РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ

Факультет физико-математических и естественных наук

Кафедра прикладной информатики и теории вероятностей

ОТЧЕТ
ПО ЛАБОРАТОРНОЙ РАБОТЕ № 10

дисциплина: Администрирование локальных сетей

Студент: Шутенко Виктория Михайловна

Группа: НФИ-бд-03-19

МОСКВА

2022 г.

Цель работы:

Освоить настройку прав доступа пользователей к ресурсам сети.

10.2. Задание

1. Требуется настроить следующие правила доступа:

1) web-сервер: разрешить доступ всем пользователям по протоколу HTTP через порт 80 протокола TCP, а для администратора открыть доступ по протоколам Telnet и FTP;

2) файловый сервер: с внутренних адресов сети доступ открыт по портам для общедоступных каталогов, с внешних — доступ по протоколу FTP;

3) 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;

4) DNS-сервер: открыть порт 53 протокола UDP для доступа из внутренней сети;

5) разрешить icmp-сообщения, направленные в сеть серверов;

6) запретить для сети Other любые запросы за пределы сети, за исключением администратора;

7) 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 (см. раздел 2.5).

Последовательность выполнения работы

В рабочей области проекта подключила 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 подсоединила ноутбук к порту 24 коммутатора msk-donskaya-sw-4 и присвоила 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. 10.1).

Права доступа пользователей сети (см. рис. 9.2) настраивала на маршрутизаторе msk-donskaya-gw-1, поскольку именно через него проходит весь трафик сети. Ограничения можно было 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.

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 рекомендуется сначала дать разрешение (permit) на какое-то действие, а уже потом накладывать ограничения (deny). Кроме того, после всех правил в конце дописывается неявное запрещение на всё, что не разрешено: deny ip any any (implicit deny).

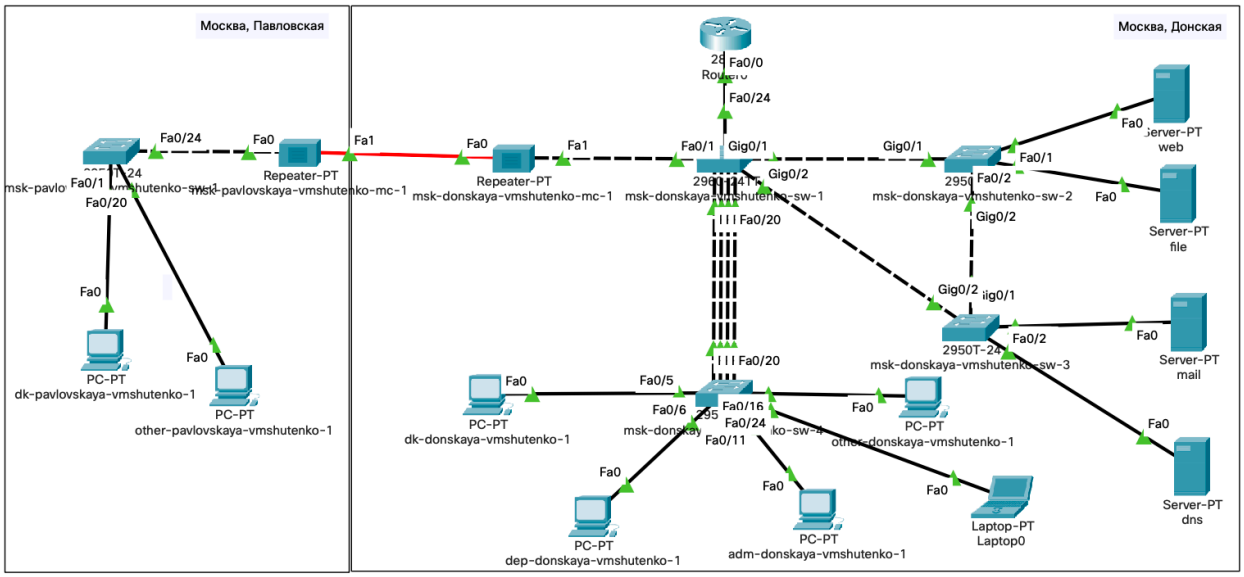

Рисунок 1. Схема сети

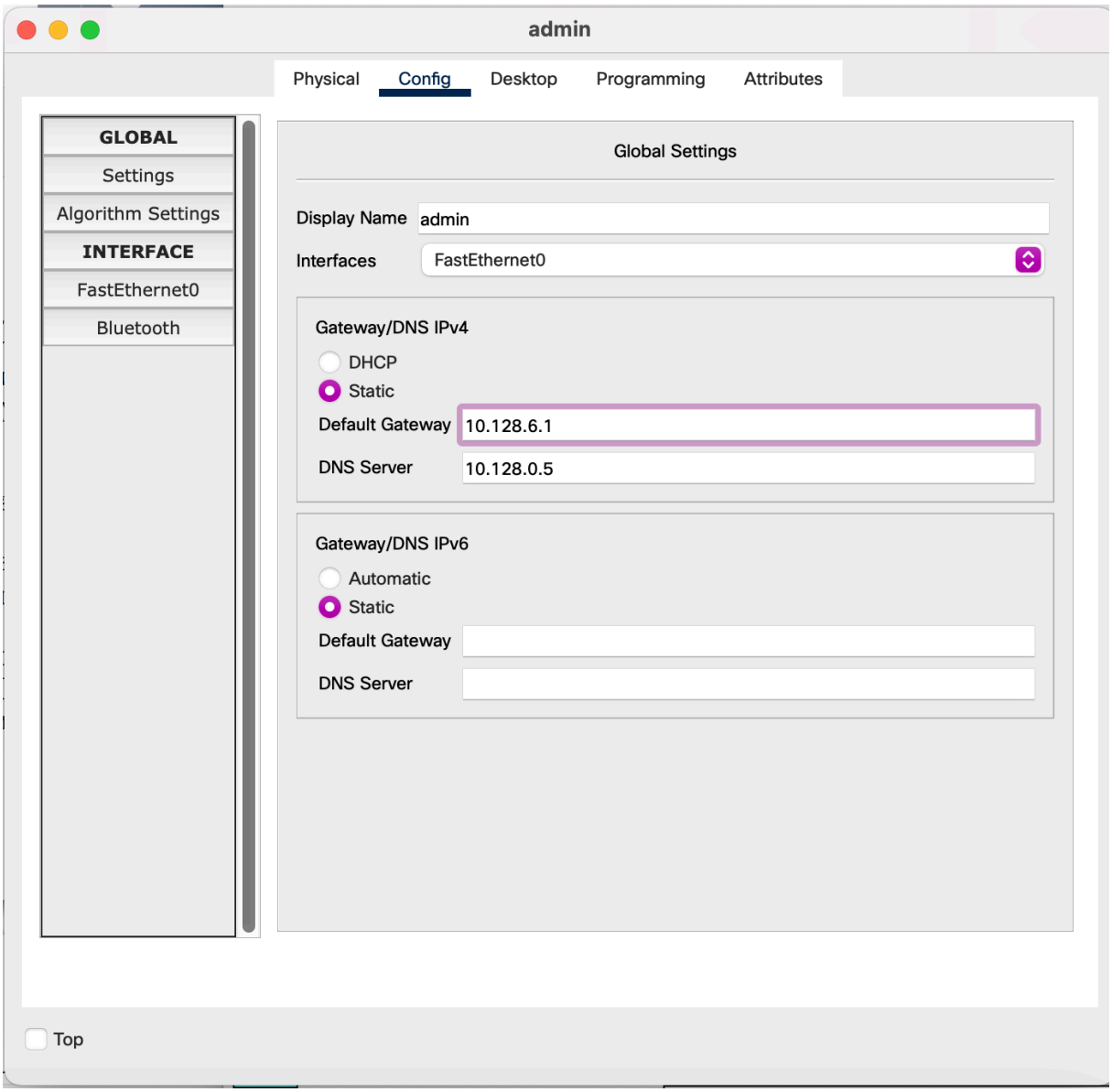

Рисунок 2. Задание gateway и dns.

