Отчёт по лабораторной работе №10

Настройка списков управления доступом (ACL)

Козлов Всеволод Павлович НФИбд-02-22

Содержание

Список иллюстраций

Список таблиц

# 1 Цель работы

Освоить настройку прав доступа пользователей к ресурсам сети

# 2 Задание

1. Требуется настроить следующие правила доступа:
2. web-сервер: разрешить доступ всем пользователям по протоколу HTTP через порт 80 протокола TCP, а для администратора открыть доступ по протоколам Telnet и FTP;
3. файловый сервер: с внутренних адресов сети доступ открыт по портам для общедоступных каталогов, с внешних — доступ по протоколу FTP;
4. 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;
5. DNS-сервер: открыть порт 53 протокола UDP для доступа из внутренней сети;
6. разрешить icmp-сообщения, направленные в сеть серверов;
7. запретить для сети Other любые запросы за пределы сети, за исключением администратора;
8. разрешить доступ в сеть управления сетевым оборудованием только администратору сети.
9. Требуется проверить правильность действия установленных правил доступа.
10. Требуется выполнить задание для самостоятельной работы по настройке прав доступа администратора сети на Павловской.
11. При выполнении работы необходимо учитывать соглашение об именовании.

# 3 Выполнение лабораторной работы

Подключил ноутбук администратора (рис. 1)

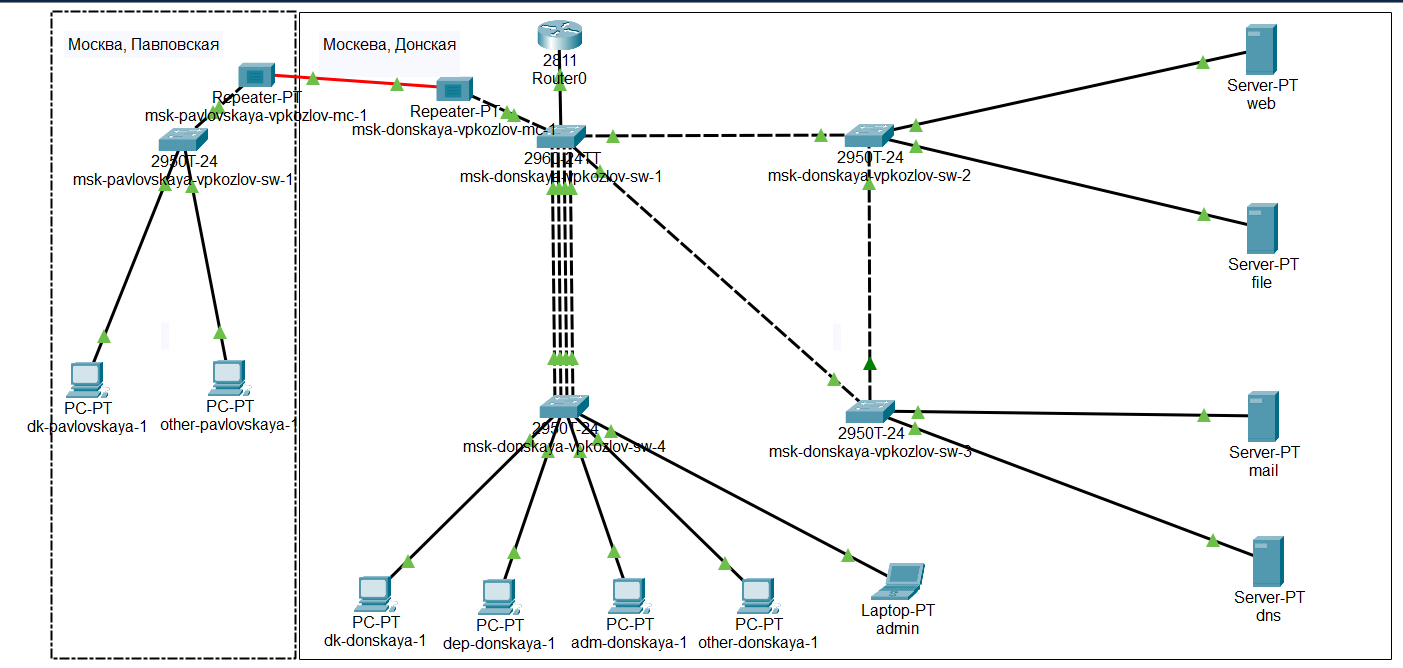


Рис. 1: Ноутбук администратора

Настроил конфигурацию ноутбука администратора (рис. 2)

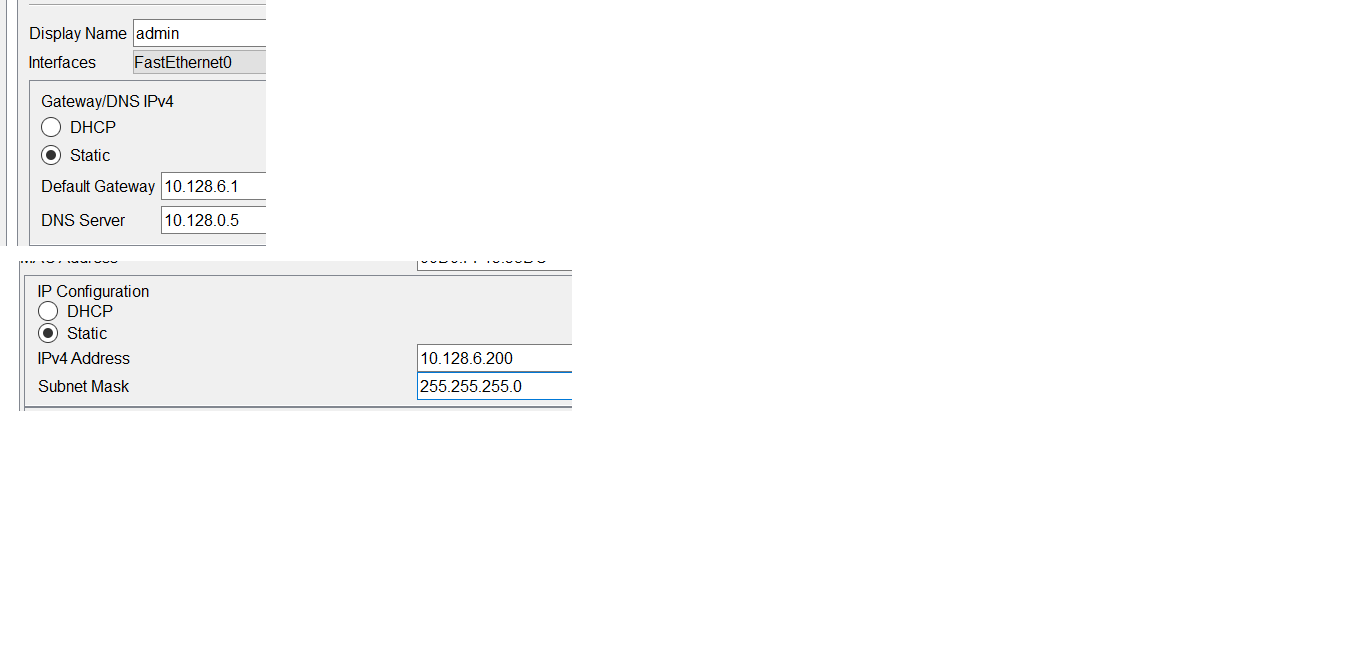


Рис. 2: Конфигурация ноутбука администратора

Проверка работоспособности соединения ноутбука admin (рис. 3)

