

Администрирование локальных сетей

Лабораторная работа №10

Скандарова Полина Юрьевна

Содержание

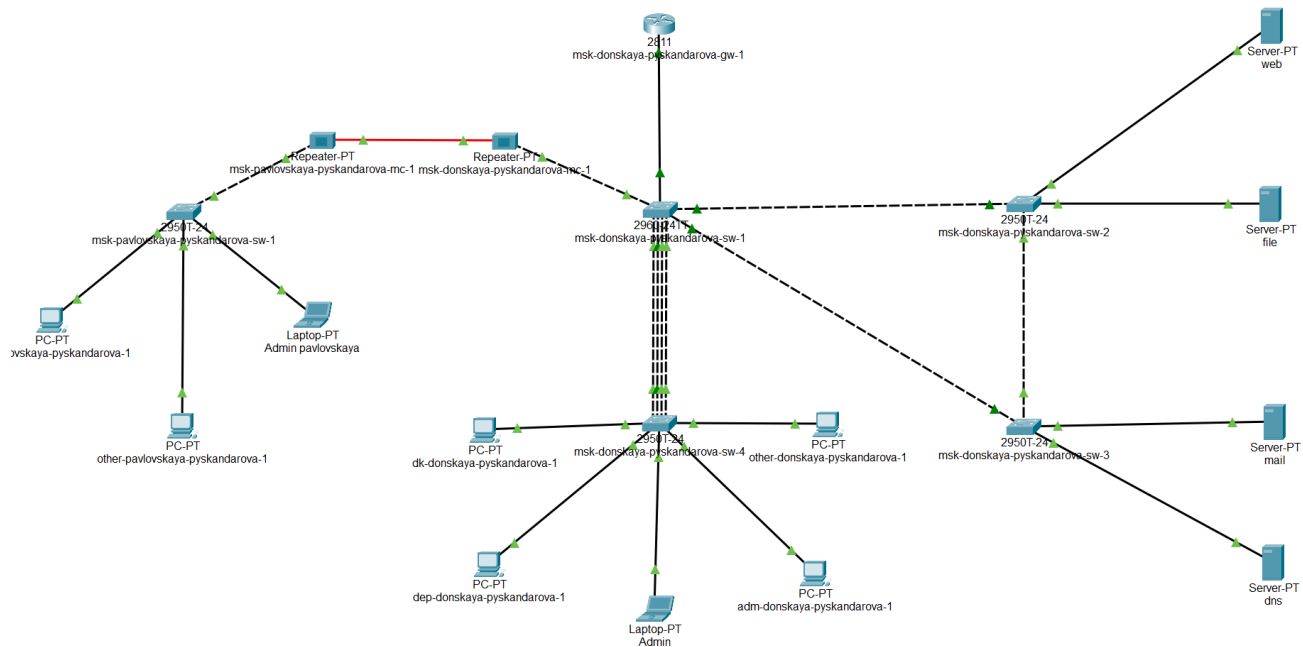
Цель работы.....	1
Выполнение лабораторной работы.....	1
Самостоятельная работа.....	9
Выводы.....	14

Цель работы

Освоить настройку прав доступа пользователей к ресурсам сети.

Выполнение лабораторной работы

В рабочей области проекта подключаю ноутбук администратора с именем admin к сети к other-donskaya-1 с тем, чтобы разрешить ему потом любые действия, связанные с управлением сетью. (рис. [-@fig:001]) Для этого подсоединяю ноутбук к порту 24 коммутатора msk-donskaya-sw-4 и присваиваю 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. [-@fig:002], рис. [-@fig:003]). Права доступа пользователей сети буду настраивать на маршрутизаторе msk-donskaya-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.