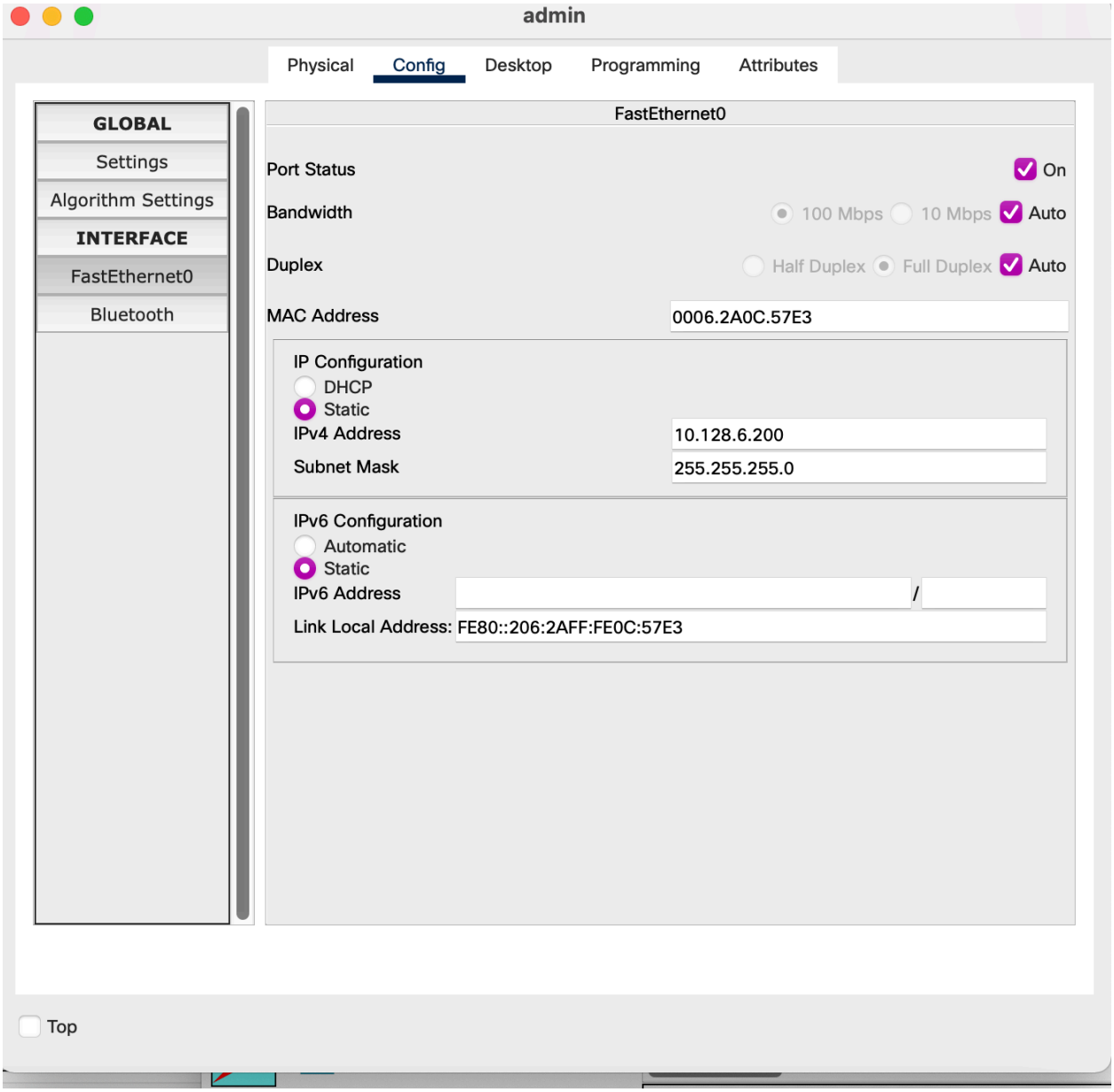

Рисунок 3. Задание статического адреса.

1. Настроила доступ 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.

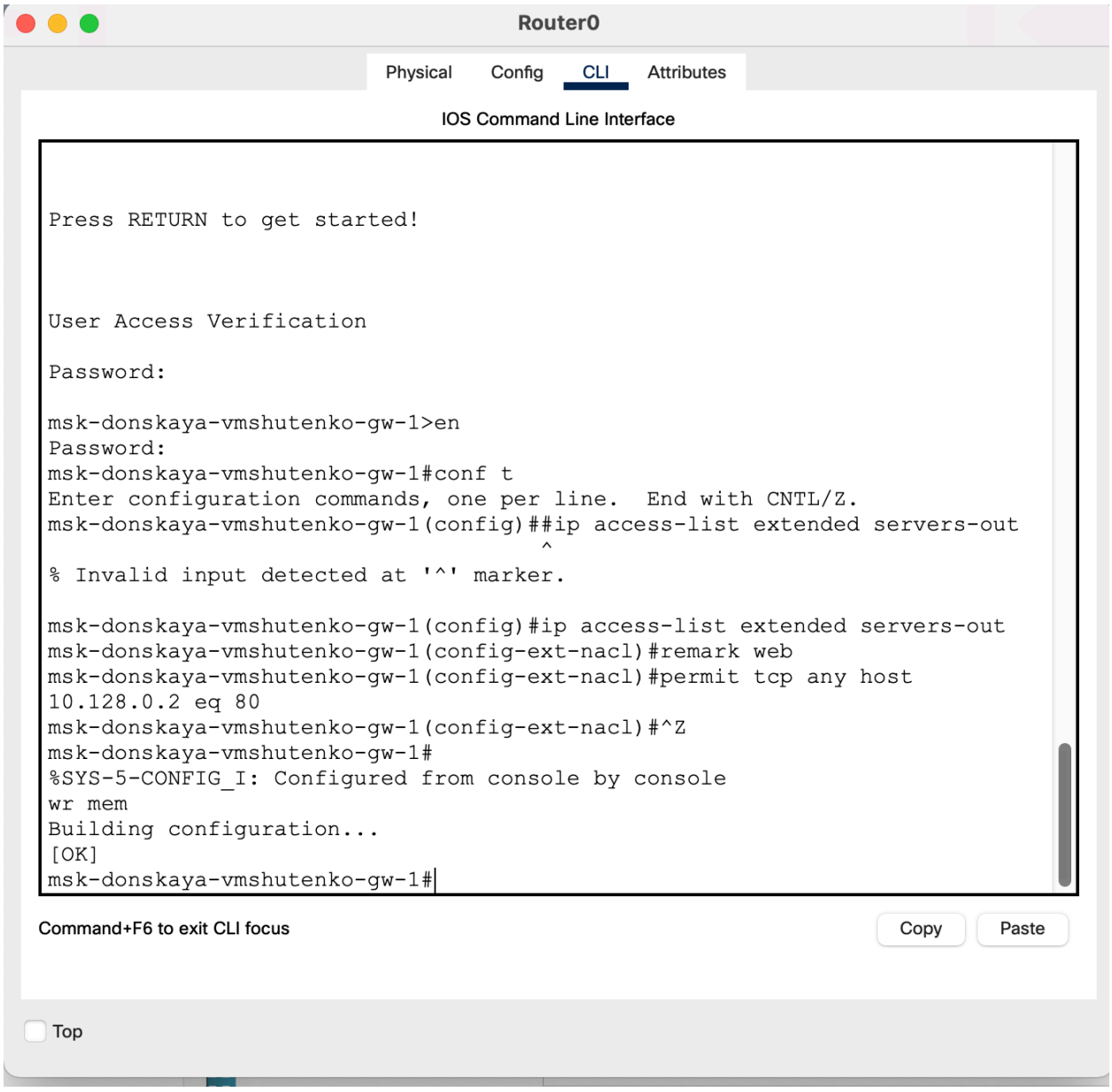

Рисунок 4. Настройка доступа к web-серверу по порту tcp 80.

2. Добавила список 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 serversout и применяется к исходящему трафику (out).

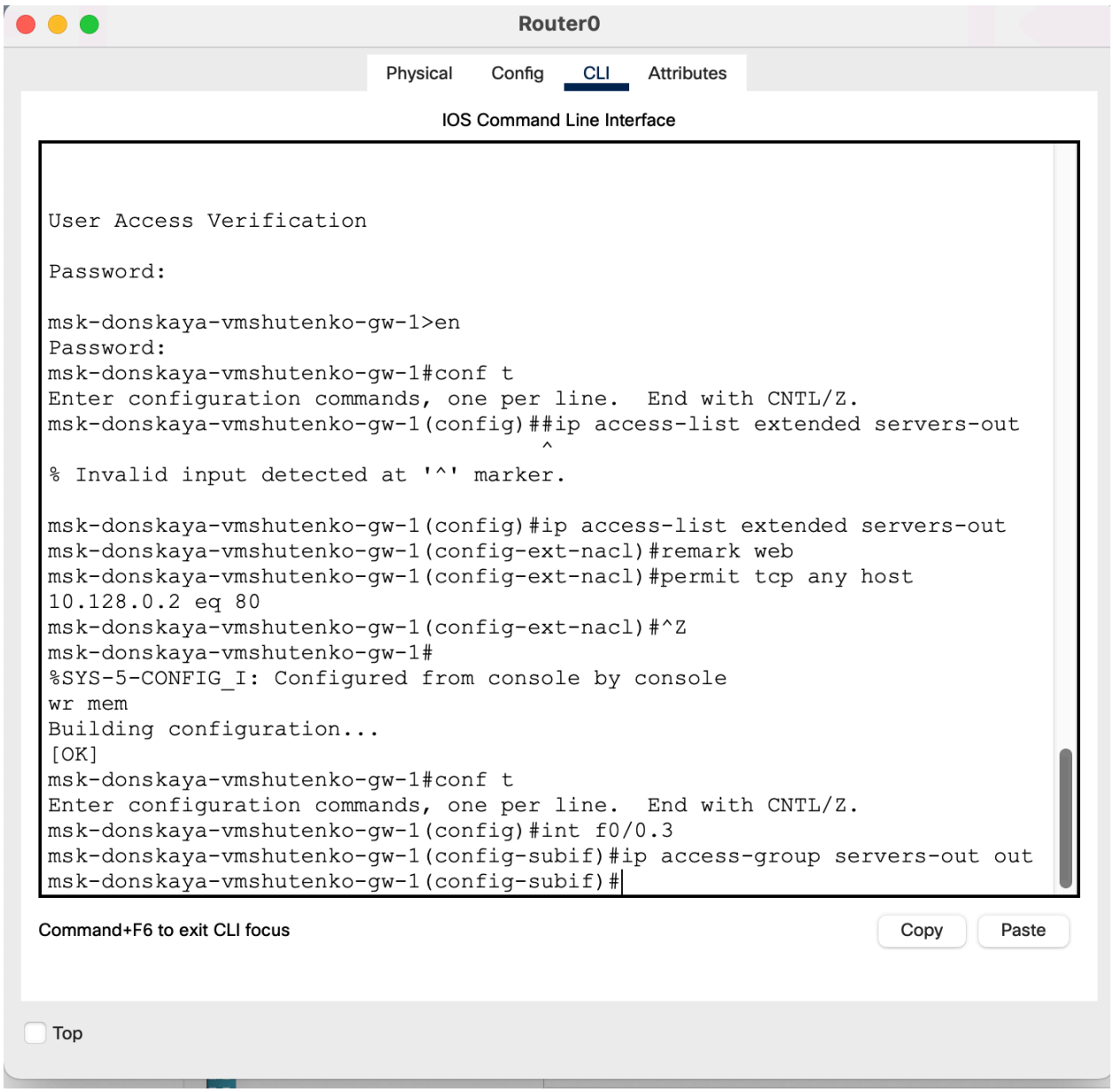

Рисунок 5. Настройка списка управления доступом к интерфейсу.

