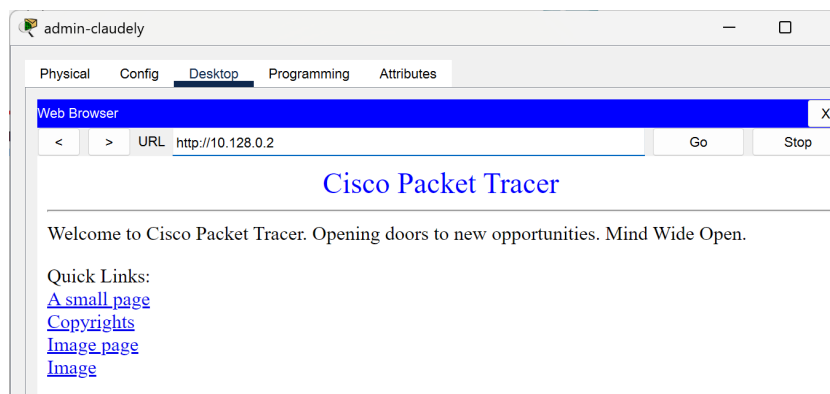


Рис. 2.8: Проверка доступа к web-серверу через протокол HTTP (ввод в строке браузера хоста ip-адреса web-сервера).

Настроим дополнительный доступ для администратора по протоколам Telnet и FTP. Здесь (Рис. 1.9):

- В список контроля доступа servers-out добавим прави-

ло, 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 (Рис. 1.10). Попробуем провести аналогичную процедуру с другого устройства сети и убедимся, что доступ будет запрещён

```

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

msk-donskaya-claudely-gw-1#
msk-donskaya-claudely-gw-1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
msk-donskaya-claudely-gw-1(config)#ip access-list extended servers-out
msk-donskaya-claudely-gw-1(config-ext-nacl)#permit tcp any host 10.128.6.200 host 10.128.0.2 range 20 ftp
% Invalid input detected at '^' marker.

msk-donskaya-claudely-gw-1(config-ext-nacl)#permit tcp host 10.128.6.200 host 10.128.0.2 range 20 ftp
msk-donskaya-claudely-gw-1(config-ext-nacl)#permit tcp host 10.128.6.200 host 10.128.0.2 eq telnet
msk-donskaya-claudely-gw-1(config-ext-nacl)#exit
msk-donskaya-claudely-gw-1(config)#exit
msk-donskaya-claudely-gw-1#
%SYS-5-CONFIG_I: Configured from console by console

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

```

Рис. 2.9: Настройка дополнительного доступа для администратора по протоколам Telnet и FTP (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).

```
admin-claudely
Physical Config Desktop Programming Attributes
Command Prompt
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:\>
C:\>
C:\>
C:\>
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<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:\>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. 2.10: Проверка доступа с узла с ip-адресом 10.128.6.200 по протоколу FTP.

```
dk-donskaya-1
Physical Config Desktop Programming Attributes
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
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. 2.11: Проверка доступа с устройства dk-donskaya-1 по протоколу FTP (доступ запрещён).

Настроим доступ к файловому серверу. Здесь (Рис. 1.12): 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-claudely-gw-1
msk-donskaya-claudely-gw-1(config-ext-nacl)#permit tcp host 10.128.6.200 host 10.128.0.2 range
20 ftp
msk-donskaya-claudely-gw-1(config-ext-nacl)#permit tcp host 10.128.6.200 host 10.128.0.2 eq
telnet
msk-donskaya-claudely-gw-1(config-ext-nacl)#exit
msk-donskaya-claudely-gw-1(config)#exit
msk-donskaya-claudely-gw-1#
%SYS-5-CONFIG_I: Configured from console by console

msk-donskaya-claudely-gw-1#wr me
Building configuration...
[OK]
msk-donskaya-claudely-gw-1#
msk-donskaya-claudely-gw-1#
msk-donskaya-claudely-gw-1#
msk-donskaya-claudely-gw-1#
msk-donskaya-claudely-gw-1#
msk-donskaya-claudely-gw-1#
msk-donskaya-claudely-gw-1#
msk-donskaya-claudely-gw-1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
msk-donskaya-claudely-gw-1(config)#ip access-list extended servers-out
msk-donskaya-claudely-gw-1(config-ext-nacl)#remark file
msk-donskaya-claudely-gw-1(config-ext-nacl)#permit tcp host 10.128.0.0 0.0.255.255 host
10.128.0.3 eq 445
% Invalid input detected at '^' marker.

