Лабораторная работа № 10

Настройка списков управления доступом (ACL)

Джахангиров Илгар Залид оглы

Содержание

Список иллюстраций

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 к other-donskaya-1 (рис. **??**) 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. **??**), указав в качестве gateway-адреса 10.128.6.1 и адреса DNS-сервера 10.128.0.5 (рис. **??**).

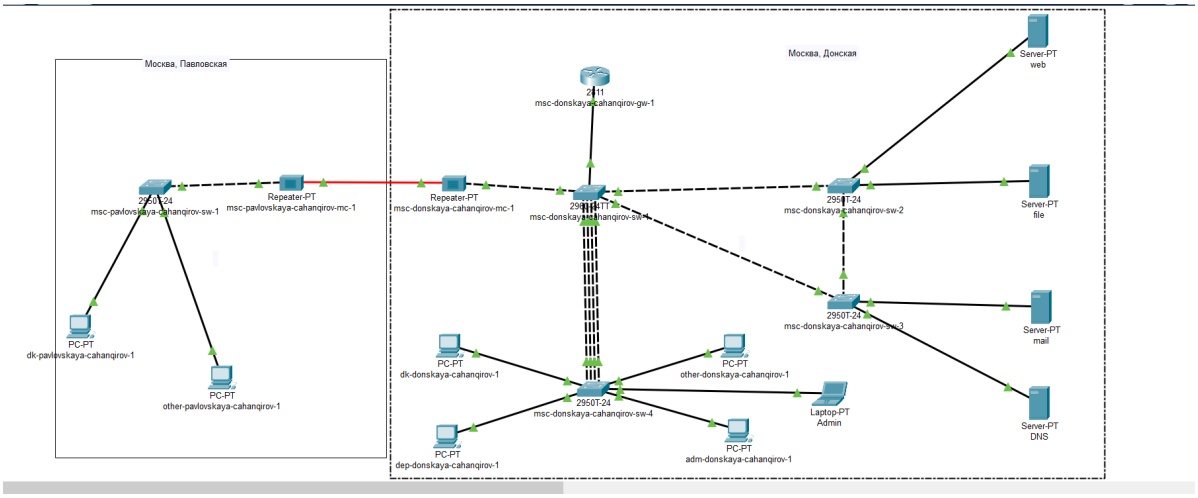

Рис. 3.1: Размещение ноутбука администратора в сети other-donskaya-1

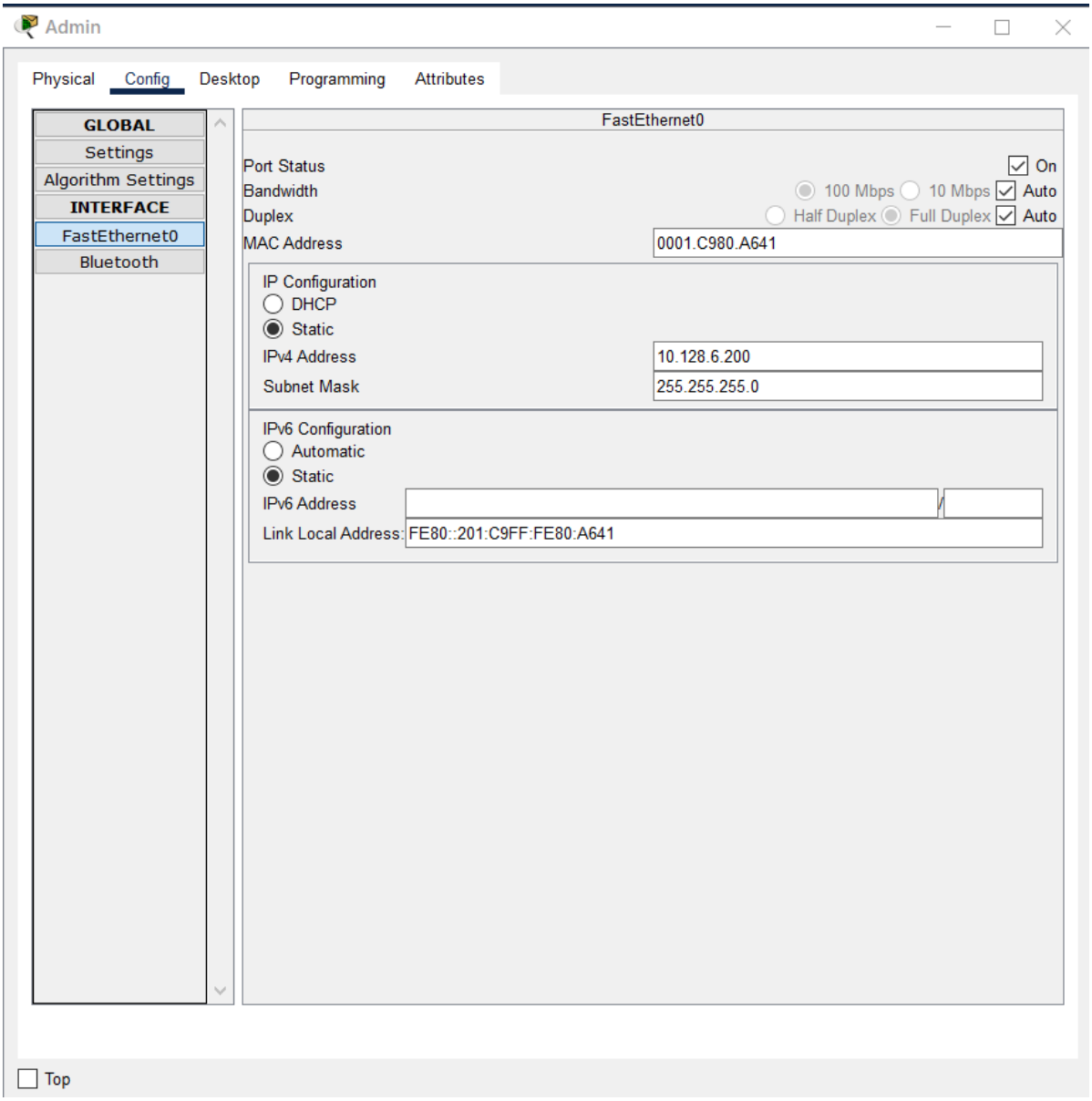

Рис. 3.2: Задание статического ip-адреса ноутбуку admin