Рабочая область проекта с добавленными ноутбуками администраторов

Admin

PhysicalConfigDesktopProgrammingAttributes

GLOBAL

Settings

Algorithm Settings

INTERFACE

FastEthernet0

Bluetooth

Global Settings

Display NameAdmin

InterfacesFastEthernet0

Gateway/DNS IPv4

DHCP

Static

Default Gateway10.128.6.1

DNS Server10.128.0.5

Gateway/DNS IPv6

Automatic

Static

Default Gateway

DNS Server

Top

Добавленные DNS и gateway адреса

The screenshot shows the Cisco IOS configuration interface for the FastEthernet0 interface. The left sidebar contains a tree view with 'GLOBAL' and 'INTERFACE' sections. Under 'INTERFACE', 'FastEthernet0' is selected. The main configuration area for FastEthernet0 includes the following settings:

- Port Status:** ☒ On
- Bandwidth:** 100 Mbps (selected), 10 Mbps
- Duplex:** Half Duplex, Full Duplex (selected)
- MAC Address:** 0001.421A.4BCD
- IP Configuration:** DHCP, Static (selected)
- IPv4 Address:** 10.128.6.200
- Subnet Mask:** 255.255.255.0
- IPv6 Configuration:** Automatic, Static (selected)
- IPv6 Address:** (empty field)
- Link Local Address:** FE80::201:42FF:FE1A:4BCD

At the bottom left, there is a 'Top' button.

Добавленный статический IP-адрес

Следует помнить, что 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 я сначала даю разрешение (permit) на какое-то действие, а уже потом накладываю ограничения (deny). Кроме того, после всех правил в конце можно дописать неявное запрещение на всё, что не разрешено: deny ip any any (implicit deny).

Настройка доступа к web-серверу по порту tcp 80: msk -donskaya -gw -1# configure terminal msk -donskaya -gw -1(config)#ip access -list extended servers -out msk -donskaya -gw -1(config -ext -nacl)# remark web msk -donskaya -gw -1(config -ext -nacl)# permit tcp any host 10.128.0.2 eq 80 Здесь: создан 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; дано 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. Добавление списка управления доступом к интерфейсу: msk -donskaya -gw -1# configure terminal msk -donskaya -gw -1(config)# interface f0 /0.3 msk -donskaya -gw -1(config -subif)#ip access -group servers -out out Здесь: к интерфейсу f0/0.3 подключается список прав доступа servers-out и применяется к исходящему трафику (out). Можно проверить, 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.

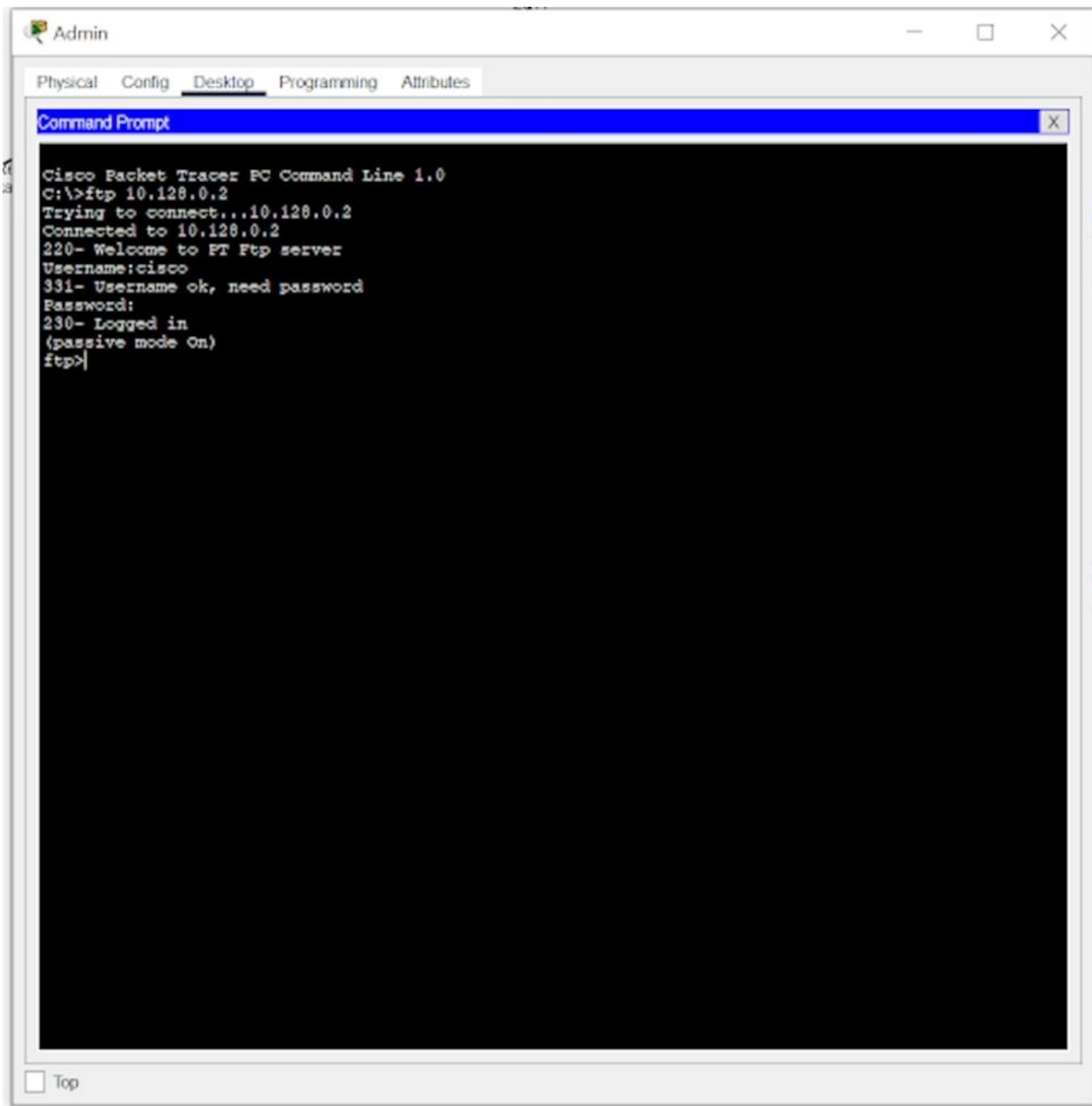
Дополнительный доступ для администратора по протоколам Telnet и FTP: msk -donskaya -gw -1# configure terminal msk -donskaya -gw -1(config)#ip access -list extended servers -out msk -donskaya -gw -1(config -ext -nacl)# permit tcp host 10.128.6.200 host 10.128.0.2 range 20 ftp msk -donskaya -gw -1(config -ext -nacl)# permit tcp host 10.128.6.200 host 10.128.0.2 eq telnet Здесь: 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. (рис. [-@fig:004])