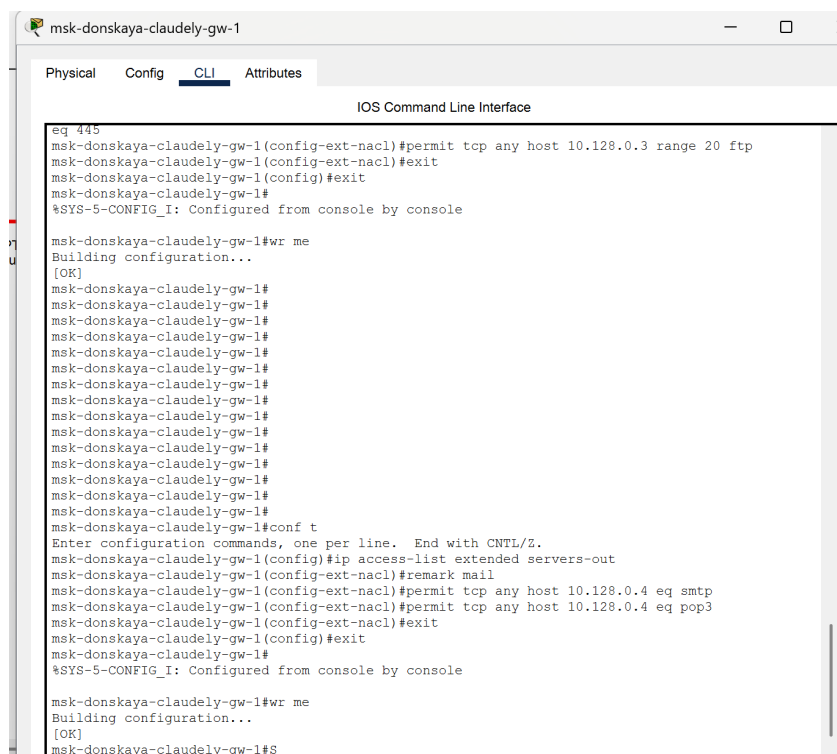
msk-donskaya-claudely-gw-1(config-ext-nacl)#permit tcp 10.128.0.0 0.0.255.255 host 10.128.0.3
eq 445
msk-donskaya-claudely-gw-1(config-ext-nacl)#permit tcp any host 10.128.0.3 range 20 ftp
msk-donskaya-claudely-gw-1(config-ext-nacl)#exit
msk-donskaya-claudely-gw-1(config)#exit
msk-donskaya-claudely-gw-1#
%SYS-5-CONFIG_I: Configured from console by console