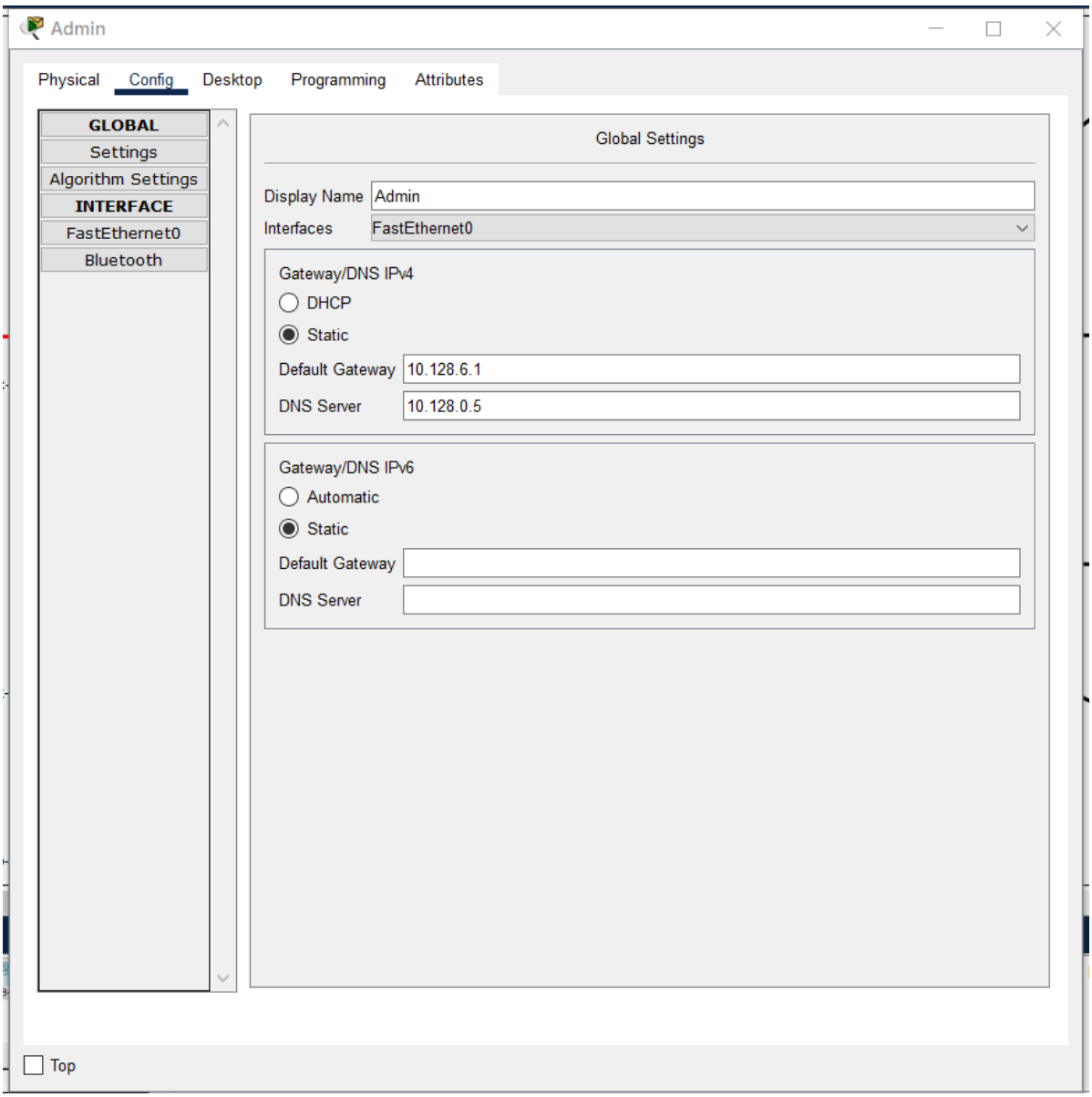

Рис. 3.3: Задание gateway-адреса и адреса DNS-сервера ноутбуку admin

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

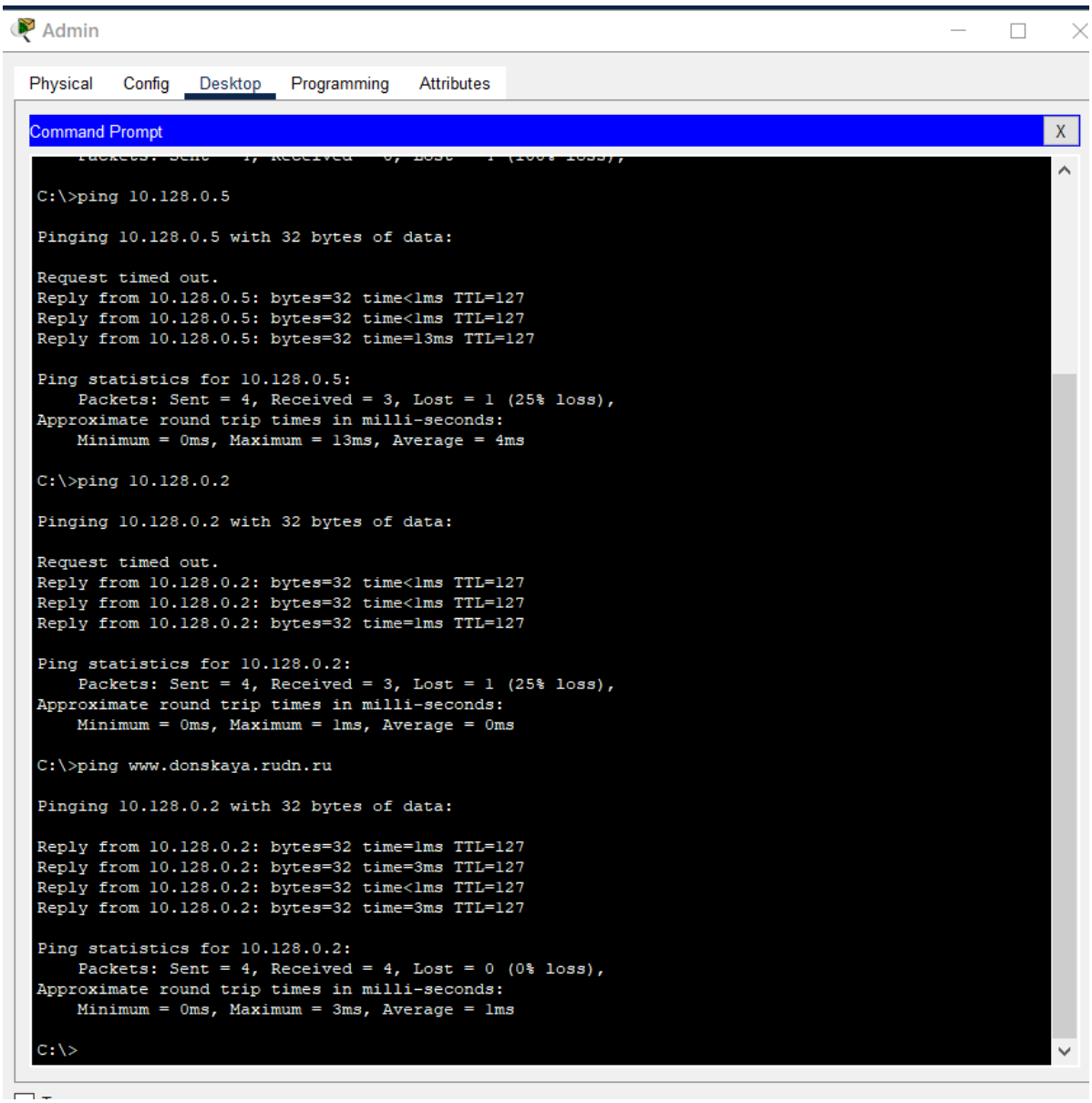

Рис. 3.4: Проверка работоспособности соединения ноутбука admin

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).

Настроем доступ к web-серверу по порту tcp 80 (рис.**??**). 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.

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

msc-donskaya-cahanqirov-gw-1(config)#ip access-list extended servers-out