Проверила, 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.

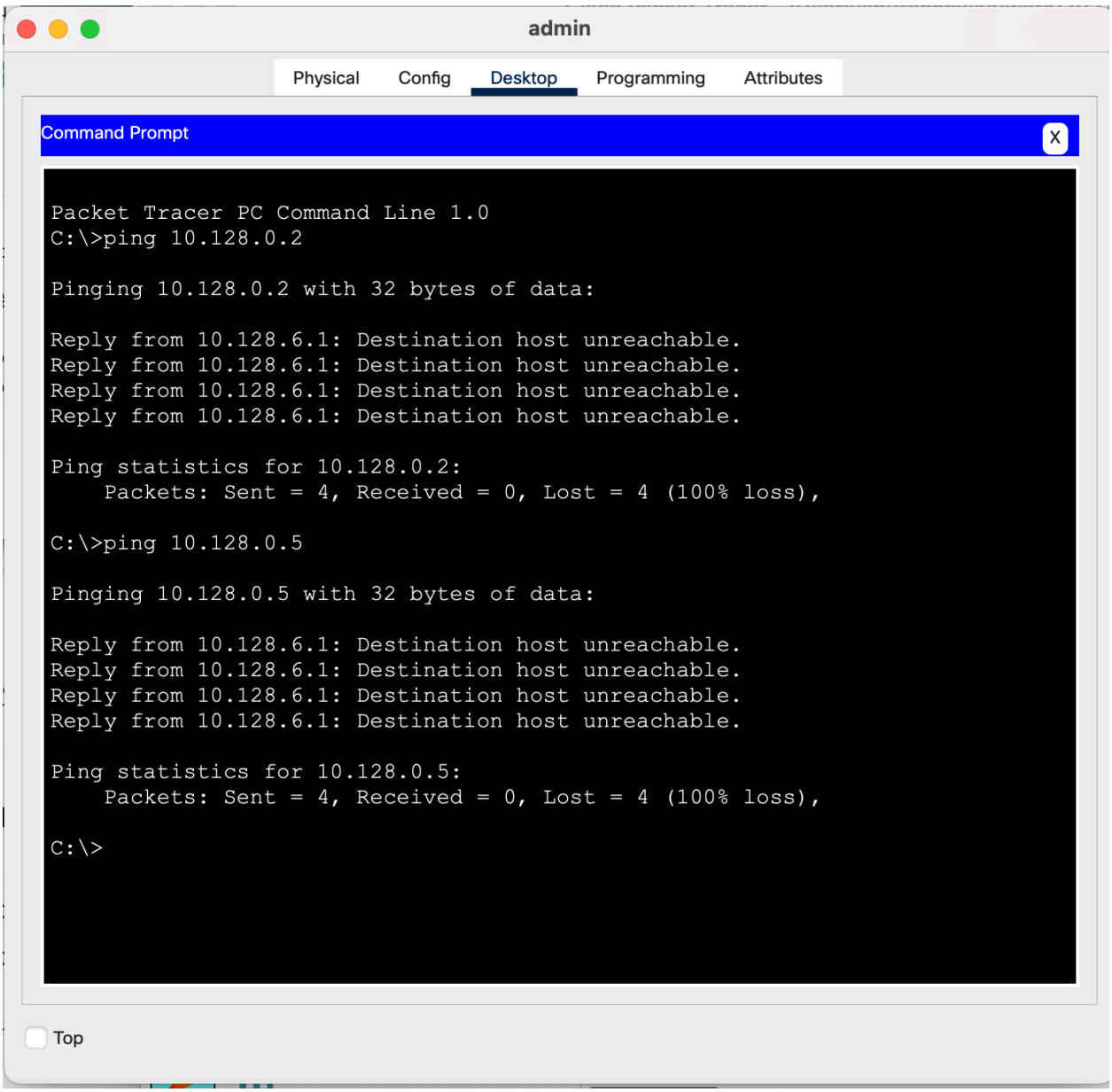

Рисунок 6. Попытка сделать ping.

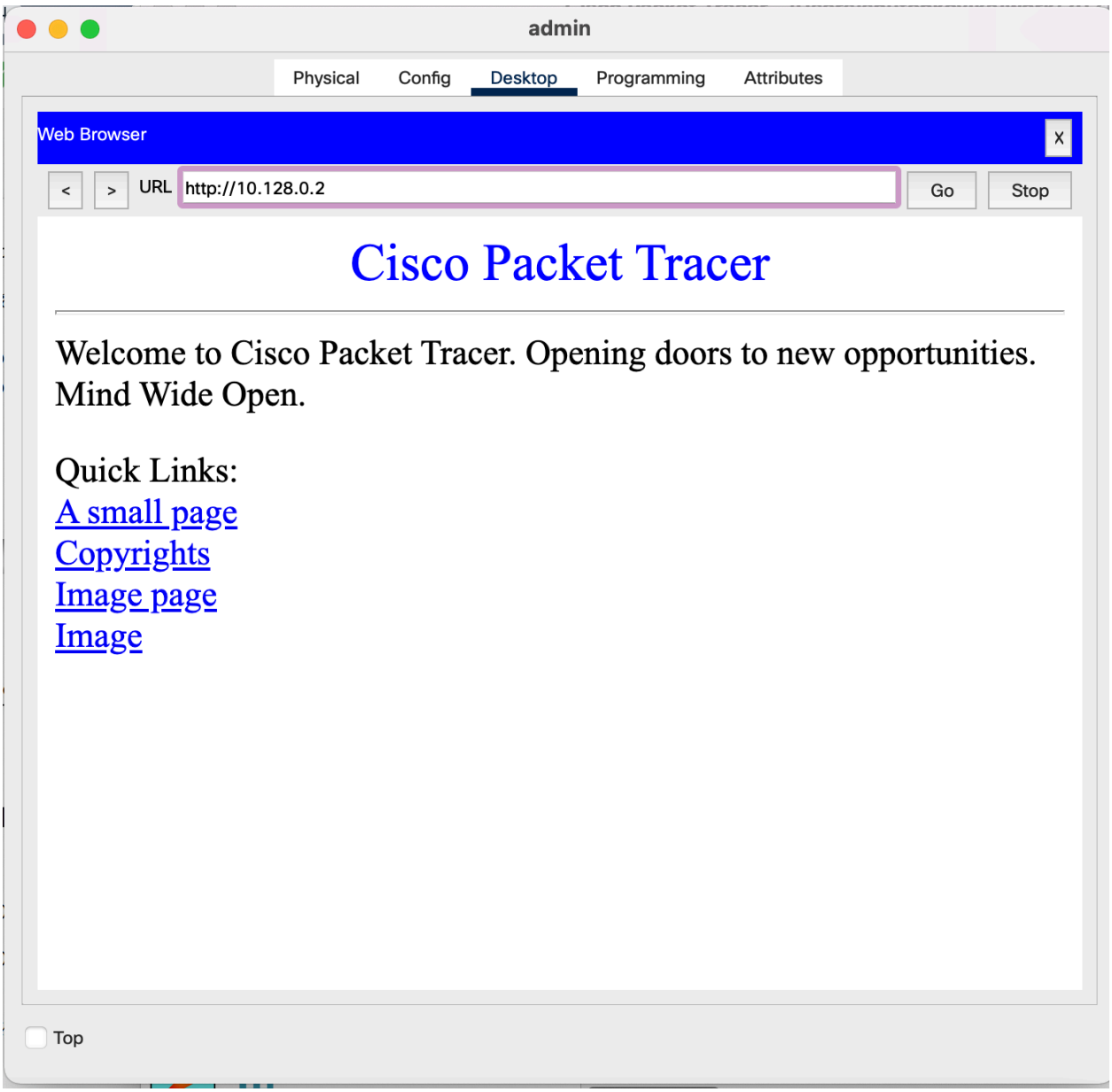

Рисунок 7. Подключение к web через браузер.

3. 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.