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

```

Рис. 2.12: Настройка доступа к файловому серверу (в списке контроля доступа servers-out указано, что следующие ограничения предназначены для работы с file-сервером; всем узлам внутренней сети (10.128.0.0) разрешён доступ по протоколу SMB к каталогам общего пользования; любым узлам разрешён доступ к file-серверу по протоколу FTP (запись 0.0.255.255 — обратная маска).

Затем настроим доступ к почтовому серверу. Здесь (Рис. 1.13): 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-claudely-gw-1
Physical Config CLI Attributes
IOS Command Line Interface
eq 445
msk-donskaya-claudely-gw-1(config-ext-nacl)#permit tcp any host 10.128.0.3 range 20 ftp
msk-donskaya-claudely-gw-1(config-ext-nacl)#exit
msk-donskaya-claudely-gw-1(config)#exit
msk-donskaya-claudely-gw-1#
%SYS-5-CONFIG_I: Configured from console by console

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

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

Рис. 2.13: Настройка доступа к почтовому серверу (в списке контроля доступа servers-out указано, что следующие ограничения предназначены для работы с почтовым сервером; всем разрешён доступ к почтовому серверу по протоколам POP3 и SMTP).

Настроим доступ к DNS-серверу. Здесь (Рис. 1.14): 1. В списке контроля доступа servers-out укажем (в качестве комментария-напоминания remark dns), что следующие ограничения предназначены для работы с DNS-сервером; 2. Всем узлам внутренней сети разрешим доступ к DNS-серверу через UDP-порт 53. Проверим доступность web-сервера (через браузер) не только по ip-адресу, но и по имени

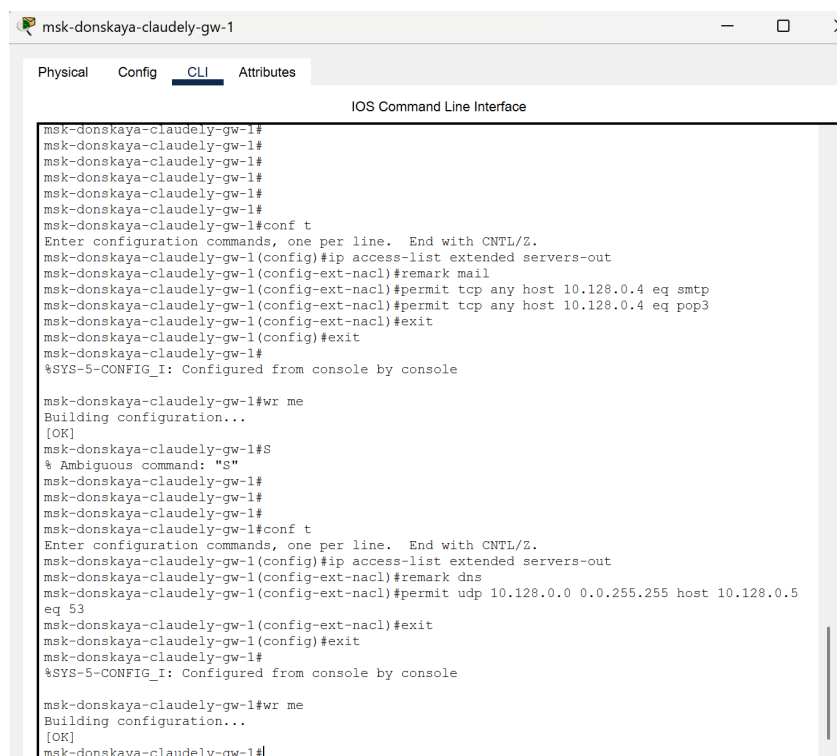


Рис. 2.14: Настройка доступа к DNS-серверу (в списке контроля доступа servers-out указано, что следующие ограничения предназначены для работы с DNS-сервером; всем узлам внутренней сети разрешён доступ к DNS-серверу через UDP-порт 53)

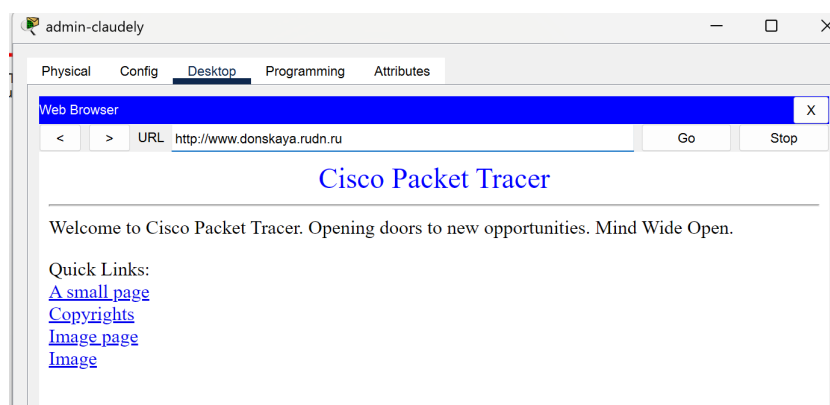
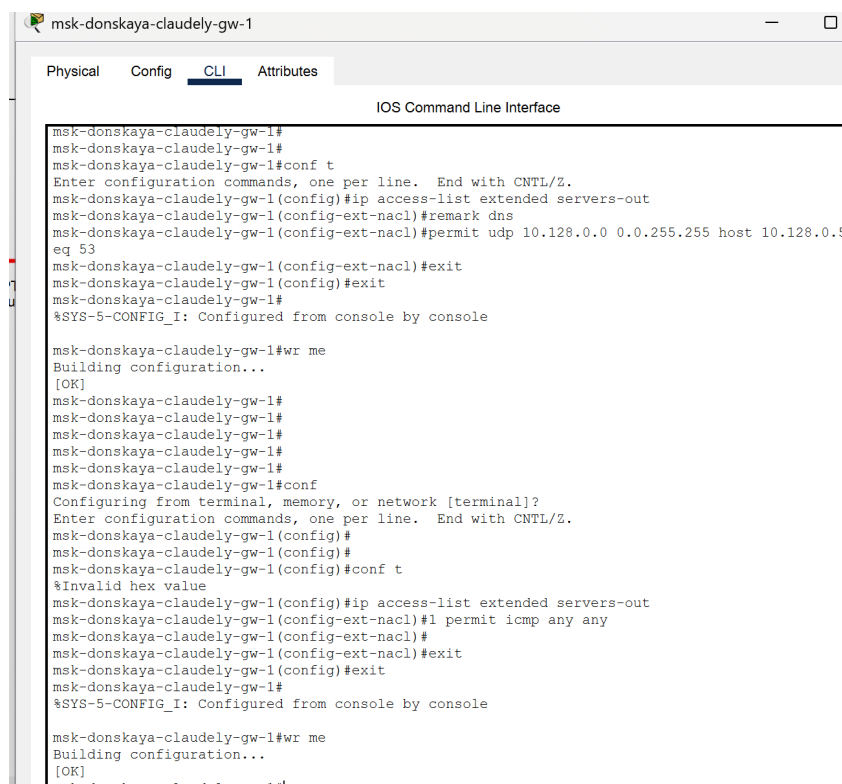


Рис. 2.15: Проверка доступности web-сервера (через браузер) по имени.

Разрешим iстр-запросы. Здесь (Рис. 1.16): • Демонстрируем явное управление порядком размещения правил — правило разрешения для iстр-запросов добавляется в начало списка контроля доступа. Номера строк правил в списке

контроля доступа можно посмотреть с помощью команды `show access -lists`

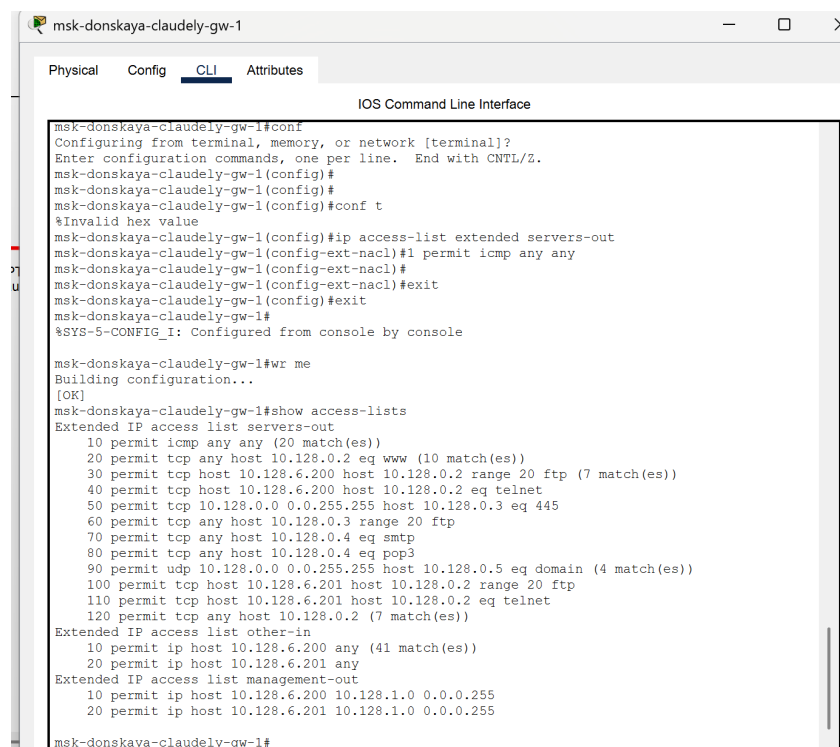