Создание списка контроля доступа с названием servers-out, подключение список прав доступа servers-out к интерфейсу f0/0.3 и применение к исходящему трафику (out), добавление правила, разрешающего устройству администратора с ip-адресом 10.128.6.200 доступ на web-сервер (10.128.0.2) по протоколам FTP и telnet, в список контроля доступа servers-out

```
msk-donskaya-pyskandarova-gw-1(config)#ip access-list extended servers-out
msk-donskaya-pyskandarova-gw-1(config-ext-nacl)#remark web
msk-donskaya-pyskandarova-gw-1(config-ext-nacl)#permit tcp any host 10.128.0.2 eq 80
msk-donskaya-pyskandarova-gw-1(config-ext-nacl)#exit
msk-donskaya-pyskandarova-gw-1(config)#interface f0/0.3
msk-donskaya-pyskandarova-gw-1(config-subif)#ip access-group servers-out out
msk-donskaya-pyskandarova-gw-1(config-subif)#exit
msk-donskaya-pyskandarova-gw-1(config)#ip access-list extended servers-out
msk-donskaya-pyskandarova-gw-1(config-ext-nacl)#permit tcp host 10.128.6.200 host 10.128.0.2
range 20 ftp
msk-donskaya-pyskandarova-gw-1(config-ext-nacl)#permit tcp host 10.128.6.200 host 10.128.0.2 eq
telnet
```

Создание списка контроля доступа с названием servers-out, подключение список прав доступа servers-out к интерфейсу f0/0.3 и применение к исходящему трафику (out), добавление правила, разрешающего устройству администратора с ip-адресом 10.128.6.200 доступ на web-сервер (10.128.0.2) по протоколам FTP и telnet, в список контроля доступа servers-out

Убеждаюсь, что с узла с ip-адресом 10.128.6.200 есть доступ по протоколу FTP. Для этого в командной строке устройства администратора ввожу ftp 10.128.0.2, а затем по запросу имя пользователя cisco и пароль cisco (рис. [-@fig:005]).