msc-donskaya-cahanqirov-gw-1(config-ext-nacl)#remark web
msc-donskaya-cahanqirov-gw-1(config-ext-nacl)#permit tcp any host 10.128.0.2 eq 80
msc-donskaya-cahanqirov-gw-1(config-ext-nacl)#^Z
msc-donskaya-cahanqirov-gw-1#
%SYS-5-CONFIG_I: Configured from console by console

msc-donskaya-cahanqirov-gw-1#wr m
Building configuration...
[OK]
msc-donskaya-cahanqirov-gw-1#
```

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

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

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

msc-donskaya-cahanqirov-gw-1#wr m
Building configuration...
[OK]
msc-donskaya-cahanqirov-gw-1#
```

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.**??**). При этом команда ping будет

демонстрировать недоступность web-сервера как по имени, так и по ip-адресу web-сервера (рис.**??**).

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

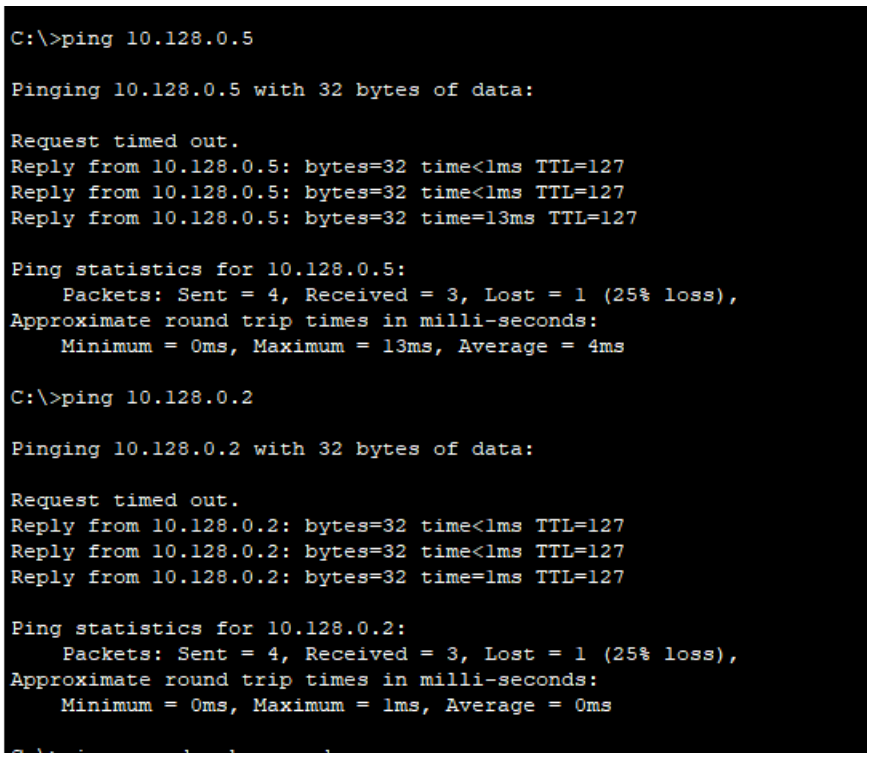

Рис. 3.8: Проверка недоступности web-сервера через ping

Настроем дополнительный доступ для администратора по протоколам Telnet и FTP (рис.**??**). 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.