```
msk-donskaya-claudely-gw-1#
msk-donskaya-claudely-gw-1#
msk-donskaya-claudely-gw-1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
msk-donskaya-claudely-gw-1(config)#ip access-list extended servers-out
msk-donskaya-claudely-gw-1(config-ext-nacl)#remark dns
msk-donskaya-claudely-gw-1(config-ext-nacl)#permit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

msk-donskaya-claudely-gw-1#wr me
Building configuration...
[OK]
msk-donskaya-claudely-gw-1#
msk-donskaya-claudely-gw-1#
msk-donskaya-claudely-gw-1#
msk-donskaya-claudely-gw-1#
msk-donskaya-claudely-gw-1#conf
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
msk-donskaya-claudely-gw-1(config)#
msk-donskaya-claudely-gw-1(config)#
msk-donskaya-claudely-gw-1(config)#conf t
%Invalid hex value
msk-donskaya-claudely-gw-1(config)#ip access-list extended servers-out
msk-donskaya-claudely-gw-1(config-ext-nacl)#1 permit icmp any any
msk-donskaya-claudely-gw-1(config-ext-nacl)#
msk-donskaya-claudely-gw-1(config-ext-nacl)#exit
msk-donskaya-claudely-gw-1(config)#exit
msk-donskaya-claudely-gw-1#
%SYS-5-CONFIG_I: Configured from console by console

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

Рис. 2.16: Разрешение icmp-запросов (демонстрируется явное управление порядком размещения правил — правило разрешения для icmp-запросов добавляется в начало списка контроля доступ).