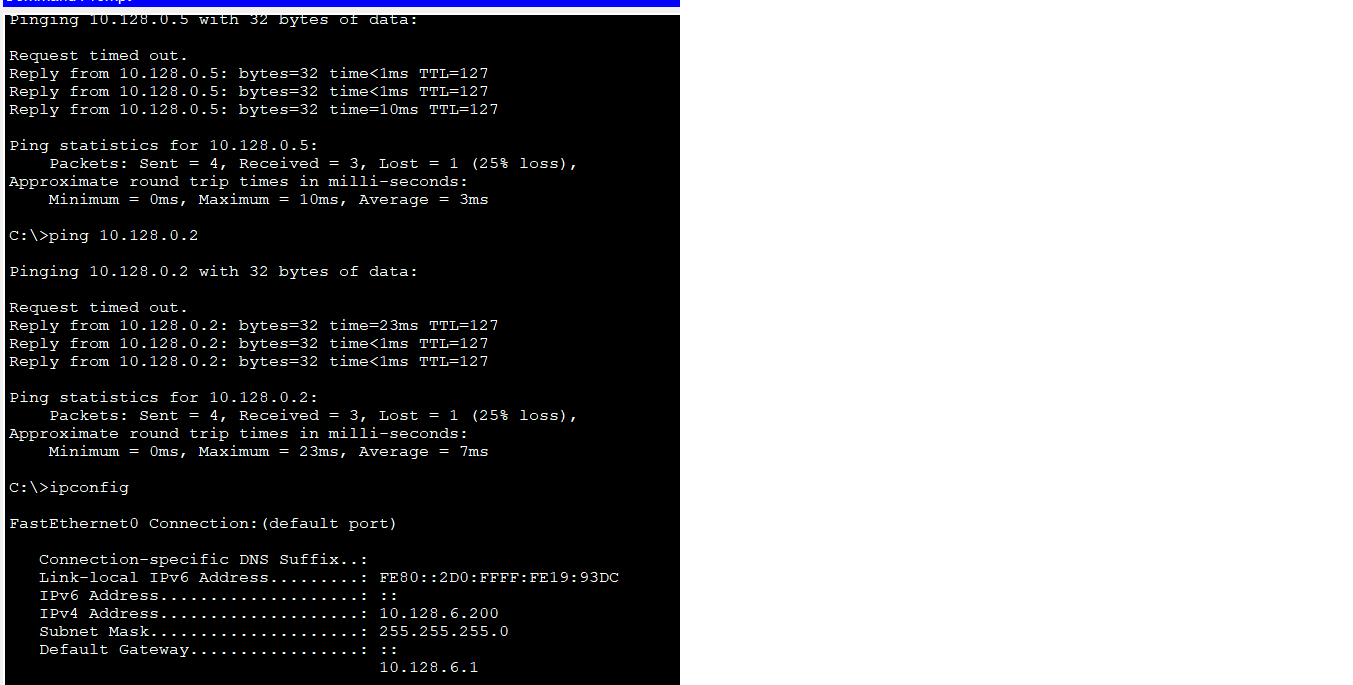


Рис. 3: Проверка работоспособности соединения ноутбука admin

Настройка доступа к web-серверу по порту tcp 80 (рис. 4)

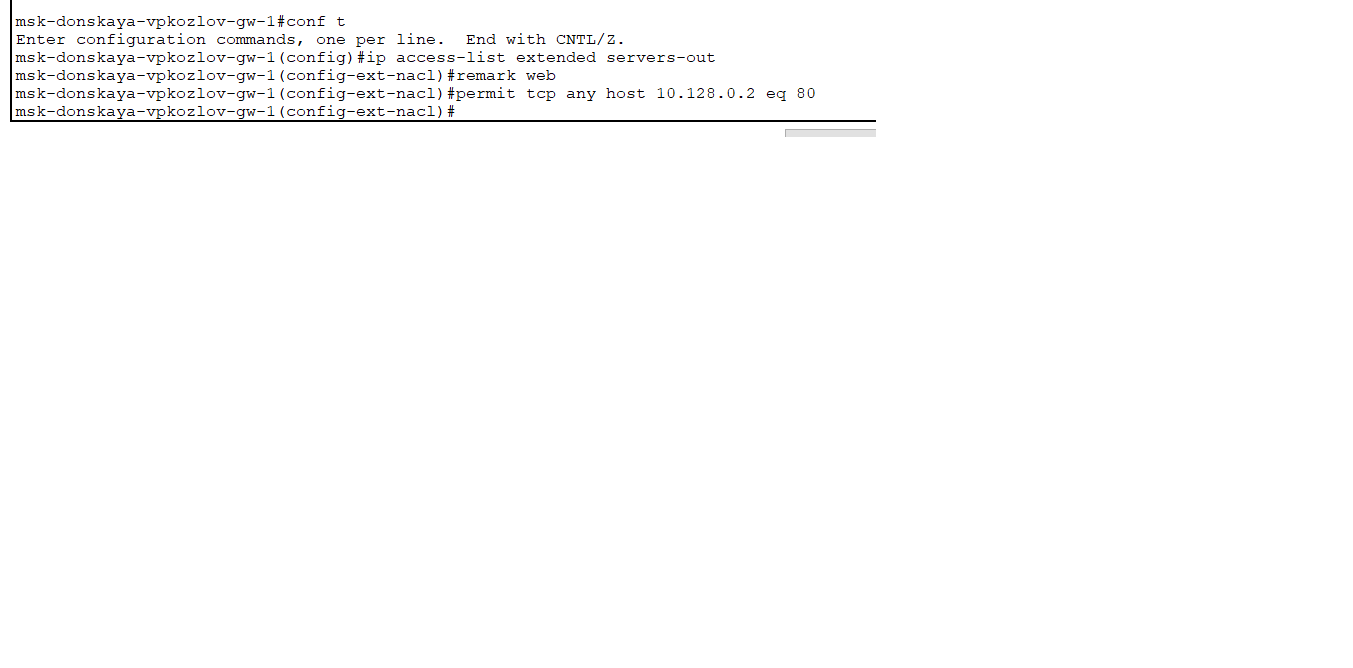


Рис. 4: Настройка доступа к web-серверу по порту tcp 80

Добавление списка управления доступом к интерфейсу (рис. 5)