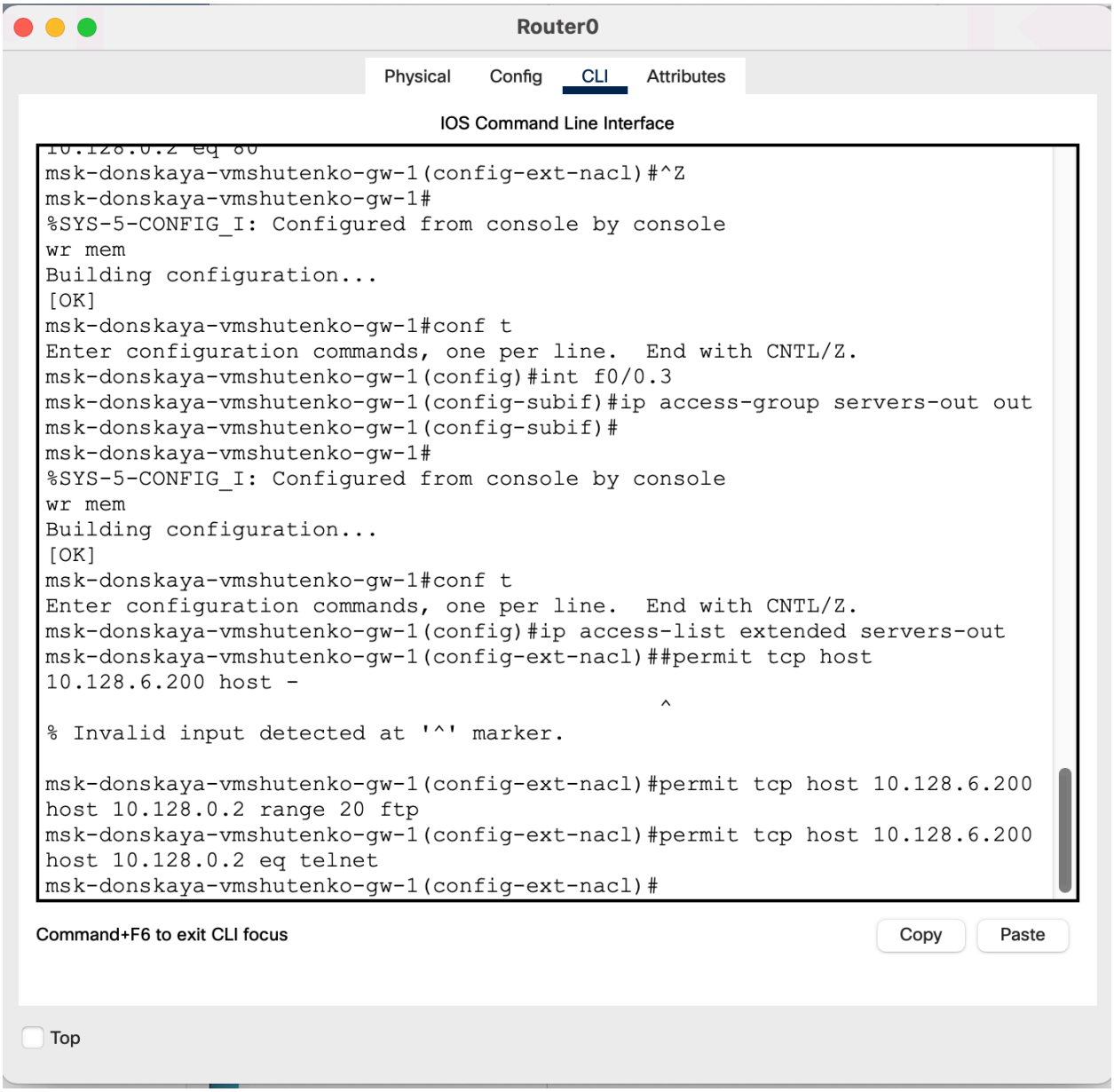

Рисунок 8. Настройка дополнительного доступа для администратора по протоколам Telnet и FTP

Убедилась, что с узла с ip-адресом 10.128.6.200 есть доступ по протоколу FTP. Для этого в командной строке устройства администратора ввела ftp 10.128.0.2, а затем по запросу имя пользователя cisco и пароль cisco (рис. 10.2).

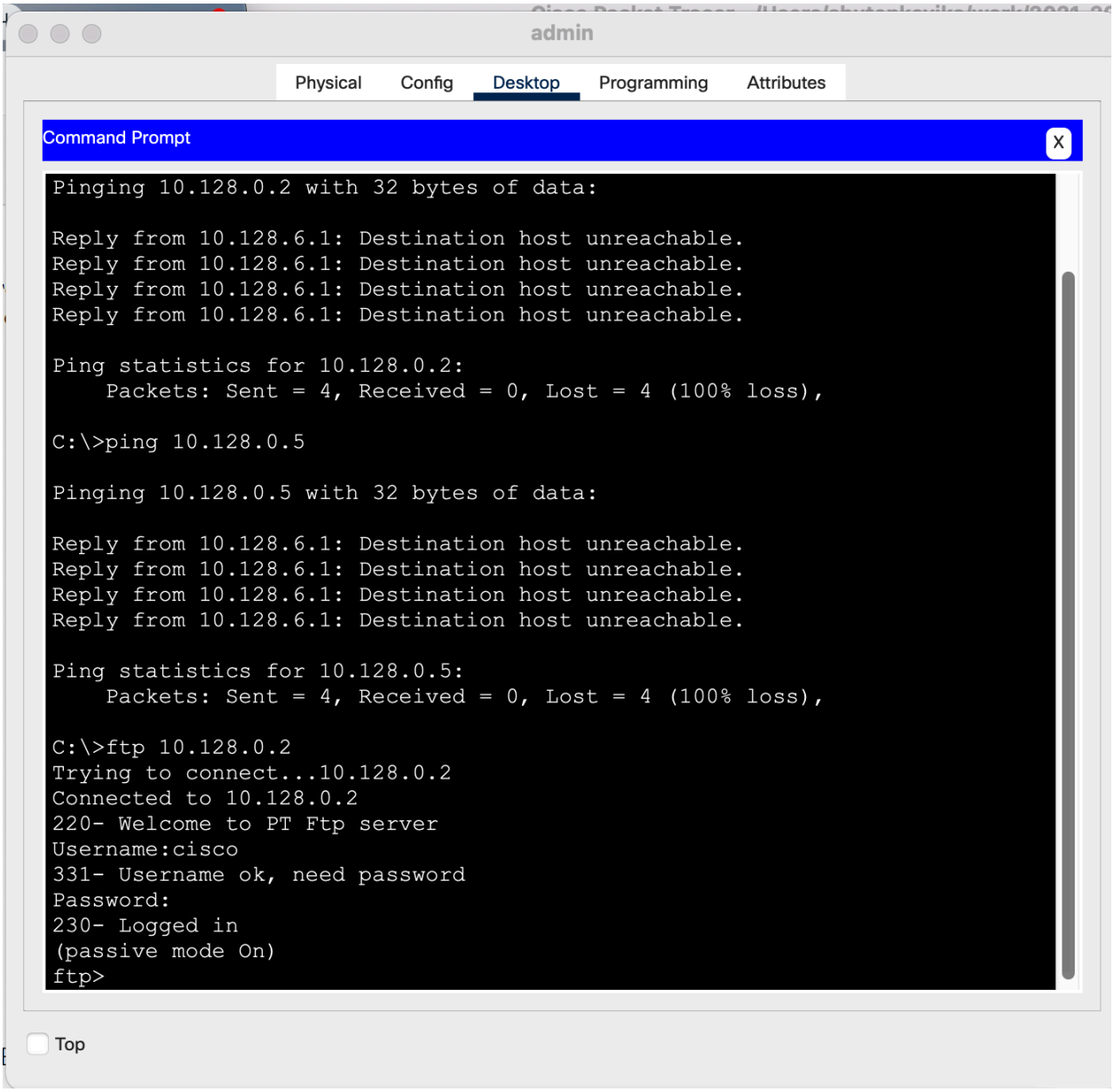

Рисунок 9. Проверка доступа по протоколу FTP.

Попробовала провести аналогичную процедуру с другого устройства сети. Убедилась, что доступ будет запрещён.

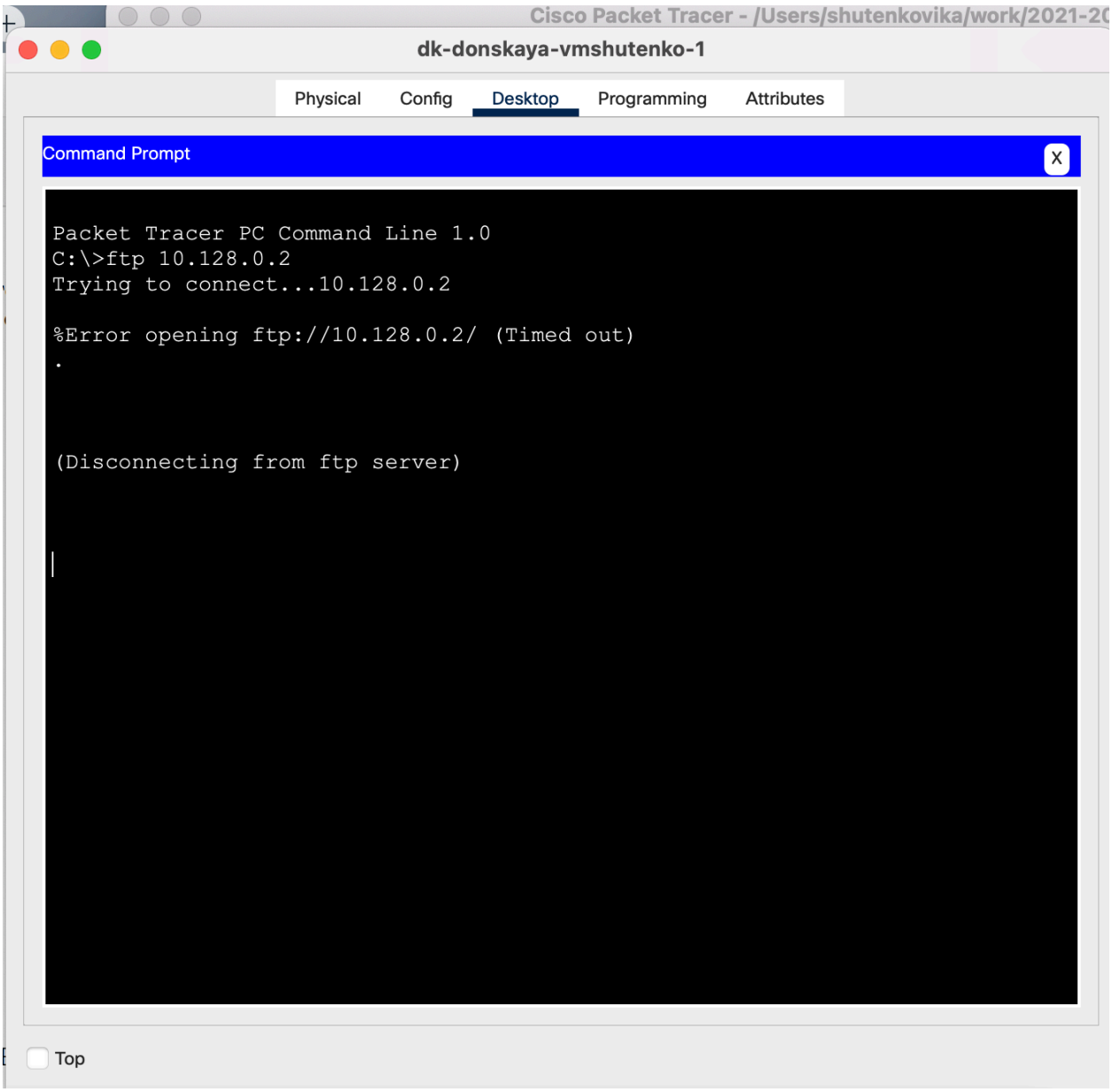

Рисунок 10. Проверка доступа по протоколу FTP.