Проверка доступа к web-серверу по протоколу FTP с устройства администратора

Настройка доступа к файловому серверу: msk -donskaya -gw -1# configure terminal msk -donskaya -gw -1(config)#ip access -list extended servers -out msk -donskaya -gw -1(config -ext -nacl)# remark file msk -donskaya -gw -1(config -ext -nacl)# permit tcp 10.128.0.0 0.0.255.255 host 10.128.0.3 eq 445 msk -donskaya -gw -1(config -ext -nacl)# permit tcp any host 10.128.0.3 range 20 ftp Здесь: 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). Настройка доступа к почтовому серверу: msk-donskaya-gw-1# configure terminal msk-donskaya-gw-1(config)#ip access-list extended servers-out msk-donskaya-gw-1(config-ext-nacl)# remark mail msk-donskaya-gw-1(config-ext-nacl)# permit tcp any host 10.128.0.4 eq smtp msk-donskaya-gw-1(config-ext-nacl)# permit tcp any host 10.128.0.4 eq pop3 Здесь: 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. Настройка доступа к DNS-серверу: msk-donskaya-gw-1# configure terminal msk-donskaya-gw-1(config)#ip access-list extended servers-out msk-donskaya-gw-1(config-ext-nacl)# remark dns msk-donskaya-gw-1(config-ext-nacl)# permit udp 10.128.0.0 0.0.255.255 host 10.128.0.5 eq 53 Здесь: 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. Проверьте доступность web-сервера (через браузер) не только по ip-адресу, но и по имени. Разрешение icmp-запросов: msk-donskaya-gw-1# configure terminal msk-donskaya-gw-1(config)#ip access-list extended servers-out msk-donskaya-gw-1(config-ext-nacl)#1 permit icmp any any Здесь демонстрируется явное управление порядком размещения правил — правило разрешения для icmp-запросов добавляется в начало списка контроля доступа (рис. [-@fig:006]).

```
msk-donskaya-pyskandarova-gw-1(config-ext-nacl)#exit
msk-donskaya-pyskandarova-gw-1(config)#ip access-list extended servers-out
msk-donskaya-pyskandarova-gw-1(config-ext-nacl)#remark file
msk-donskaya-pyskandarova-gw-1(config-ext-nacl)#permit tcp 10.128.0.0.0.0.255.255 host
10.128.0.3 eq 445
^
% Invalid input detected at '^' marker.

msk-donskaya-pyskandarova-gw-1(config-ext-nacl)#permit tcp 10.128.0.0.0.0.255.255 host
10.128.0.3 eq 445
^
% Invalid input detected at '^' marker.

msk-donskaya-pyskandarova-gw-1(config-ext-nacl)#permit tcp 10.128.0.0 0.0.255.255
% Incomplete command.
msk-donskaya-pyskandarova-gw-1(config-ext-nacl)# host 10.128.0.3 eq 445
^
% Invalid input detected at '^' marker.

msk-donskaya-pyskandarova-gw-1(config-ext-nacl)#permit tcp 10.128.0.0 0.0.255.255 host
10.128.0.3 eq 445
msk-donskaya-pyskandarova-gw-1(config-ext-nacl)#permit tcp any host 10.128.0.3 range 20 ftp
msk-donskaya-pyskandarova-gw-1(config-ext-nacl)#remark mail
msk-donskaya-pyskandarova-gw-1(config-ext-nacl)#permit tcp any host 10.128.0.4 eq smtp
msk-donskaya-pyskandarova-gw-1(config-ext-nacl)#permit tcp any host 10.128.0.4 eq pop3
msk-donskaya-pyskandarova-gw-1(config-ext-nacl)#remark dns
msk-donskaya-pyskandarova-gw-1(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-pyskandarova-gw-1(config-ext-nacl)#permit udp 10.128.0.0 0.0.255.255 host
10.128.0.5 eq 53
msk-donskaya-pyskandarova-gw-1(config-ext-nacl)#1 permit icmp any any
msk-donskaya-pyskandarova-gw-1(config-ext-nacl)#exit
msk-donskaya-pyskandarova-gw-1#
```

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, всем разрешён доступ к почтовому серверу по протоколам POP3 и SMTP, правило разрешения для istr-запросов добавлено в начало списка контроля доступа

Номера строк правил в списке контроля доступа можно посмотреть с помощью команды `msk-donskaya-gw-1# show access-lists` (рис. [-@fig:007])

```
msk-donskaya-pyskandarova-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
20 permit tcp host 10.128.6.200 host 10.128.0.2 range 20 ftp (8 match(es))
30 permit tcp host 109.128.6.200 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
```