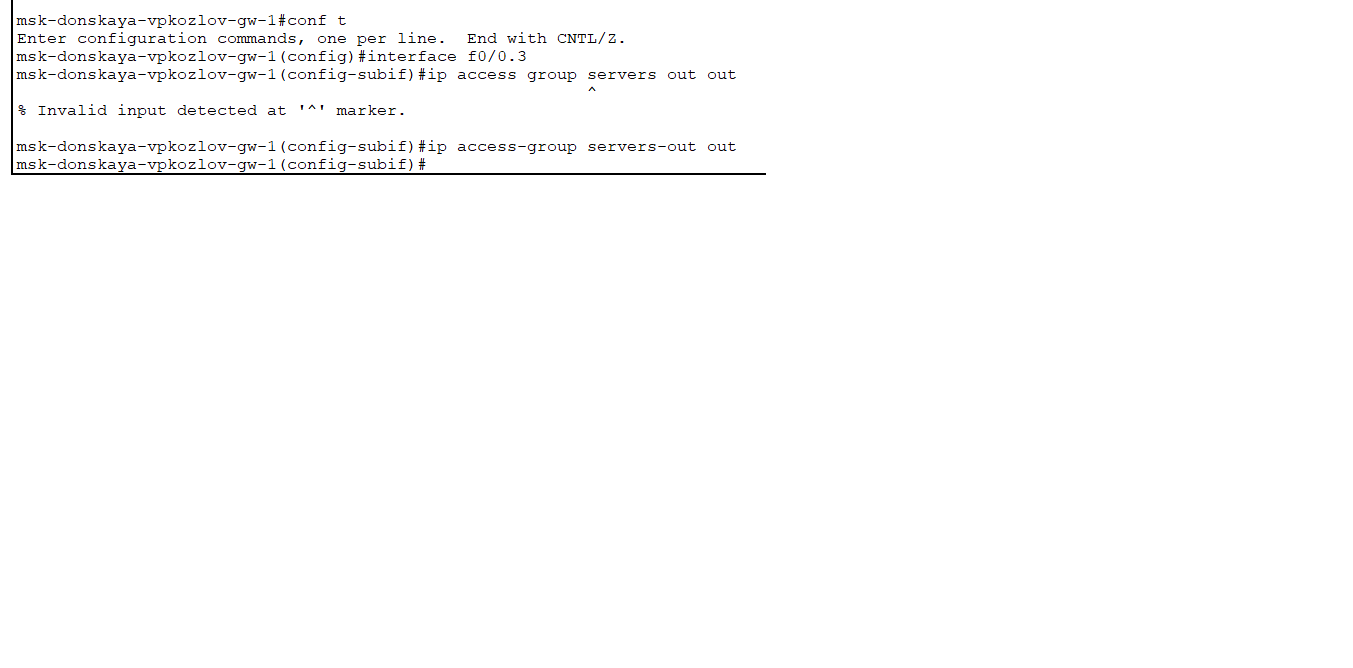


Рис. 5: Добавление списка управления доступом к интерфейсу

Проверка недоступности web-сервера через ping (рис. 6)

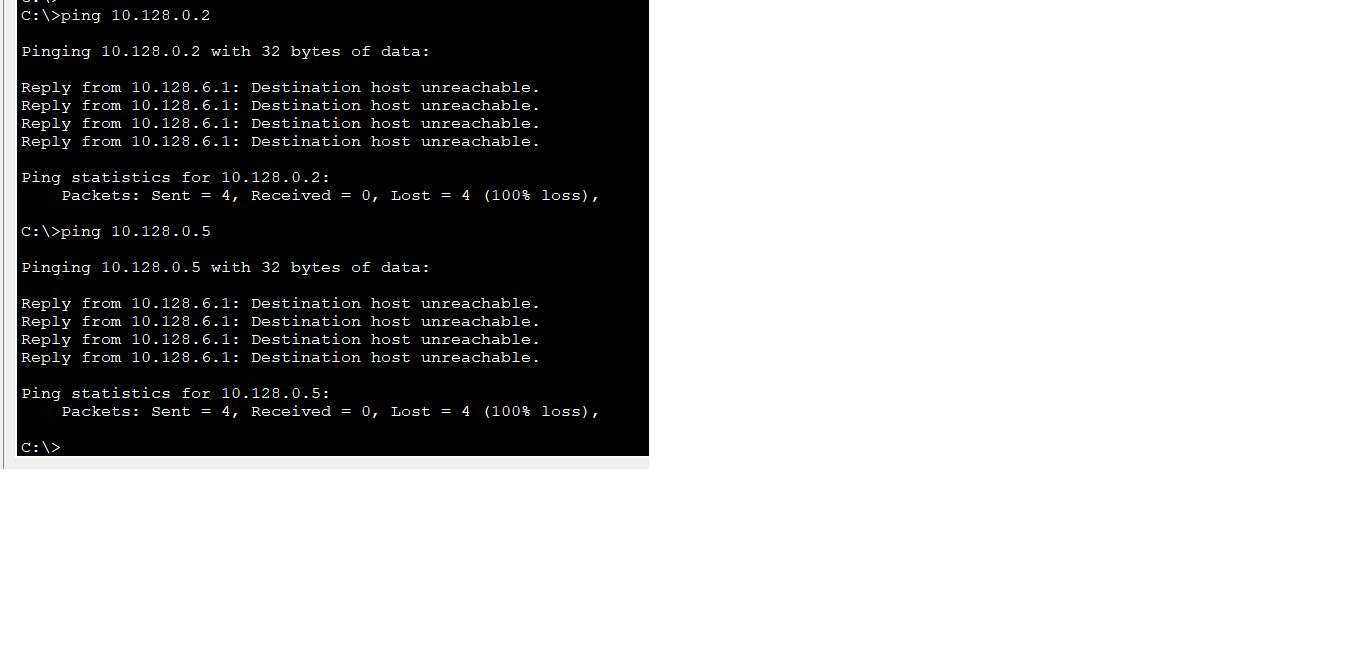


Рис. 6: Недоступность web-сервера через ping

Дополнительный доступ для администратора по протоколам Telnet и FTP (рис. 7)

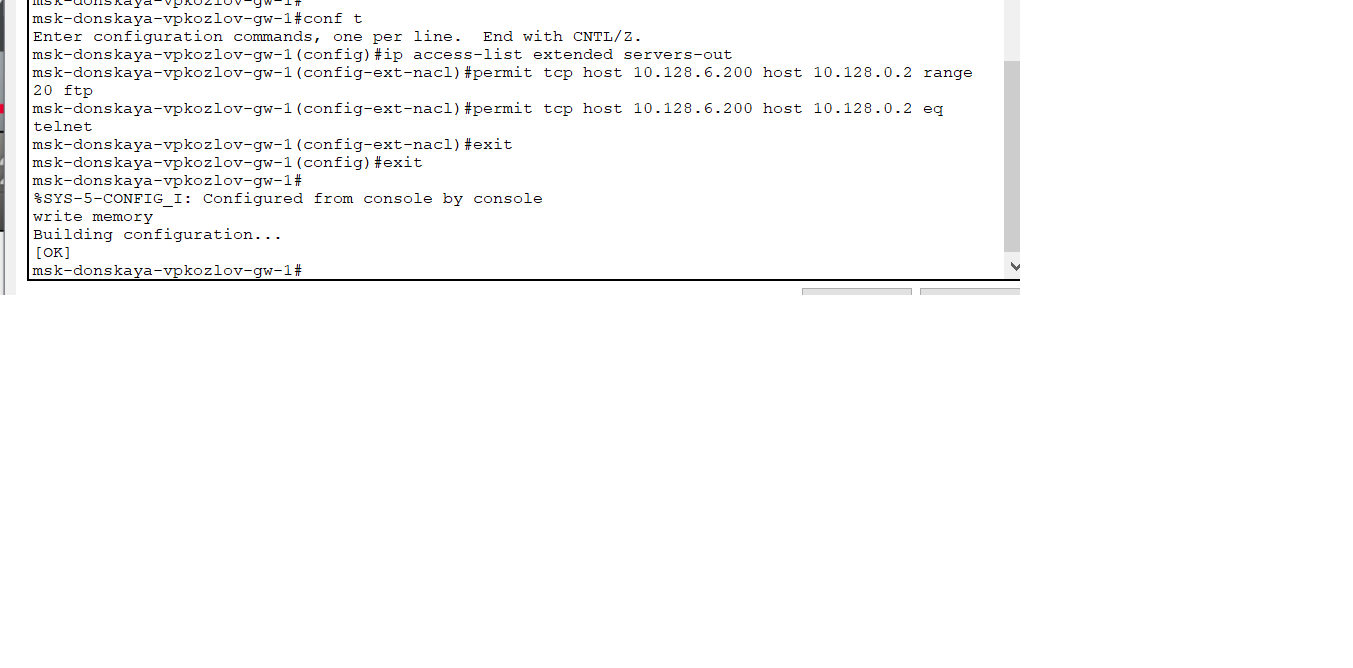


Рис. 7: Дополнительный доступ для администратора по протоколам Telnet и FTP

Попытка подключения по FTP (рис. 8)



Рис. 8: Попытка подключения по FTP

Настройка доступа к файловому серверу (рис. 9)