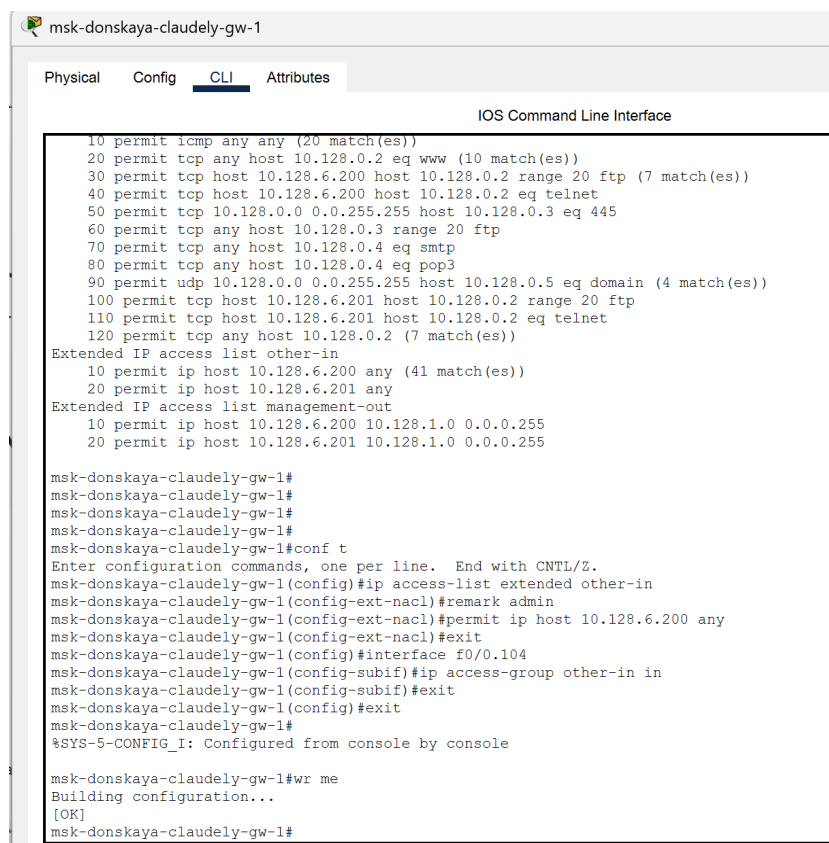


```
msk-donskaya-claudely-gw-1#conf t
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
msk-donskaya-claudely-gw-1(config)#
msk-donskaya-claudely-gw-1(config)#
msk-donskaya-claudely-gw-1(config)#conf t
%Invalid hex value
msk-donskaya-claudely-gw-1(config)#ip access-list extended servers-out
msk-donskaya-claudely-gw-1(config-ext-nacl)#1 permit icmp any any
msk-donskaya-claudely-gw-1(config-ext-nacl)#
msk-donskaya-claudely-gw-1(config-ext-nacl)#exit
msk-donskaya-claudely-gw-1(config)#exit
msk-donskaya-claudely-gw-1#
%SYS-5-CONFIG_I: Configured from console by console

msk-donskaya-claudely-gw-1#wr me
Building configuration...
[OK]
msk-donskaya-claudely-gw-1#show access-lists
Extended IP access list servers-out
 10 permit icmp any any (20 match(es))
 20 permit tcp any host 10.128.0.2 eq www (10 match(es))
 30 permit tcp host 10.128.6.200 host 10.128.0.2 range 20 ftp (7 match(es))
 40 permit tcp host 10.128.6.200 host 10.128.0.2 eq telnet
 50 permit tcp 10.128.0.0 0.0.255.255 host 10.128.0.3 eq 445
 60 permit tcp any host 10.128.0.3 range 20 ftp
 70 permit tcp any host 10.128.0.4 eq smtp
 80 permit tcp any host 10.128.0.4 eq pop3
 90 permit udp 10.128.0.0 0.0.255.255 host 10.128.0.5 eq domain (4 match(es))
100 permit tcp host 10.128.6.201 host 10.128.0.2 range 20 ftp
110 permit tcp host 10.128.6.201 host 10.128.0.2 eq telnet
120 permit tcp any host 10.128.0.2 (7 match(es))
Extended IP access list other-in
 10 permit ip host 10.128.6.200 any (41 match(es))
 20 permit ip host 10.128.6.201 any
Extended IP access list management-out
 10 permit ip host 10.128.6.200 10.128.1.0 0.0.0.255
 20 permit ip host 10.128.6.201 10.128.1.0 0.0.0.255
msk-donskaya-claudely-gw-1#
```

Рис. 2.17: Просмотр номеров строк правил в списке контроля доступа.