4. Настроила 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).

Рисунок 11. Настройка доступа к файловому серверу

5. Настроила 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.

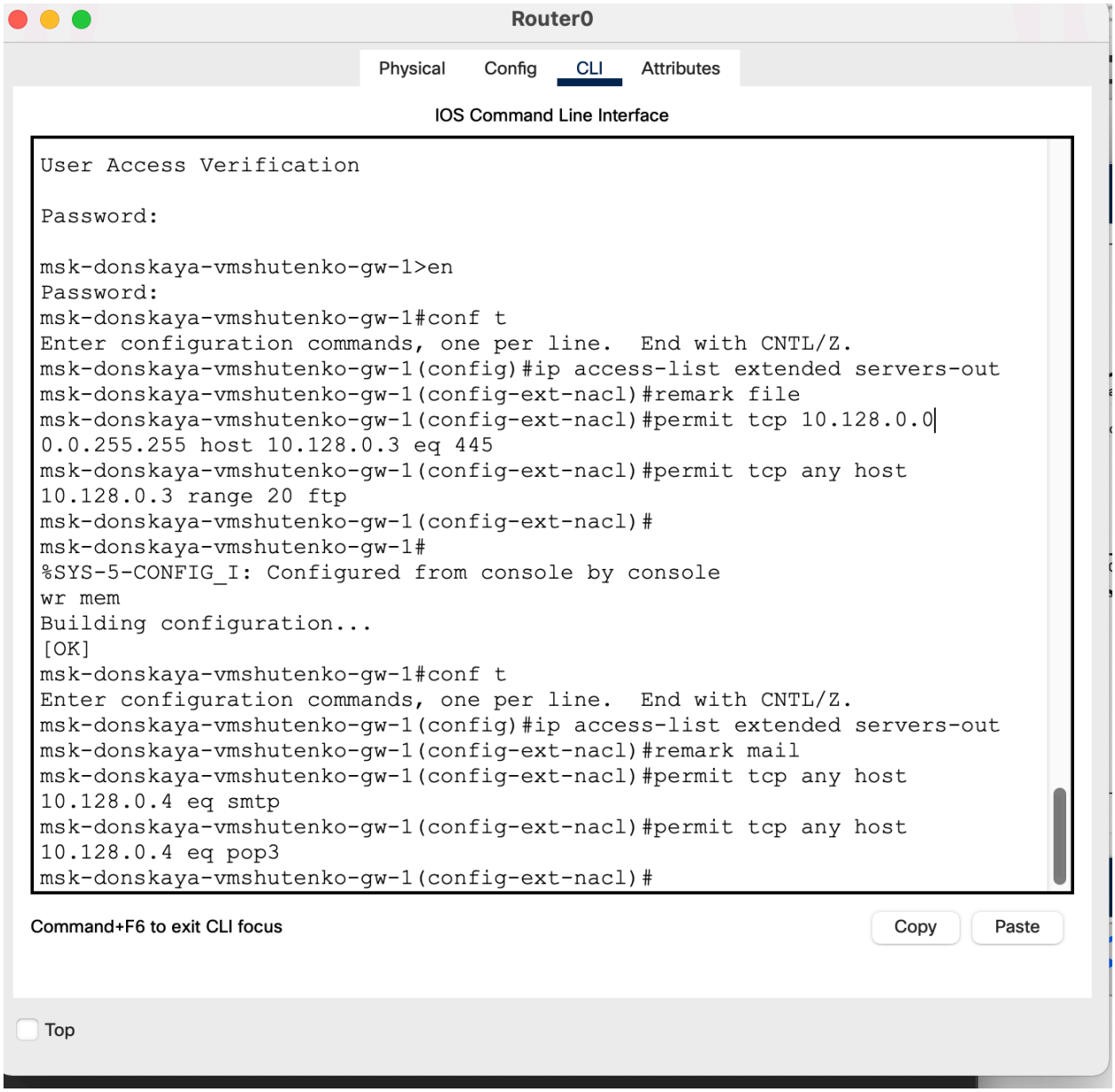

Рисунок 12. Настройка доступа к почтовому серверу.

6. Настроила 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.

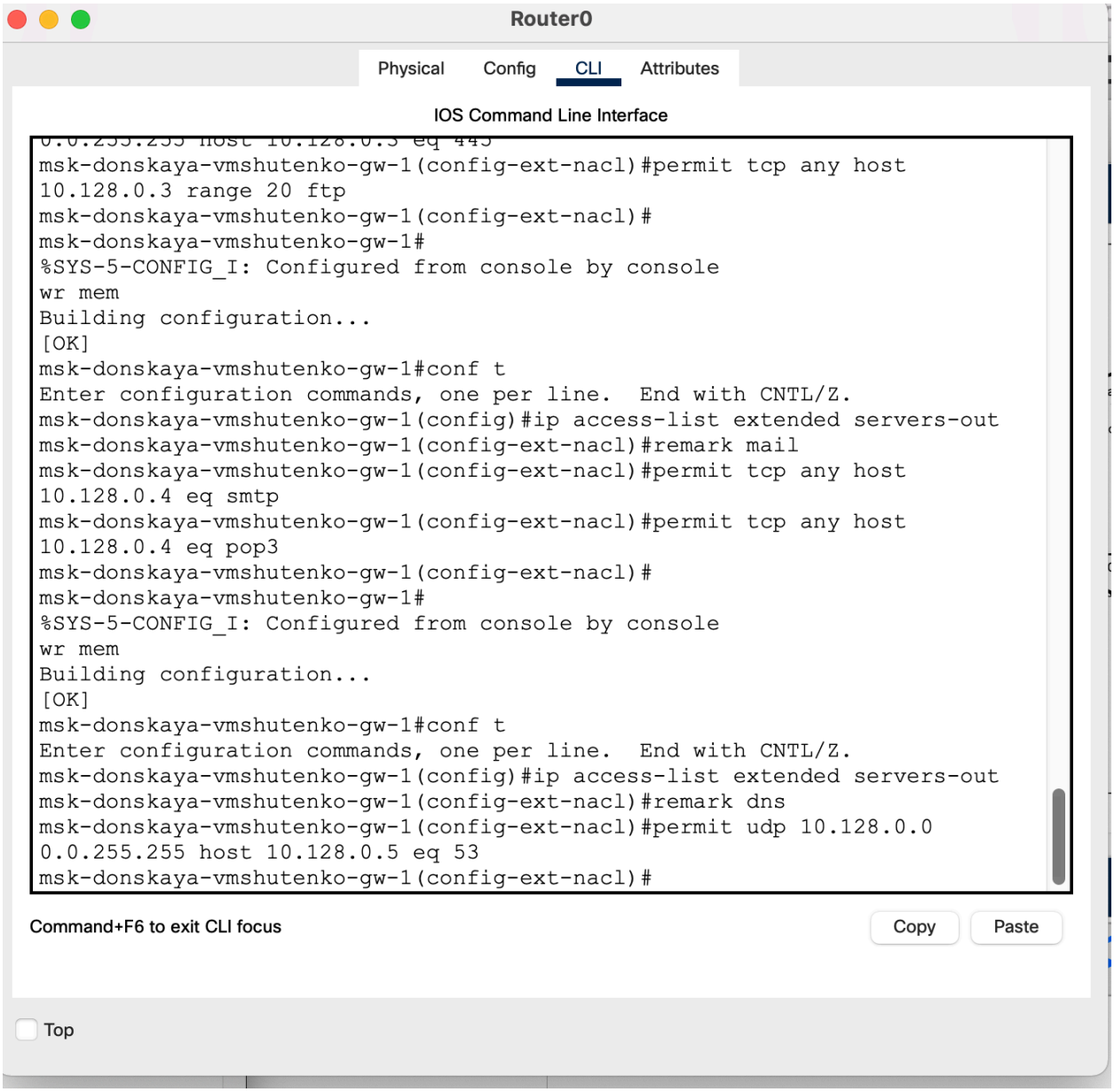

Рисунок 13. Настройка доступа к DNS-серверу

Проверила доступность web-сервера (через браузер) не только по ip-адресу, но и по имени.