Применение команды `msk-donskaya-gw-1# show access-lists`

Настройка 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): `msk-donskaya-gw-1# configure terminal` `msk-donskaya-gw-1(config)#ip access-list extended other` `msk-donskaya-gw-1(config-ext -nacl)# remark admin` `msk-donskaya-gw-1(config-ext -nacl)# permit ip host 10.128.6.200 any` `msk-donskaya-gw-1(config-ext -nacl)#exit` `msk-donskaya-gw-1(config-subif)# interface f0 /0.104` `msk-donskaya-gw-1(config-subif)#ip access-group other in` Здесь: 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`). Настройка доступа администратора к сети сетевого оборудования: `msk-donskaya-gw-1# configure terminal` `msk-donskaya-gw-1(config)#ip access-list extended management-out` `msk-donskaya-gw-1(config-ext -nacl)# remark admin` `msk-donskaya-gw-1(config-ext -nacl)# permit ip host 10.128.6.200 10.128.1.0 0.0.0.255` `msk-donskaya-gw-1(config-ext -nacl)#exit` `msk-donskaya-gw-1(config)# interface f0 /0.2` `msk-donskaya-gw-1(config-subif)#ip access-group management-out out` Здесь: 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`) (рис. [-@fig:008]).


```

msk-donskaya-pyskandarova-gw-1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
msk-donskaya-pyskandarova-gw-1(config)#ip access-list extended other-in
msk-donskaya-pyskandarova-gw-1(config-ext-nacl)#remark admin
msk-donskaya-pyskandarova-gw-1(config-ext-nacl)#permit ip host 10.128.6.200 any
msk-donskaya-pyskandarova-gw-1(config-ext-nacl)#exit
msk-donskaya-pyskandarova-gw-1(config)#interface f0/0.104
msk-donskaya-pyskandarova-gw-1(config-subif)#ip access-group other-in in
msk-donskaya-pyskandarova-gw-1(config-subif)#remark admin
^
% Invalid input detected at '^' marker.

msk-donskaya-pyskandarova-gw-1(config-subif)#exit
msk-donskaya-pyskandarova-gw-1(config)#remark admin
^
% Invalid input detected at '^' marker.

msk-donskaya-pyskandarova-gw-1(config)#ip access-list extended management-out
msk-donskaya-pyskandarova-gw-1(config-ext-nacl)#remark admin
msk-donskaya-pyskandarova-gw-1(config-ext-nacl)#permit ip host 10.128.6.200 10.128.1.0.0.0.255
^
% Invalid input detected at '^' marker.

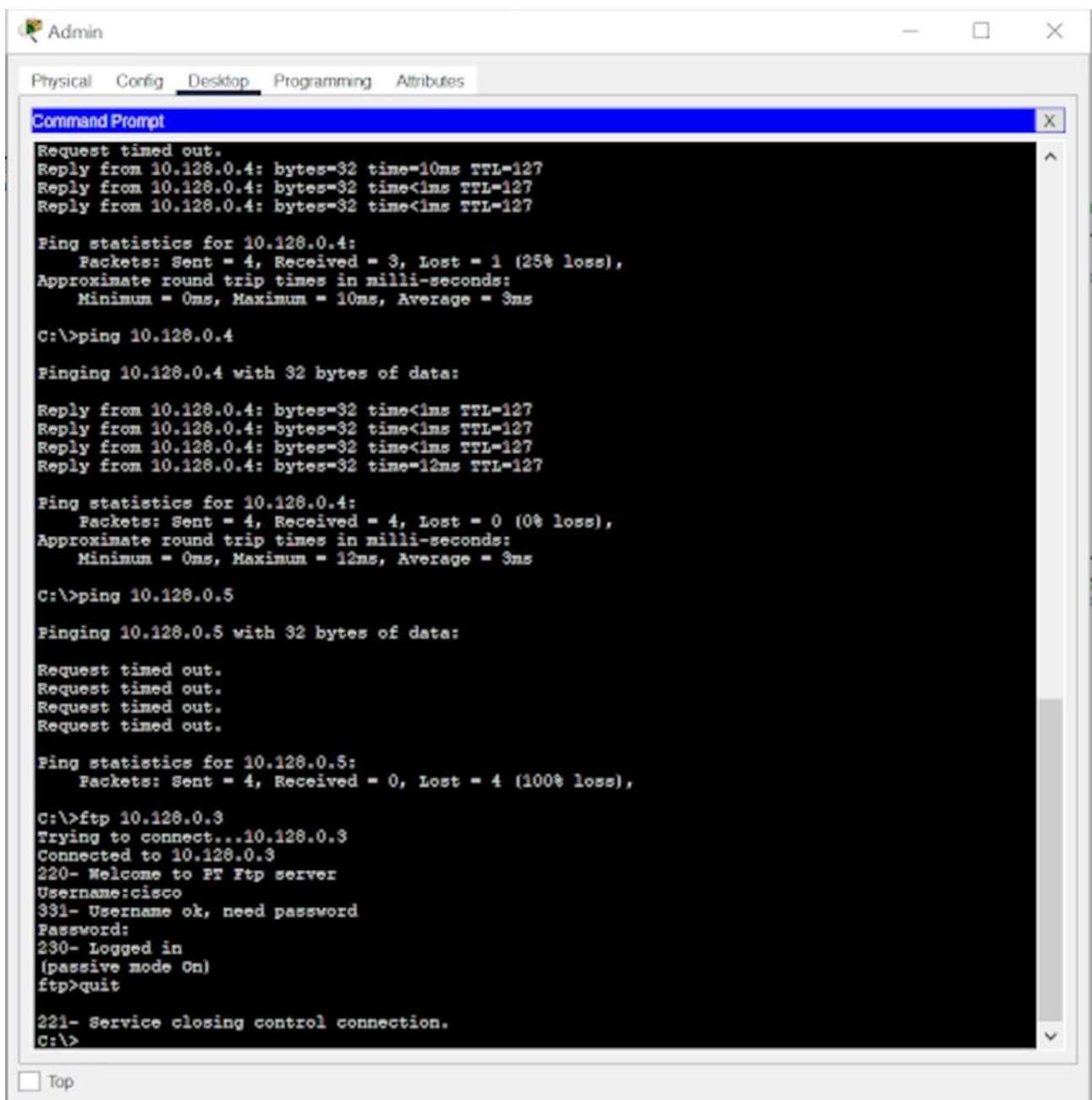
msk-donskaya-pyskandarova-gw-1(config-ext-nacl)#permit ip host 10.128.6.200 10.128.1.0 0.0.0.255
msk-donskaya-pyskandarova-gw-1(config-ext-nacl)#exit
msk-donskaya-pyskandarova-gw-1(config)#interface f0/0.2
msk-donskaya-pyskandarova-gw-1(config-subif)#ip access-group management-out out