Теперь настроим доступ для сети Other (требуется наложить ограничение на исходящий из сети Other трафик, который по отношению к маршрутизатору msk-claudely-donskaya-gw-1 является входящим трафиком). Здесь (Рис. 1.18): 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 применяем к входящему трафику



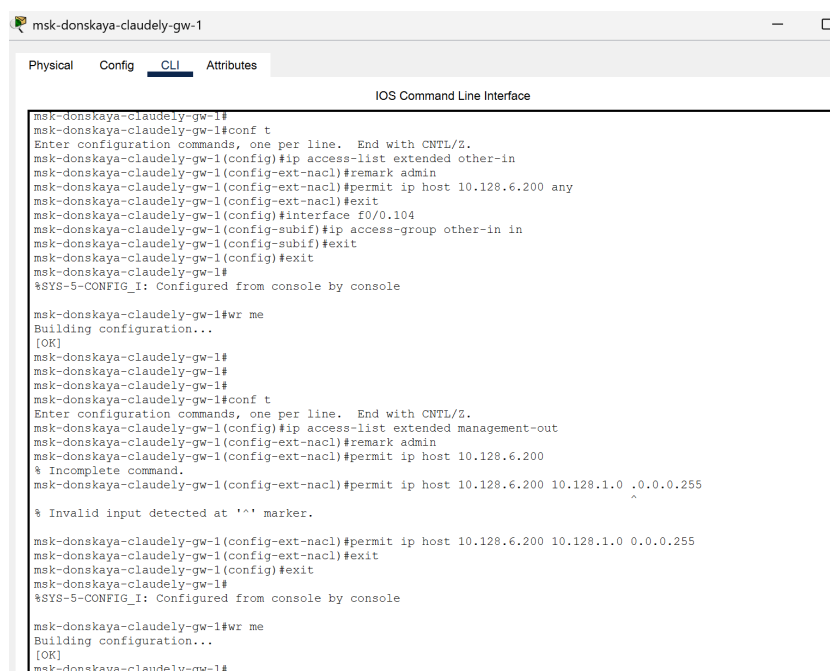
```
msk-donskaya-claudely-gw-1
Physical Config CLI Attributes
IOS Command Line Interface
10 permit icmp any any (20 match(es))
20 permit tcp any host 10.128.0.2 eq www (10 match(es))
30 permit tcp host 10.128.6.200 host 10.128.0.2 range 20 ftp (7 match(es))
40 permit tcp host 10.128.6.200 host 10.128.0.2 eq telnet
50 permit tcp 10.128.0.0 0.0.255.255 host 10.128.0.3 eq 445
60 permit tcp any host 10.128.0.3 range 20 ftp
70 permit tcp any host 10.128.0.4 eq smtp
80 permit tcp any host 10.128.0.4 eq pop3
90 permit udp 10.128.0.0 0.0.255.255 host 10.128.0.5 eq domain (4 match(es))
100 permit tcp host 10.128.6.201 host 10.128.0.2 range 20 ftp
110 permit tcp host 10.128.6.201 host 10.128.0.2 eq telnet
120 permit tcp any host 10.128.0.2 (7 match(es))
Extended IP access list other-in
10 permit ip host 10.128.6.200 any (41 match(es))
20 permit ip host 10.128.6.201 any
Extended IP access list management-out
10 permit ip host 10.128.6.200 10.128.1.0 0.0.0.255
20 permit ip host 10.128.6.201 10.128.1.0 0.0.0.255

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

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

Рис. 2.18: Настройка доступа для сети Other (в списке контроля доступа other-in указано, что следующие правила относятся к администратору сети; разрешение устройству с адресом 10.128.6.200 на любые действия; подключение к интерфейсу f0/0.104 списка прав доступа other-in и применение к входящему трафику).

Настроим доступ администратора к сети сетевого оборудования. Здесь (Рис. 1.19): 1. В списке контроля доступа management-out укажем (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-claudely-gw-1#
msk-donskaya-claudely-gw-1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
msk-donskaya-claudely-gw-1(config)#ip access-list extended other-in
msk-donskaya-claudely-gw-1(config-ext-nacl)#remark admin
msk-donskaya-claudely-gw-1(config-ext-nacl)#permit ip host 10.128.6.200 any
msk-donskaya-claudely-gw-1(config-ext-nacl)#exit
msk-donskaya-claudely-gw-1(config)#interface f0/0.104
msk-donskaya-claudely-gw-1(config-subif)#ip access-group other-in in
msk-donskaya-claudely-gw-1(config-subif)#exit
msk-donskaya-claudely-gw-1(config)#exit
msk-donskaya-claudely-gw-1#
%SYS-5-CONFIG_I: Configured from console by console

msk-donskaya-claudely-gw-1#wr me
Building configuration...
[OK]
msk-donskaya-claudely-gw-1#
msk-donskaya-claudely-gw-1#
msk-donskaya-claudely-gw-1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
msk-donskaya-claudely-gw-1(config)#ip access-list extended management-out
msk-donskaya-claudely-gw-1(config-ext-nacl)#remark admin
msk-donskaya-claudely-gw-1(config-ext-nacl)#permit ip host 10.128.6.200
% Incomplete command.
msk-donskaya-claudely-gw-1(config-ext-nacl)#permit ip host 10.128.6.200 10.128.1.0 .0.0.0.255
% Invalid input detected at '^' marker.
msk-donskaya-claudely-gw-1(config-ext-nacl)#permit ip host 10.128.6.200 10.128.1.0 0.0.0.255
msk-donskaya-claudely-gw-1(config-ext-nacl)#exit
msk-donskaya-claudely-gw-1(config)#exit
msk-donskaya-claudely-gw-1#
%SYS-5-CONFIG_I: Configured from console by console

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

Рис. 2.19: Настройка доступа администратора к сети сетевого оборудования (в списке контроля доступа management-out указано, что устройству администратора с адресом 10.128.6.200 разрешён доступ к сети сетевого оборудования (10.128.1.0); к интерфейсу f0/0.2 подключён список прав доступа management-out и применено к исходящему трафику)

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

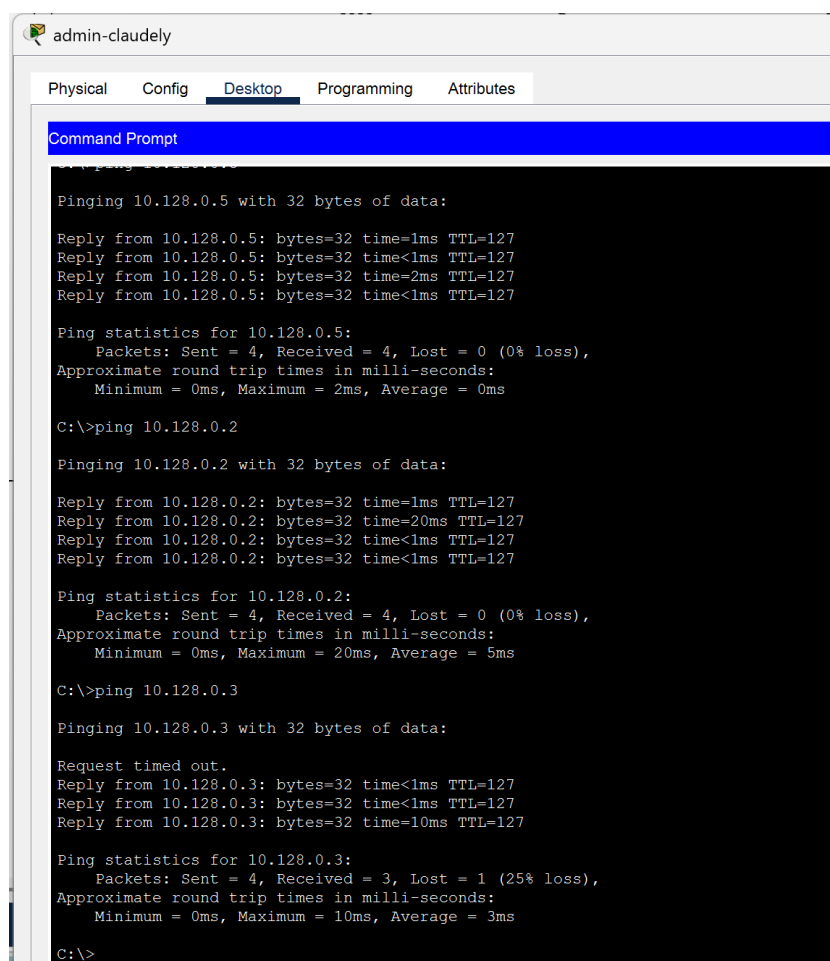


Рис. 2.20: Проверка корректности установленных правил доступа с оконечного устройства admin-claudely.