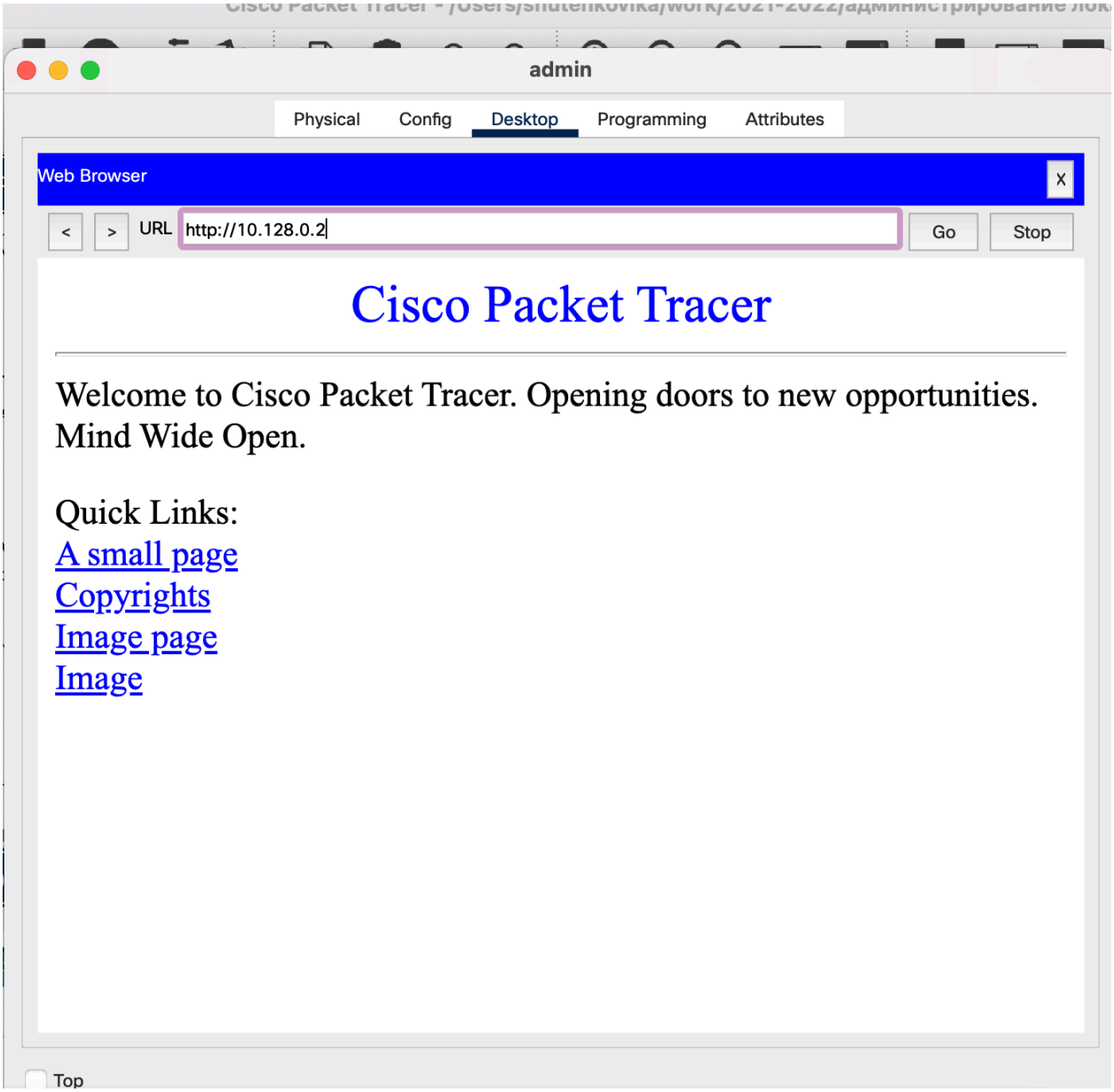

Рисунок 14. Проверка доступности web-сервера (через браузер) по ip-адресу.

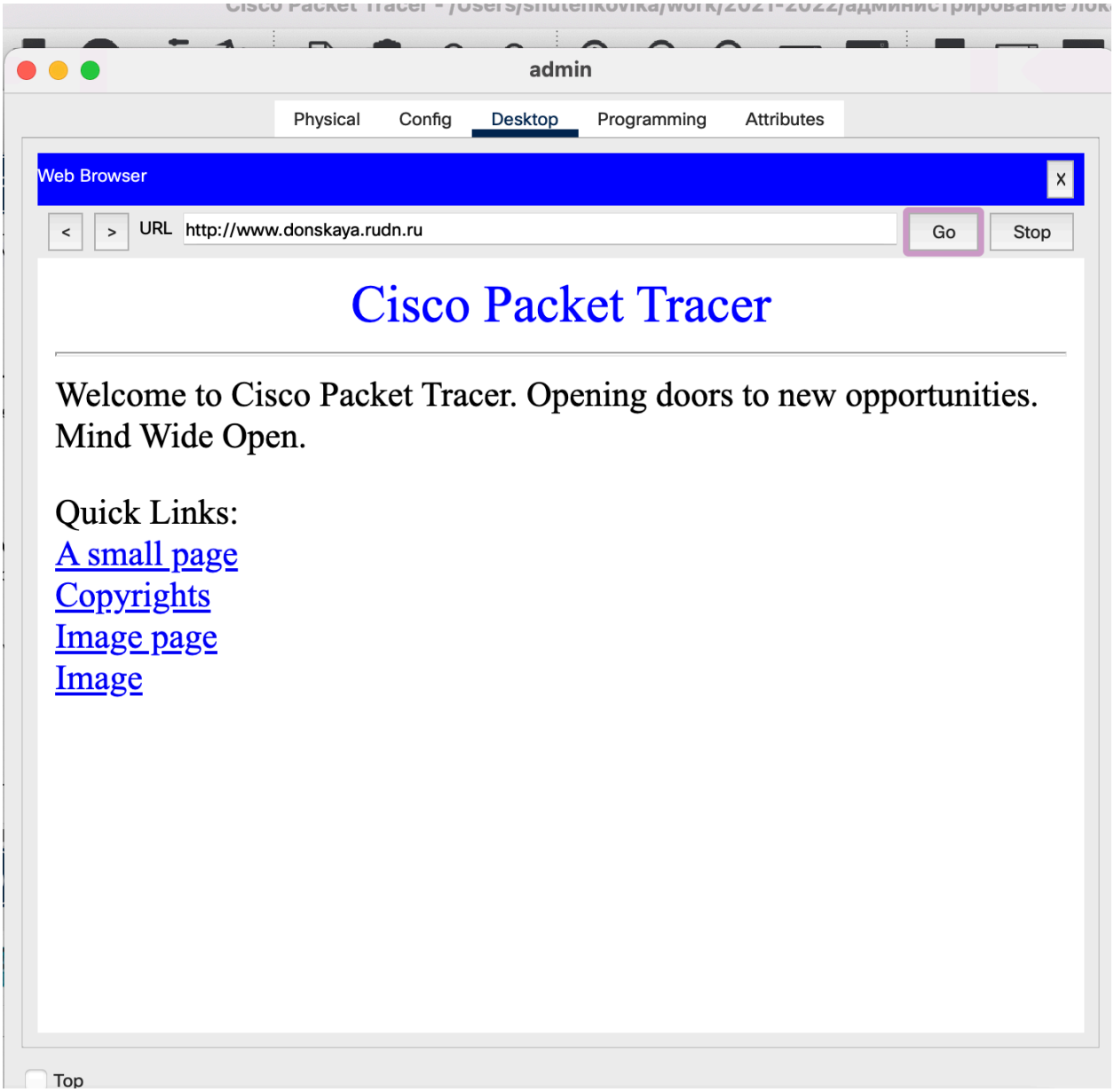

Рисунок 15. Проверка доступности web-сервера (через браузер) по имени.

7. 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.

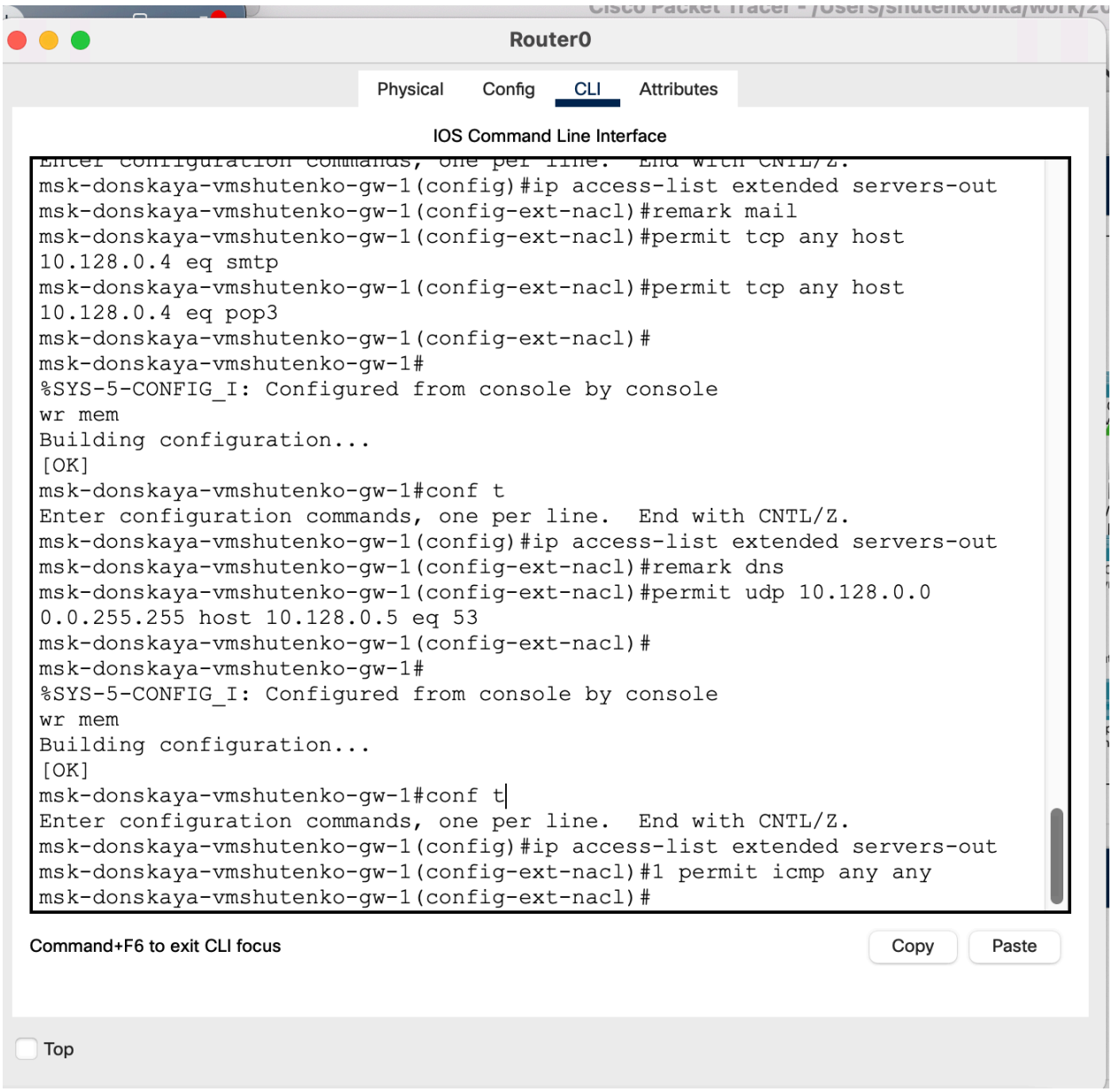

Рисунок 16. Разрешение icmp-запросов.