```

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), 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)

Самостоятельная работа

Проверяю корректность установленных правил доступа, попытавшись получить доступ по различным протоколам с разных устройств сети к подсети серверов и подсети сетевого оборудования (рис. [-@fig:009]).



The screenshot shows a desktop environment with a window titled "Admin" containing tabs for "Physical", "Config", "Desktop", "Programming", and "Attributes". The "Desktop" tab is active, displaying a "Command Prompt" window. The command prompt shows the following sequence of commands and outputs:

```
Request timed out.
Reply from 10.128.0.4: bytes=32 time=10ms TTL=127
Reply from 10.128.0.4: bytes=32 time<1ms TTL=127
Reply from 10.128.0.4: bytes=32 time<1ms TTL=127

Ping statistics for 10.128.0.4:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 10ms, Average = 3ms

C:\>ping 10.128.0.4

Pinging 10.128.0.4 with 32 bytes of data:

Reply from 10.128.0.4: bytes=32 time<1ms TTL=127
Reply from 10.128.0.4: bytes=32 time<1ms TTL=127
Reply from 10.128.0.4: bytes=32 time<1ms TTL=127
Reply from 10.128.0.4: bytes=32 time=12ms TTL=127

Ping statistics for 10.128.0.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 12ms, Average = 3ms

C:\>ping 10.128.0.5

Pinging 10.128.0.5 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

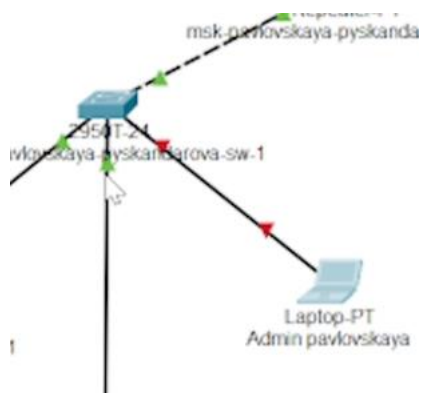
Ping statistics for 10.128.0.5:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ftp 10.128.0.3
Trying to connect...10.128.0.3
Connected to 10.128.0.3
220- Welcome to FT Ftp server
Username:cisco
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>quit
221- Service closing control connection.
C:\>
```