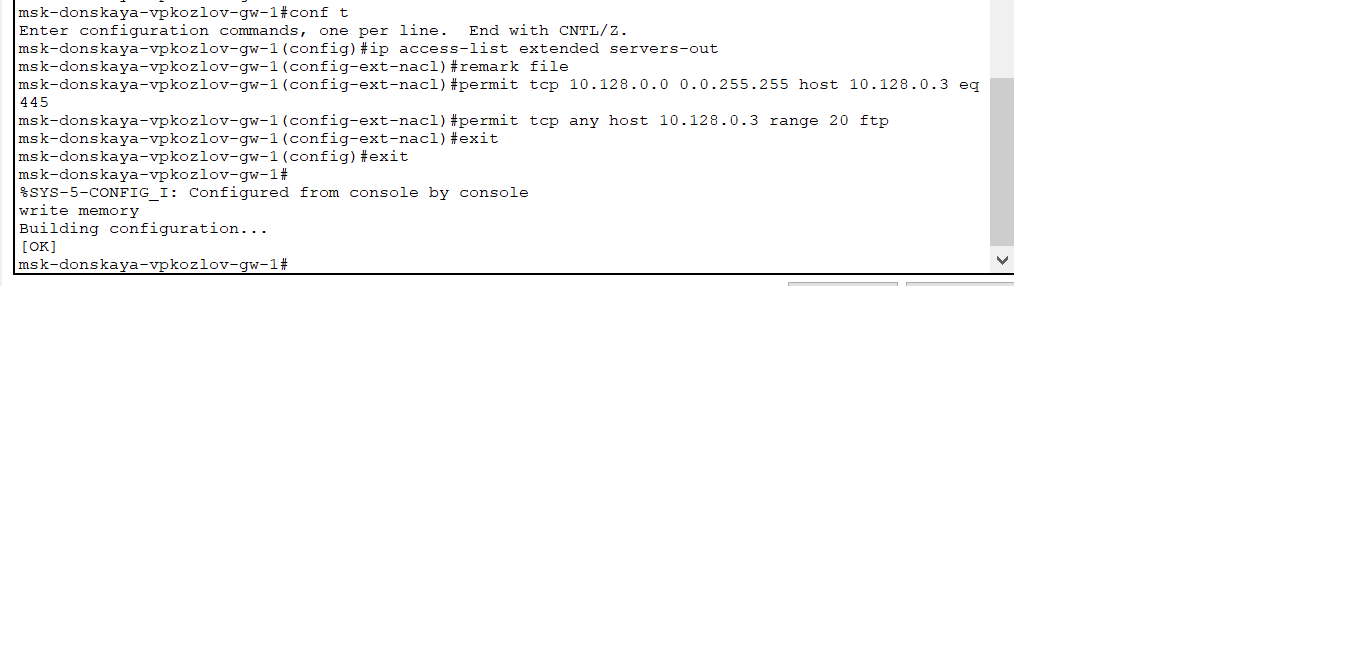


Рис. 9: Настройка доступа к файловому серверу

Настройка доступа к почтовому серверу (рис. 10)

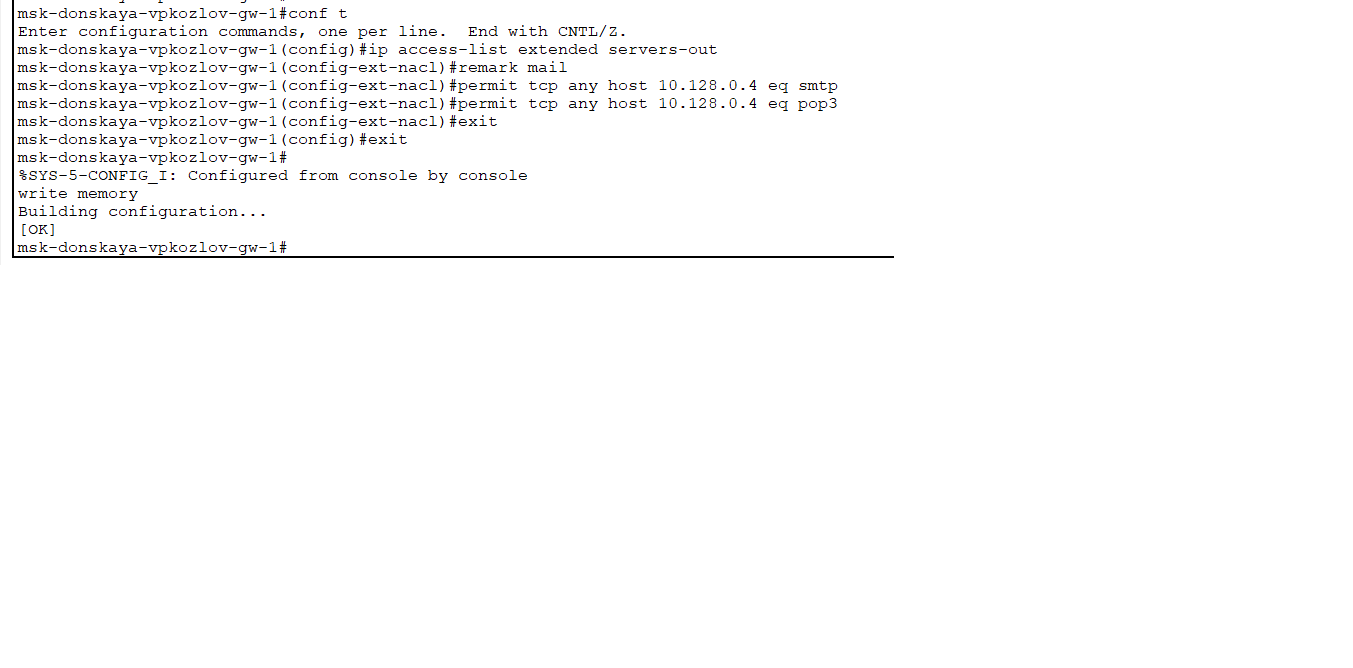


Рис. 10: Настройка доступа к почтовому серверу

Настройка доступа к DNS-серверу (рис. 11)