Номера строк правил в списке контроля доступа можно посмотреть с помощью команды

msk−donskaya−gw−1#show access−lists

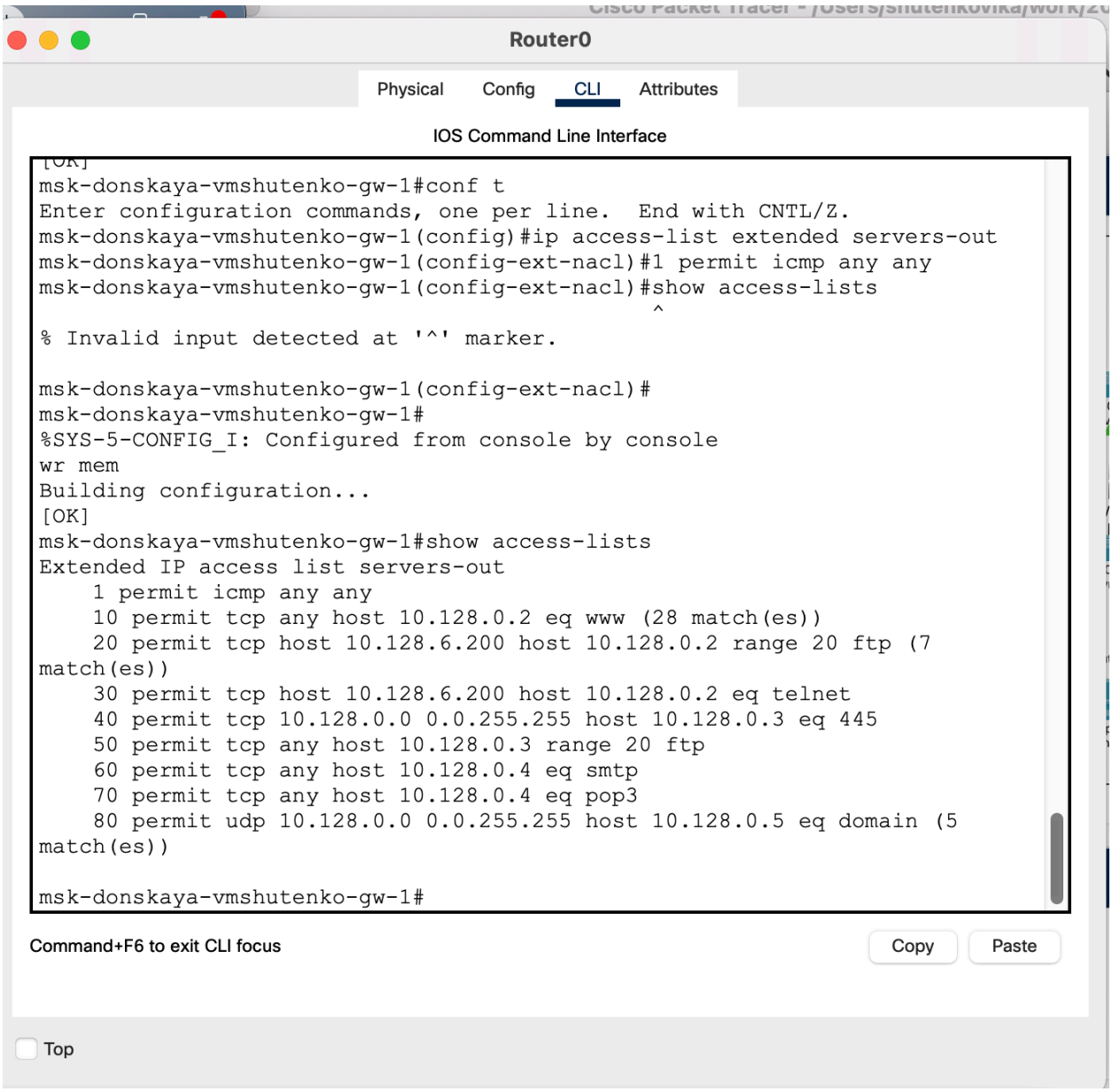

Рисунок 17. Просмотр номера строк правил в списке контроля доступа.

8. Настроила доступа для сети Other (требовалось 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–in

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 in

Здесь: в списке контроля доступа other-in указано, что следующие правила относятся к администратору сети; даётся разрешение устройству с

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).

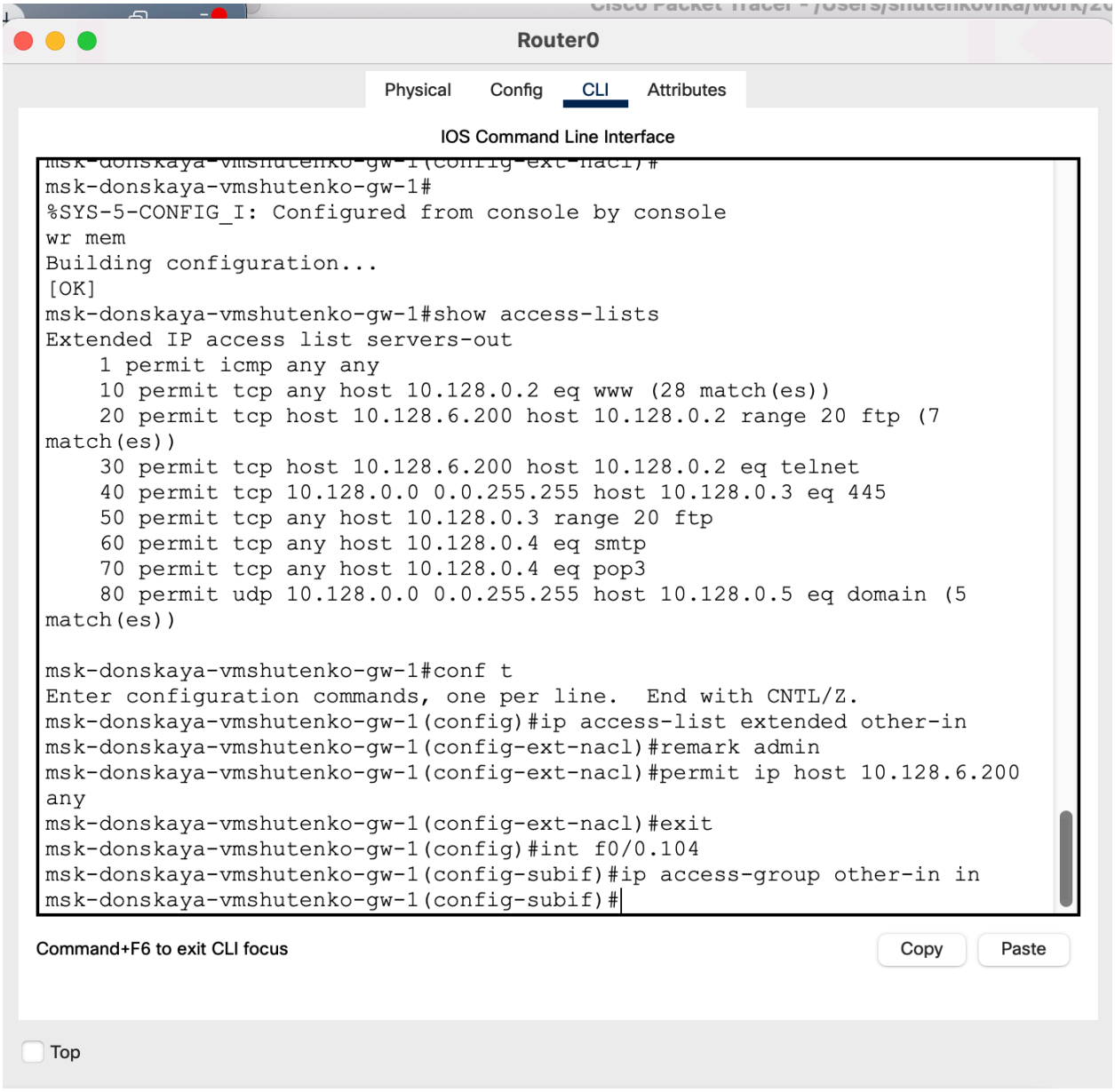

Рисунок 18. Настройка доступа для сети Other.

9. 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).