At the bottom left of the window, there is a checkbox labeled "Top" which is currently unchecked.

Проверка доступа к разным серверам с устройства администратора

Разрешите администратору из сети Other на Павловской действия, аналогичные действиям администратора сети Other на Донской. При дополнении схемы ноутбуком администратора на Павловской у меня сначала произошли трудности с соединением, но я исправила их, перенесла ноутбук с Донской, где он сначала появился, на Павловскую (рис. [-@fig:010], рис. [-@fig:011]). Далее повторила шаги работы, связанные с IP ноутбука, т.к. он отличается от ноутбука на Донской (рис. [-@fig:012], рис. [-@fig:013], рис. [-@fig:014], рис. [-@fig:015])



Проблемы с доступом у ноутбука



Исправление проблем с доступом

Admin pavlovskaya

Physical Config Desktop Programming Attributes

GLOBAL

Settings

Algorithm Settings

INTERFACE

FastEthernet0

Bluetooth

Global Settings

Display Name: Admin pavlovskaya

Interfaces: FastEthernet0

Gateway/DNS IPv4

☐ DHCP

☒ Static

Default Gateway: 10.128.6.1

DNS Server: 10.128.0.5

Gateway/DNS IPv6

☐ Automatic

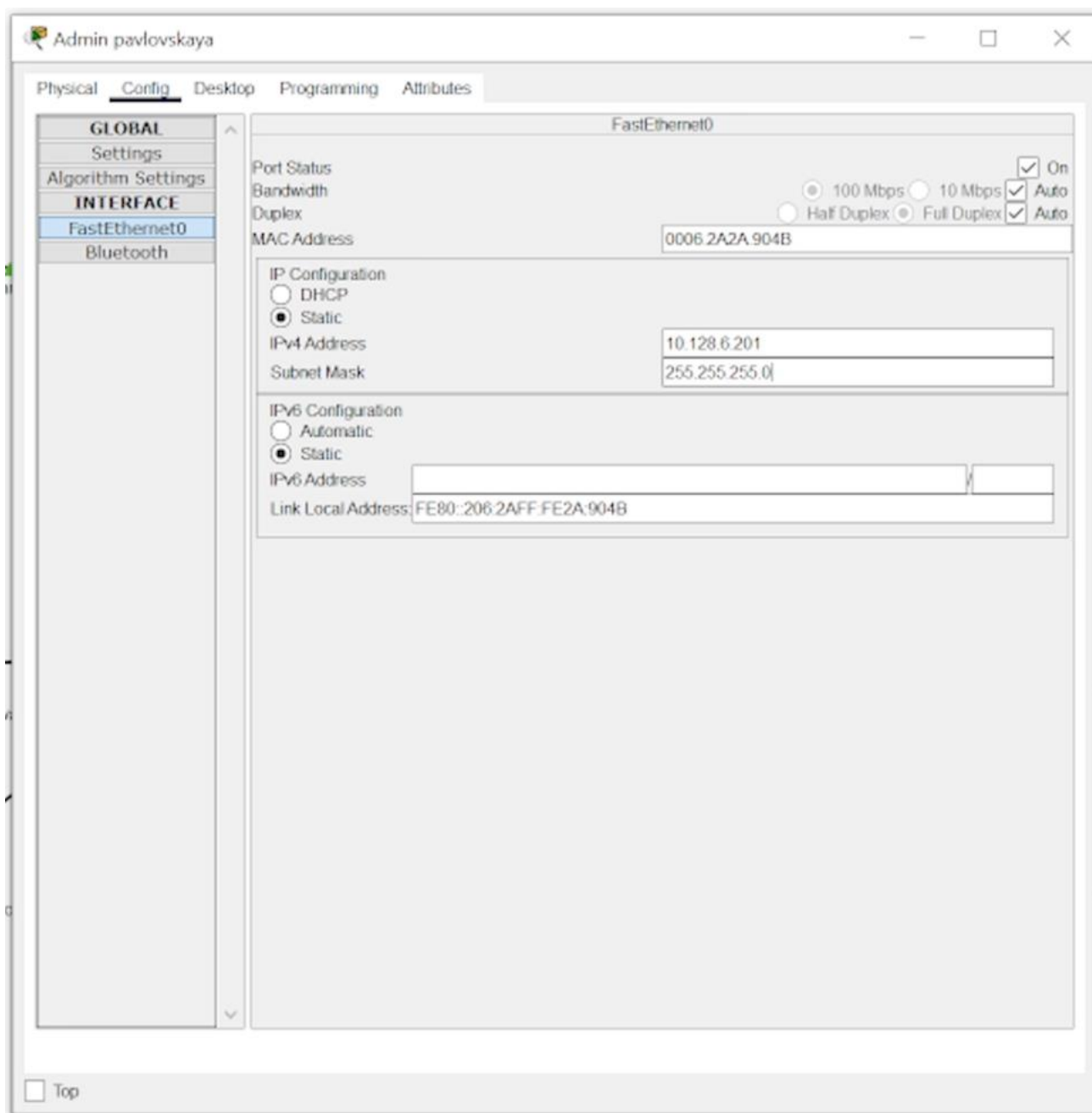
☒ Static

Default Gateway:

DNS Server:

☐ Top

Добавленные DNS и gateway адреса



Добавленный статический IP-адрес

```

msk-donskaya-pyskandarova-gw-1(config)#ip access-list extended other-in
msk-donskaya-pyskandarova-gw-1(config-ext-nacl)#remark admin pavlovskaya
msk-donskaya-pyskandarova-gw-1(config-ext-nacl)#permit ip host 10.128.6.201 any
msk-donskaya-pyskandarova-gw-1(config-ext-nacl)#exit
msk-donskaya-pyskandarova-gw-1(config)#interface f0/0.104
msk-donskaya-pyskandarova-gw-1(config-subif)#ip access group other in in
^
% Invalid input detected at '^' marker.