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

msc-donskaya-cahanqirov-gw-1#wr m
Building configuration...
[OK]
msc-donskaya-cahanqirov-gw-1#
```

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.**??**). 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.

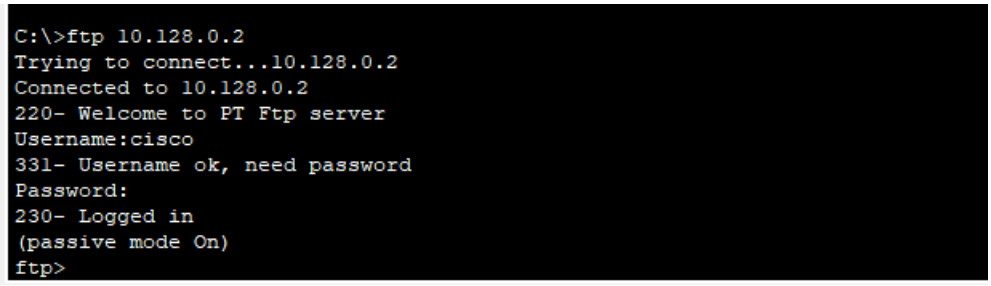

Рис. 3.10: Проверка работы ftp у администратора

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

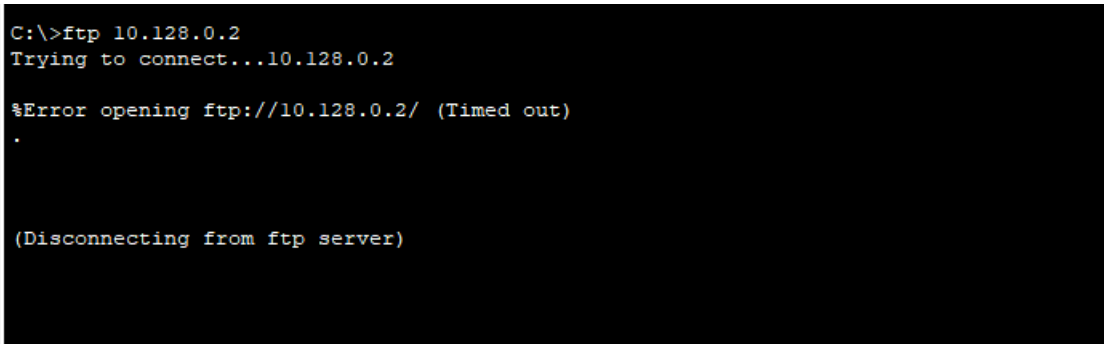

Рис. 3.11: Проверка недоступности подключения по ftp у просто пользователя

Настроем доступ к файловому серверу (рис.**??**). 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).

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

msc-donskaya-cahanqirov-gw-1#wr m
Building configuration...
[OK]
msc-donskaya-cahanqirov-gw-1#
```

Рис. 3.12: Настройка доступа к файловому серверу

Настроем доступ к почтовому серверу (рис.**??**). 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.

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

msc-donskaya-cahanqirov-gw-1#wr m
Building configuration...
[OK]
```

Рис. 3.13: Настройка доступа к почтовому серверу

Настроем доступ к DNS-серверу (рис.**??**). 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.

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

msc-donskaya-cahanqirov-gw-1#wr m
Building configuration...
[OK]
msc-donskaya-cahanqirov-gw-1#
```

Рис. 3.14: Настройка доступа к DNS-серверу

Разрешим icmp-запросы (рис.**??**).

```
msc-donskaya-cahanqirov-gw-1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
msc-donskaya-cahanqirov-gw-1(config)#ip access-list extended servers-out
msc-donskaya-cahanqirov-gw-1(config-ext-nacl)#1 permit icmp any an
msc-donskaya-cahanqirov-gw-1(config-ext-nacl)#^Z
msc-donskaya-cahanqirov-gw-1#
%SYS-5-CONFIG_I: Configured from console by console

msc-donskaya-cahanqirov-gw-1#wr m
Building configuration...
[OK]
msc-donskaya-cahanqirov-gw-1#
```