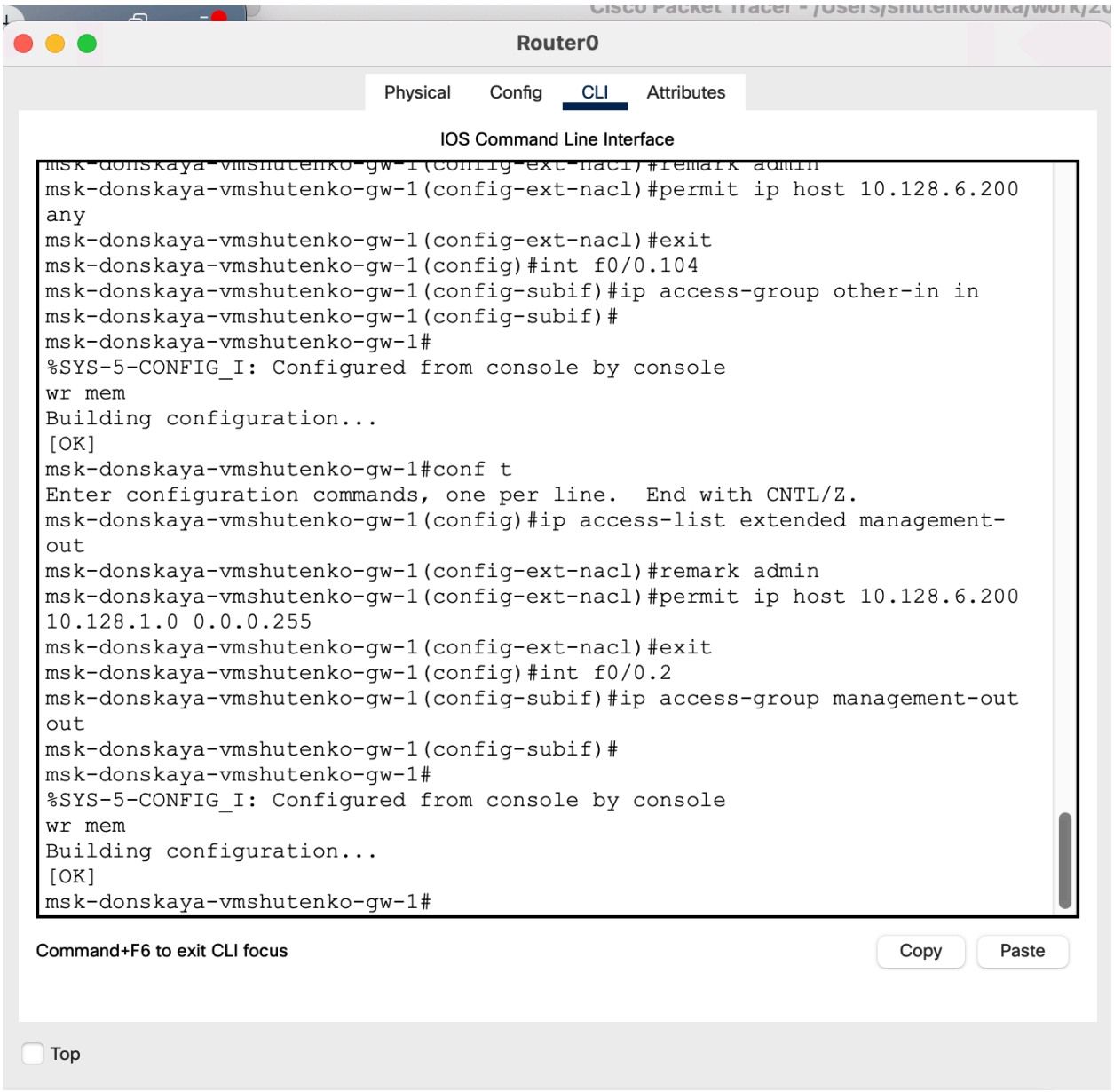

Рисунок 19. Настройка доступа администратора к сети сетевого оборудования.

10.4. Самостоятельная работа

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

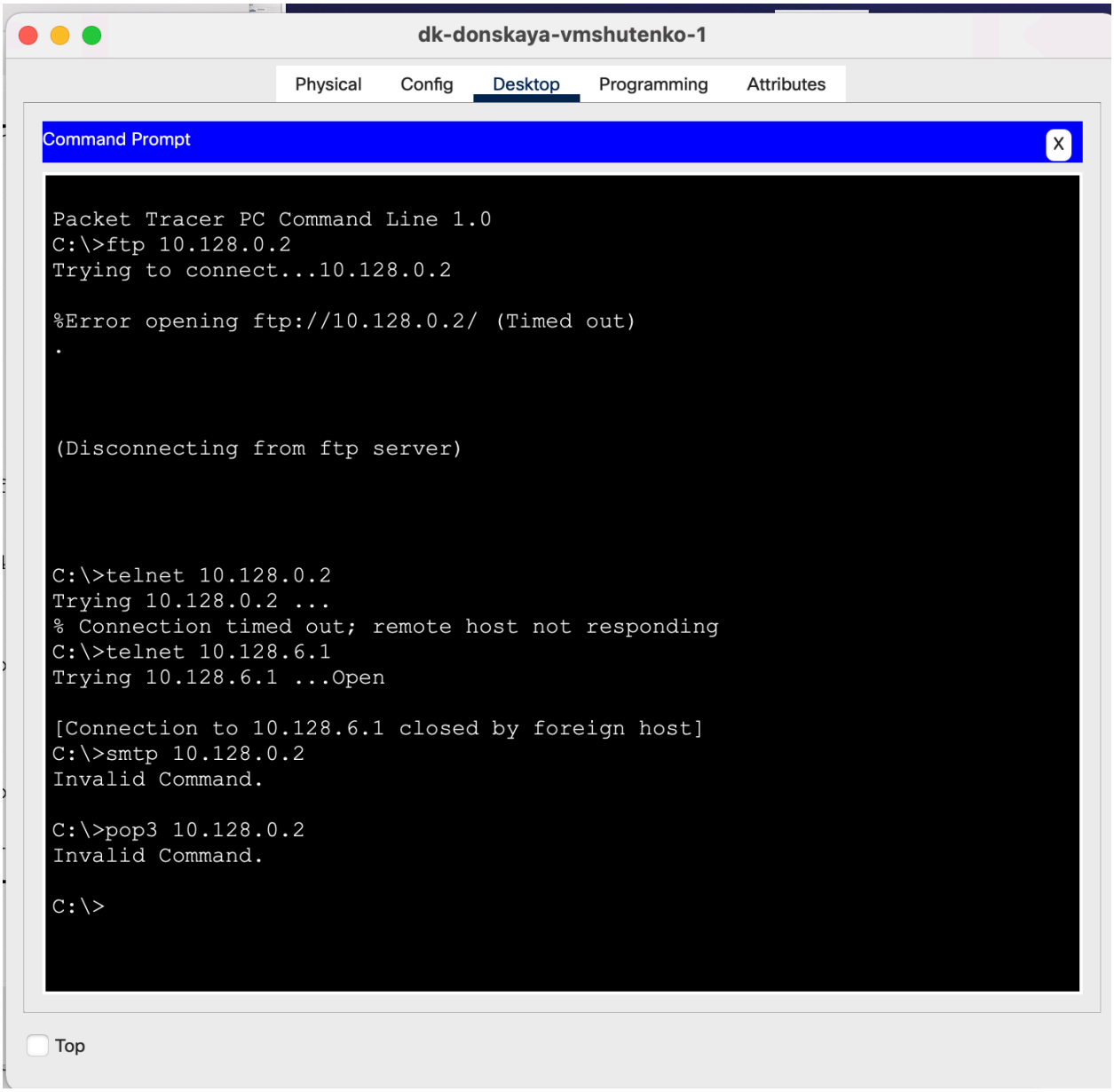

Рисунок 20. Проверка корректности установленных правил доступа.

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

Контрольные вопросы

1. Как задать действие правила для конкретного протокола?

   Стандартный список доступа

   Router(config)#access-list <номер списка от 1 до 99> {permit | deny | remark} {address | any | host} [source-wildcard] [log]

   - permit: разрешить
   - deny: запретить

- remark: комментарий о списке доступа
- address: запрещаем или разрешаем сеть
- any: разрешаем или запрещаем всё
- host: разрешаем или запрещаем хосту
- source-wildcard: WildCard маска сети
- log: включаем логгирование пакеты проходящие через данную запись ACL

2. Как задать действие правила сразу для нескольких портов?
   Router(config)#access-list <номер списка от 100 до 199> {permit | deny | remark} protocol source [source-wildcard] [operator operand] [port <порт или название протокола> [established]
   - protocol source: какой протокол будем разрешать или закрывать (ICMP, TCP, UDP, IP, OSPF и т.д)
   - deny: запретить
   - operator:
     - A.B.C.D — адрес получателя
     - any — любой конечный хост
     - eq — только пакеты на этом порте
     - gt — только пакеты с большим номером порта
     - host — единственный конечный хост
     - lt — только пакеты с более низким номером порта
     - neq — только пакеты не на данном номере порта
     - range — диапазон портов
   - port: номер порта (TCP или UDP), можно указать имя
   - established: разрешаем прохождение TCP-сегментов, которые являются частью уже созданной TCP-сессии
3. Как узнать номер правила в списке прав доступа?
   - R#show access-lists {ACL номер | имя} — смотрим информацию о списке доступа.

- R#show access-lists — смотрим все списки доступа на маршрутизаторе.

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

Для фильтрации адресов в ACL используется WildCard-маска. Это обратная маска. Берем шаблонное выражение: 255.255.255.255 и отнимаем от шаблона обычную маску.

255.255.255.255-255.255.255.0, у нас получается маска 0.0.0.255, что является обычной маски 255.255.255.0, только 0.0.0.255 является WildCard маской.