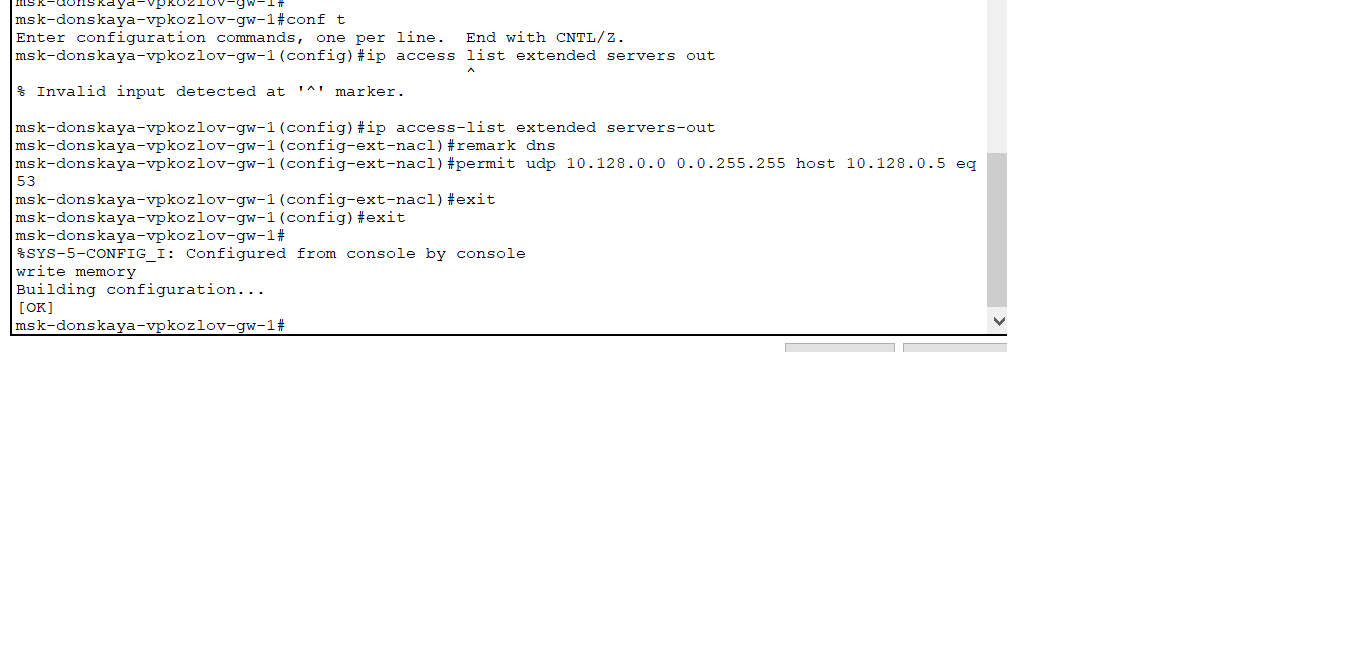


Рис. 11: Настройка доступа к DNS-серверу

Проверил доступность web-сервера в браузере (рис. 12)



Рис. 12: Доступность web-сервера в браузере

Разрешение icmp-запросов (рис. 13)

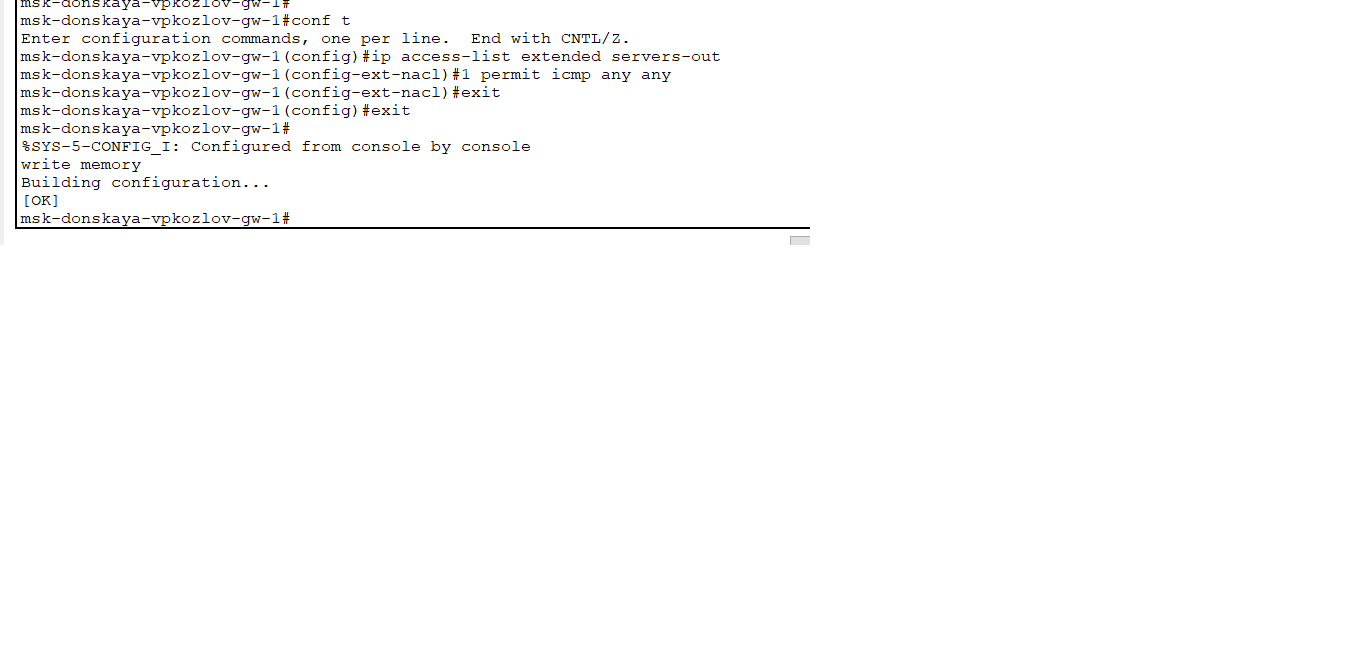


Рис. 13: Разрешение icmp-запросов

Посмотрел правила в списке контроля доступа (рис. 14)

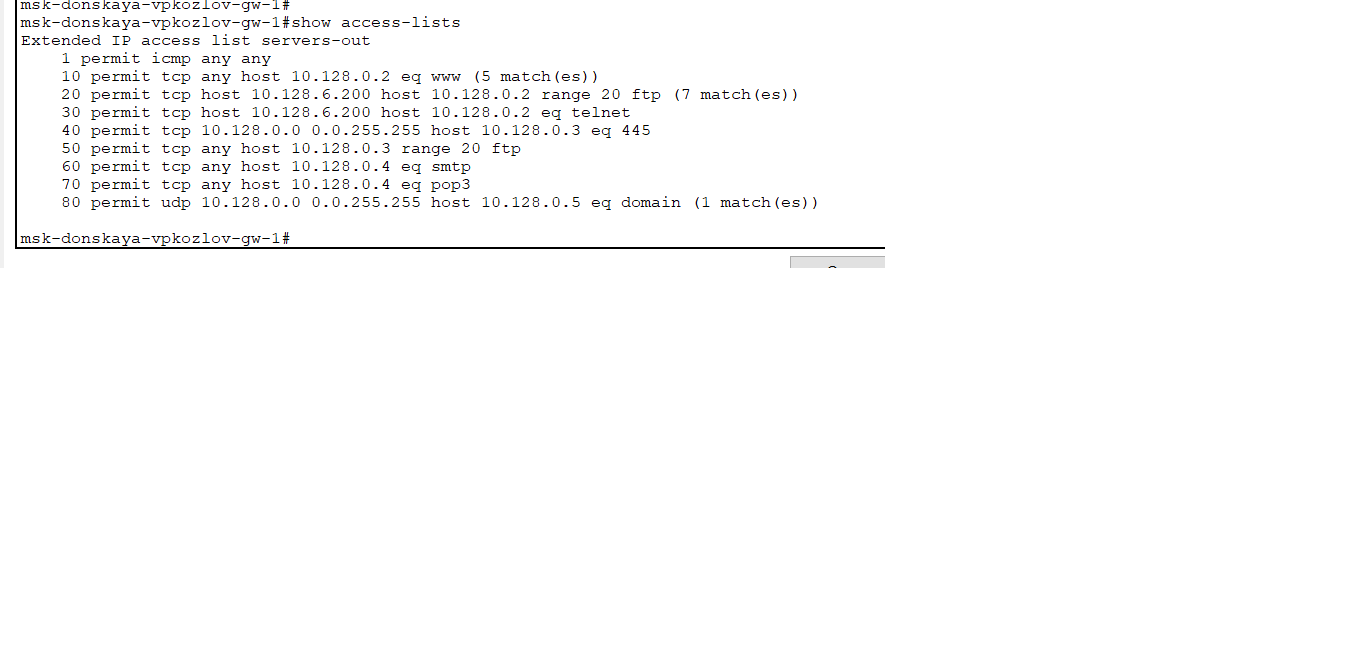


Рис. 14: Правила в списке контроля доступа

Проверил пингование (рис. 15)