```
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:\>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.
```

Рис. 2.21: 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

```
msk-donskaya-claudely-gw-1
Physical Config CLI Attributes
IOS Command Line Interface
msk-donskaya-claudely-gw-1(config-ext-nacl)#permit ip host 10.128.6.200 10.128.1.0 0.0.0.255
msk-donskaya-claudely-gw-1(config-ext-nacl)#exit
msk-donskaya-claudely-gw-1(config)#exit
msk-donskaya-claudely-gw-1#
%SYS-5-CONFIG_I: Configured from console by console

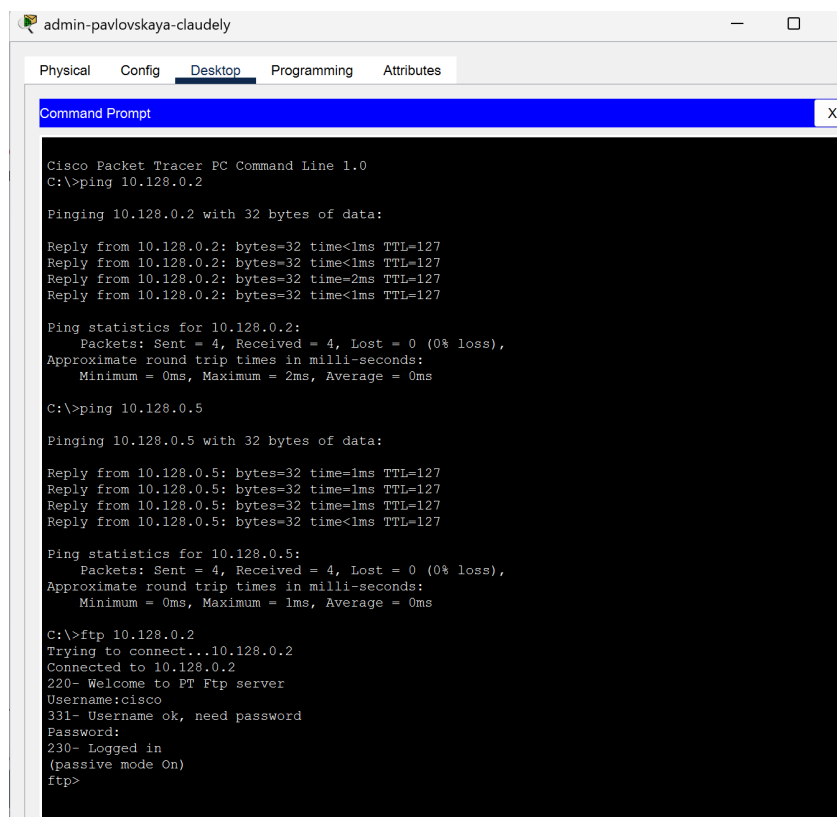
msk-donskaya-claudely-gw-1#wr me
Building configuration...
[OK]
msk-donskaya-claudely-gw-1#
msk-donskaya-claudely-gw-1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
msk-donskaya-claudely-gw-1(config)#ip access-list extended management-out
msk-donskaya-claudely-gw-1(config-ext-nacl)#remark admin
msk-donskaya-claudely-gw-1(config-ext-nacl)#permit ip host 10.128.6.200 10.128.1.0 0.0.0.255
msk-donskaya-claudely-gw-1(config-ext-nacl)#permit ip host 10.128.6.201 10.128.1.0 0.0.0.255
msk-donskaya-claudely-gw-1(config-ext-nacl)#exit
msk-donskaya-claudely-gw-1(config)#interface f0/0.2
msk-donskaya-claudely-gw-1(config-subif)#ip access-group management-out
% Incomplete command.
msk-donskaya-claudely-gw-1(config-subif)#ip access-group management-out out
msk-donskaya-claudely-gw-1(config-subif)#exit
msk-donskaya-claudely-gw-1(config)#wr me
^
% Invalid input detected at '^' marker.

msk-donskaya-claudely-gw-1(config)#
msk-donskaya-claudely-gw-1(config)#wr me
^
% Invalid input detected at '^' marker.

msk-donskaya-claudely-gw-1(config)#exit
msk-donskaya-claudely-gw-1#
%SYS-5-CONFIG_I: Configured from console by console

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

Рис. 2.22: Разрешение администратору из сети Other на Павловской действия, аналогичные действиям администратора сети Other на Донской.



The screenshot shows a Cisco Packet Tracer PC Command Line window for a device named 'admin-pavlovskaya-claudely'. The window has tabs for 'Physical', 'Config', 'Desktop', 'Programming', and 'Attributes', with 'Desktop' selected. The command prompt shows the following sequence of commands and outputs:

```
Cisco Packet Tracer PC Command Line 1.0
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=2ms 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 = 2ms, 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:\>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. 2.23: Проверка разрешений администратора из сети Other на Павловской.

3 Выводы

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

4 Ответы на контрольные вопросы:

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...`