Рис. 3.15: Разрешение icmp-запросов

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

```
msc-donskaya-cahanqirov-gw-1#show access-lists
Extended IP access list servers-out
    10 permit icmp any any (16 match(es))
    20 permit tcp 10.128.0.0 0.0.255.255 host 10.128.0.3 eq 445
    30 permit tcp any host 10.128.0.3 range 20 ftp
    40 permit tcp any host 10.128.0.4 eq smtp
    50 permit tcp any host 10.128.0.4 eq pop3
    60 permit udp 10.128.0.0 0.0.255.255 host 10.128.0.5 eq domain (2 match(es))
    70 permit tcp any host 10.128.0.2 eq www (10 match(es))
    80 permit tcp host 10.128.6.200 host 10.128.0.2 range 20 ftp (7 match(es))
    90 permit tcp host 10.128.6.200 host 10.128.0.2 eq telnet
    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
Extended IP access list other-in
    10 permit ip host 10.128.6.200 any (33 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
Extended IP access list servers-in
    10 permit ip host 10.128.6.200 any

msc-donskaya-cahanqirov-gw-1#
```

Рис. 3.16: Просмотр строк в списке контроля доступа

Настроем доступ для сети Other (рис.**??**). 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).

```
msc-donskaya-cahanqirov-gw-1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
msc-donskaya-cahanqirov-gw-1(config)#ip access-list extended other-in
msc-donskaya-cahanqirov-gw-1(config-ext-nacl)#remark admin
msc-donskaya-cahanqirov-gw-1(config-ext-nacl)#permit ip host 10.128.6.200 any
msc-donskaya-cahanqirov-gw-1(config-ext-nacl)#exit
msc-donskaya-cahanqirov-gw-1(config)#interface f0/0.104
msc-donskaya-cahanqirov-gw-1(config-subif)#ip access group other in in
                                                          ^
% Invalid input detected at '^' marker.

msc-donskaya-cahanqirov-gw-1(config-subif)#ip access group other in in
                                                          ^
% Invalid input detected at '^' marker.

msc-donskaya-cahanqirov-gw-1(config-subif)#ip access-group other-in in
msc-donskaya-cahanqirov-gw-1(config-subif)#^Z
msc-donskaya-cahanqirov-gw-1#
%SYS-5-CONFIG_I: Configured from console by console

msc-donskaya-cahanqirov-gw-1#wr m
Building configuration...
[OK]
msc-donskaya-cahanqirov-gw-1#
```

Рис. 3.17: Настройка доступа для сети Other

Настроем доступ администратора к сети сетевого оборудования (рис.**??**). 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).

```
msc-donskaya-cahanqirov-gw-1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
msc-donskaya-cahanqirov-gw-1(config)#ip access-list extended management-out
msc-donskaya-cahanqirov-gw-1(config-ext-nacl)#remark admin
msc-donskaya-cahanqirov-gw-1(config-ext-nacl)#permit ip host 10.128.6.200 10.128.1.0 0.0.0.255
msc-donskaya-cahanqirov-gw-1(config-ext-nacl)#exit
msc-donskaya-cahanqirov-gw-1(config)#interface f0/0.2
msc-donskaya-cahanqirov-gw-1(config-subif)#ip access-group management-out out
msc-donskaya-cahanqirov-gw-1(config-subif)#^Z
msc-donskaya-cahanqirov-gw-1#
%SYS-5-CONFIG_I: Configured from console by console

msc-donskaya-cahanqirov-gw-1#wr m
Building configuration...
[OK]
msc-donskaya-cahanqirov-gw-1#
```

Рис. 3.18: Настройка доступа администратора к сети сетевого оборудования

Проверим получившийся список контроля доступа (рис.**??**).

```
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
ip access-list extended servers-in
 remark admin
 permit ip host 10.128.6.200 any
ip access-list extended management-out
 remark admin
 permit ip host 10.128.6.200 10.128.1.0 0.0.0.255
!
.
```

Рис. 3.19: Список контроля доступа

4 Выводы

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