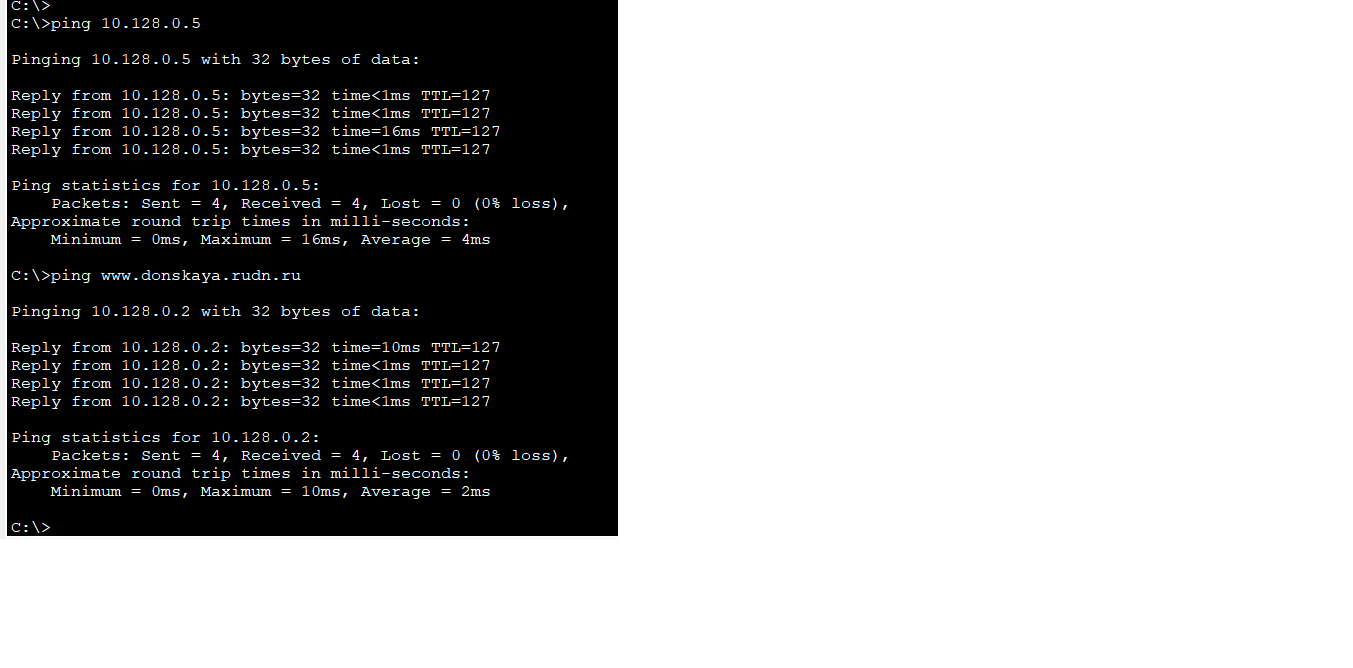


Рис. 15: Проверка пингования

Настройка доступа для сети Other (рис. 16)

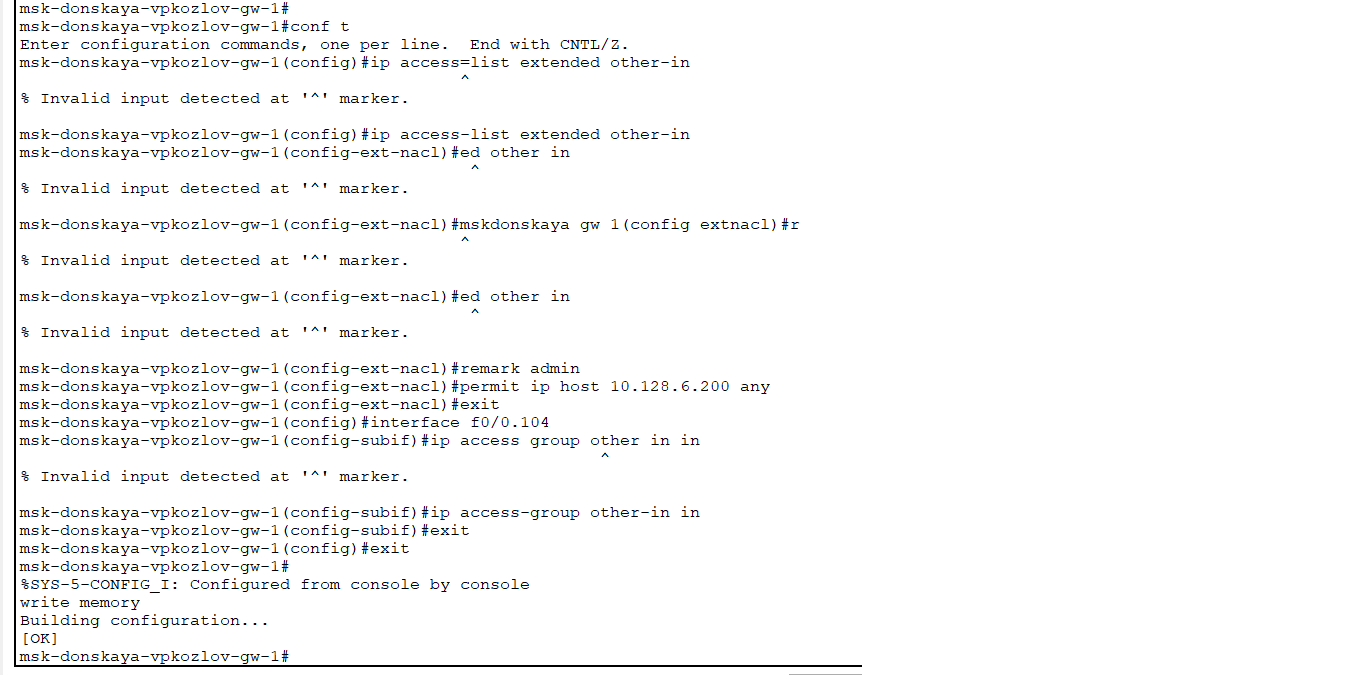


Рис. 16: Настройка доступа для сети Other

# 4 Самостоятельная работа

Пингование с устройства dep-donskaya-vpkozlov-1 (рис. 17)