msk-donskaya-pyskandarova-gw-1(config-subif)#ip access-group other-in in
msk-donskaya-pyskandarova-gw-1(config-subif)#exit
msk-donskaya-pyskandarova-gw-1(config)#ip access list extended management out
^
% Invalid input detected at '^' marker.

msk-donskaya-pyskandarova-gw-1(config)#ip access-list extended management-out
msk-donskaya-pyskandarova-gw-1(config-ext-nacl)#remark admin
msk-donskaya-pyskandarova-gw-1(config-ext-nacl)#permit ip host 10.128.6.201
% Incomplete command.
msk-donskaya-pyskandarova-gw-1(config-ext-nacl)#permit ip host 10.128.6.201 10.128.1.0 0.0.0.255
msk-donskaya-pyskandarova-gw-1(config-ext-nacl)#exit
msk-donskaya-pyskandarova-gw-1(config)#interface f0/0.2
msk-donskaya-pyskandarova-gw-1(config-subif)#ip access-group management-out out
msk-donskaya-pyskandarova-gw-1(config-subif)#exit
msk-donskaya-pyskandarova-gw-1(config)#exit

```

Настройка разрешений для ноутбука администратора на Павловской

```

msk-donskaya-pyskandarova-gw-1#show access-list
Extended IP access list servers-out
 1 permit icmp any any (28 match(es))
10 permit tcp any host 10.128.0.2 eq www
20 permit tcp host 10.128.6.200 host 10.128.0.2 range 20 ftp (11 match(es))
30 permit tcp host 109.128.6.200 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 (10 match(es))
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
90 permit tcp host 10.128.6.201 host 10.128.0.2 range 20 ftp
100 permit tcp host 10.128.6.201 host 10.128.0.2 eq telnet
110 permit ip host 10.128.6.201 any
120 permit ip host 10.128.6.201 10.128.0.0 0.0.0.255
Extended IP access list other-in
 10 permit ip host 10.128.6.200 any (65 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

```

Проверка списка разрешений

Выводы

Освоена настройка прав доступа пользователей к ресурсам сети.