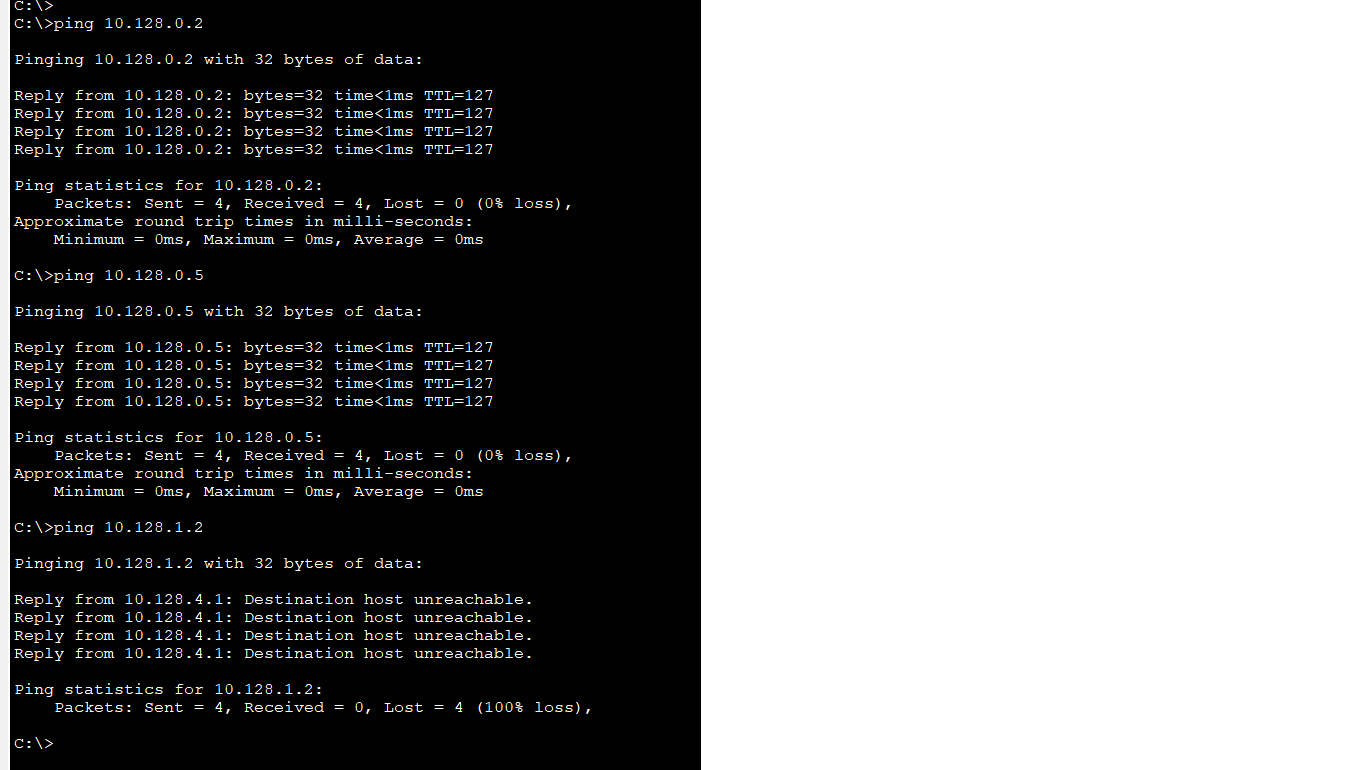


Рис. 17: Пингование с устройства dep-donskaya-vpkozlov-1

Пингование с устройства dk-donskaya-vpkozlov-1 (рис. 18)

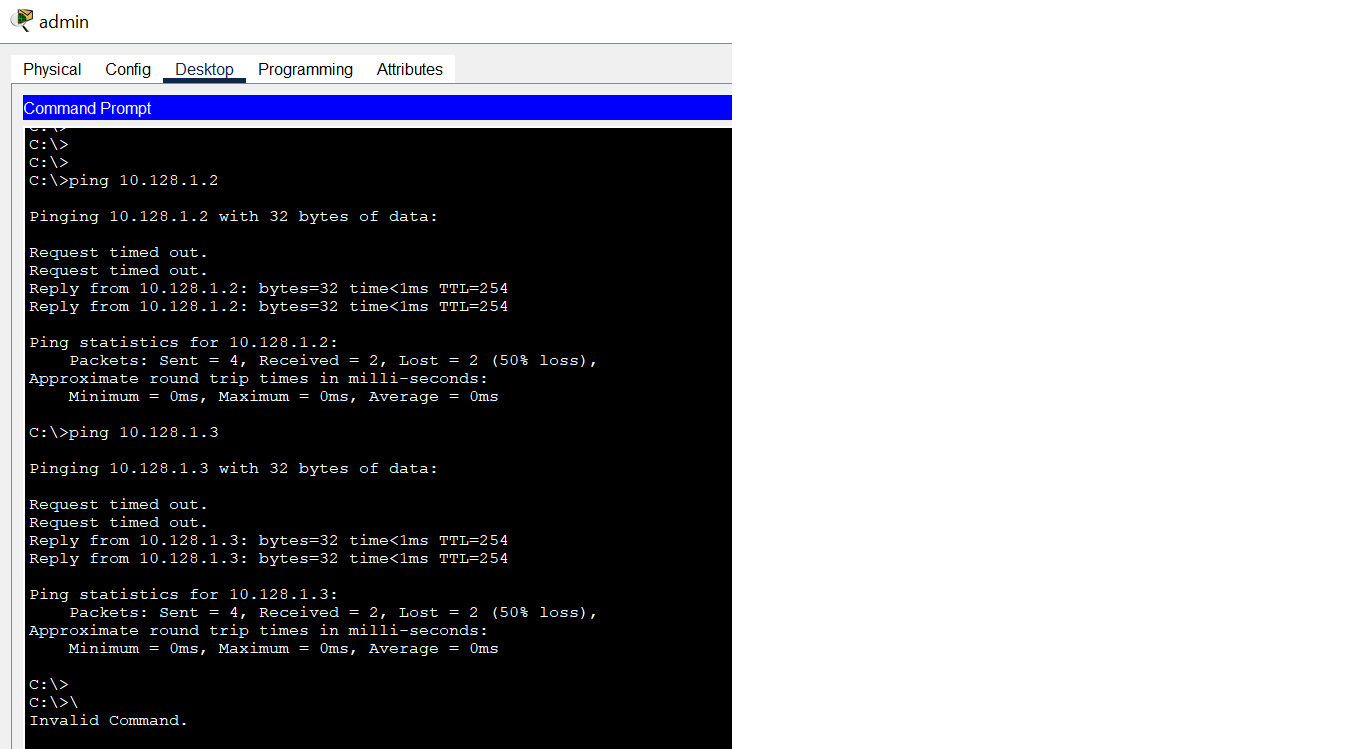


Рис. 18: Пингование с устройства dk-donskaya-vpkozlov-1

Размещение ноутбука admin на Павловской (рис. 19)

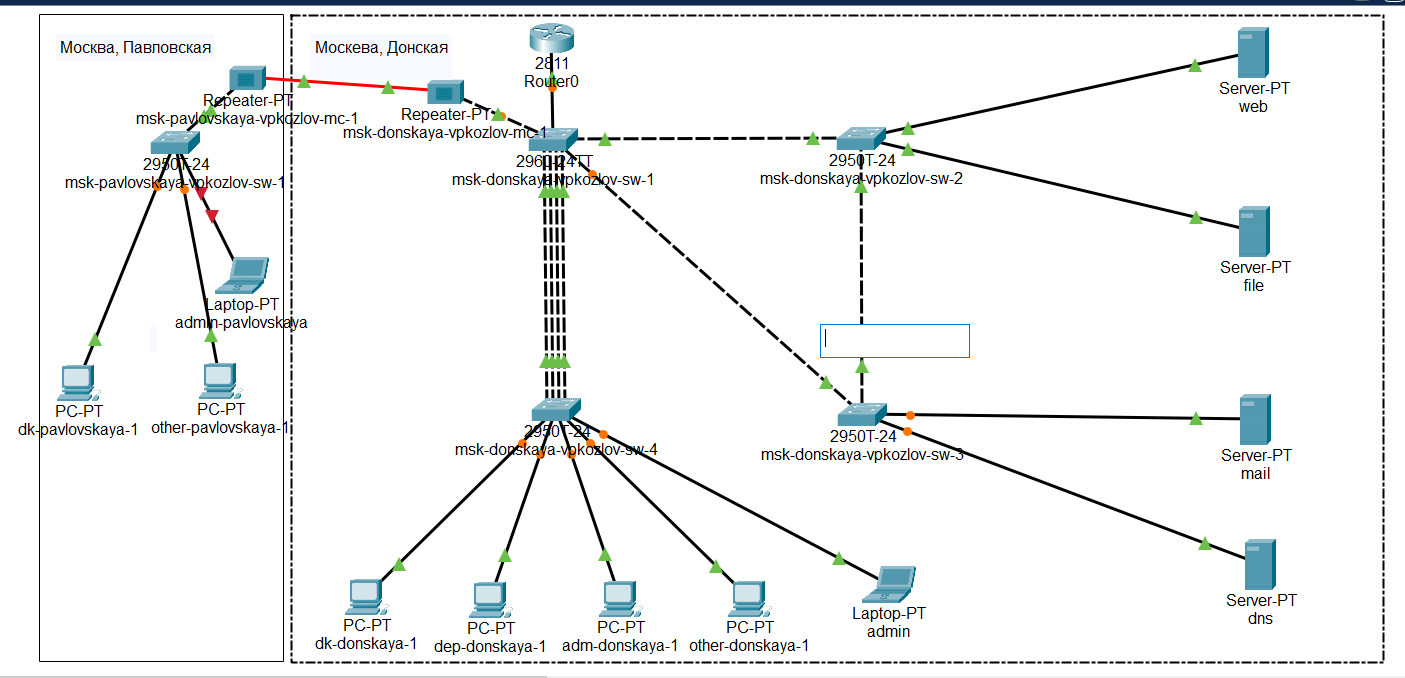


Рис. 19: Размещение ноутбука admin на Павловской

Настройка доступа для admin-pavlovskaya (рис. 20)

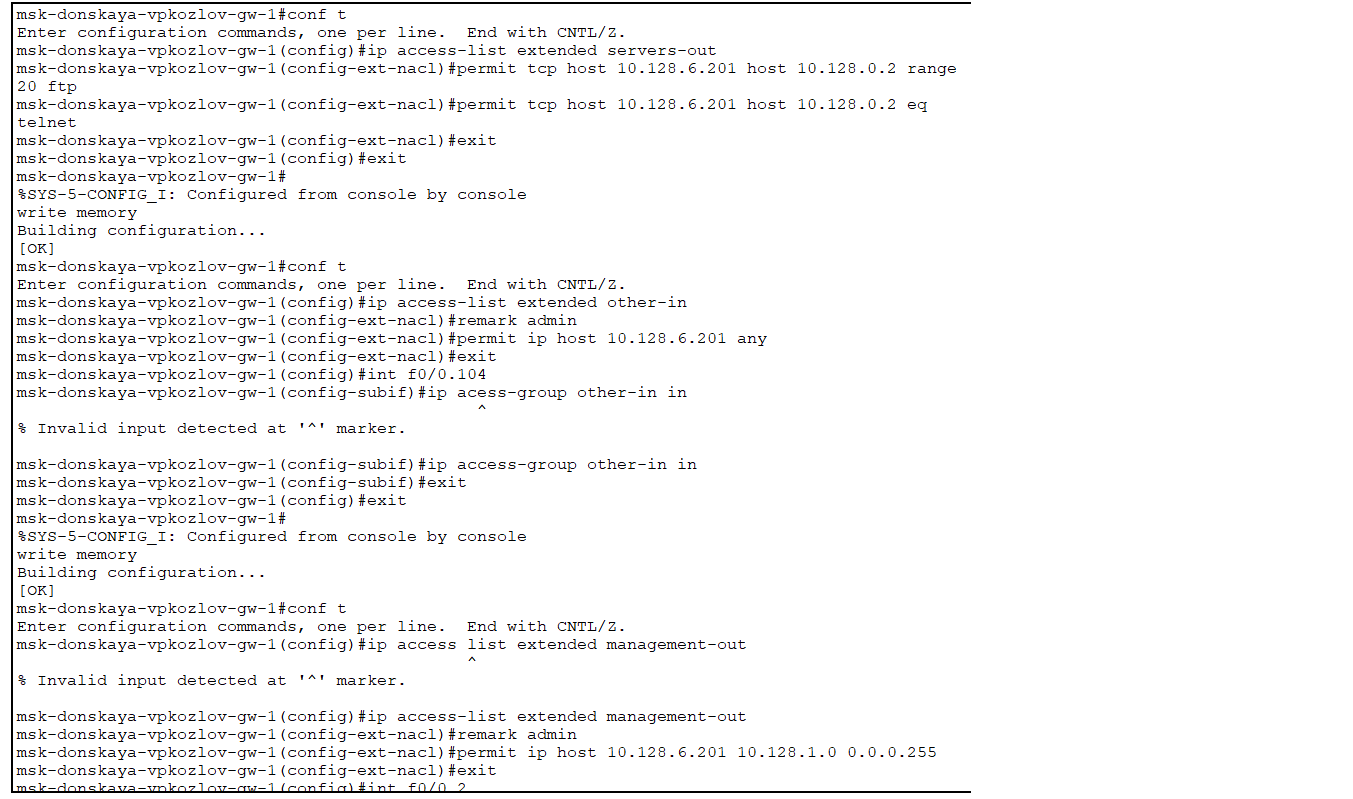


Рис. 20: Настройка доступа для admin-pavlovskaya

Список контроля доступа (рис. 21)

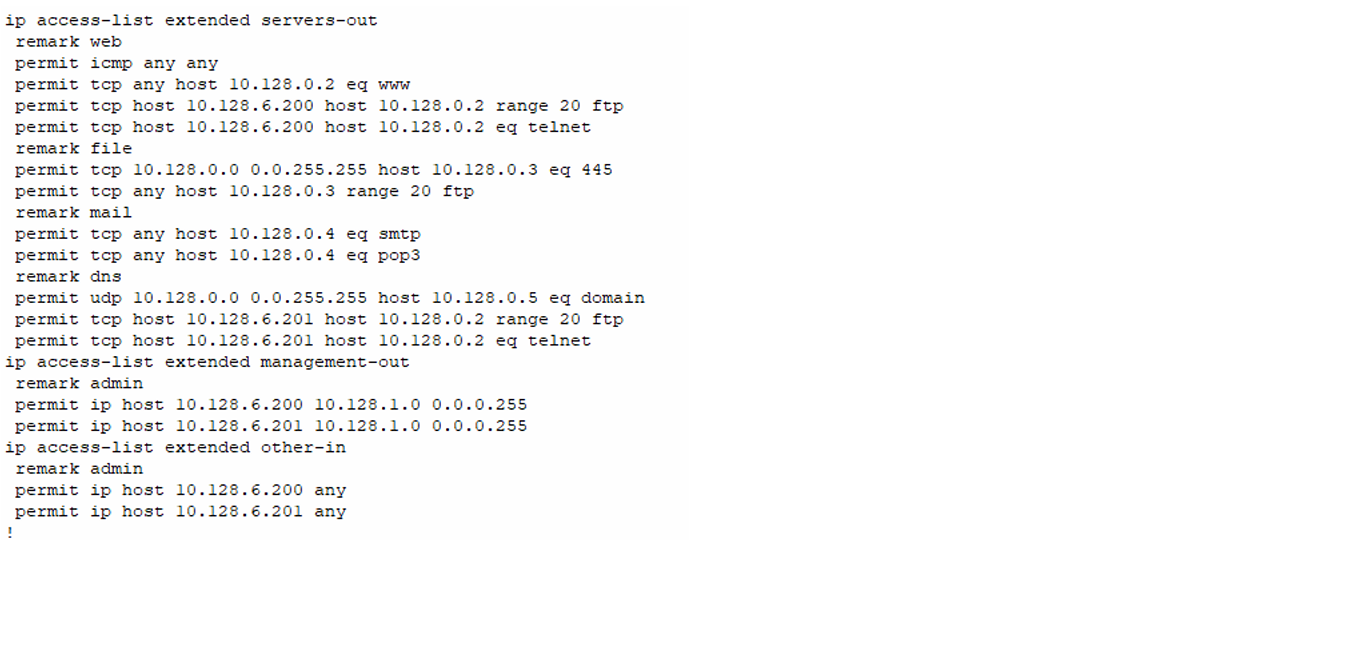


Рис. 21: Список контроля доступа

Проверка корректности настроенного доступа (рис. 22)

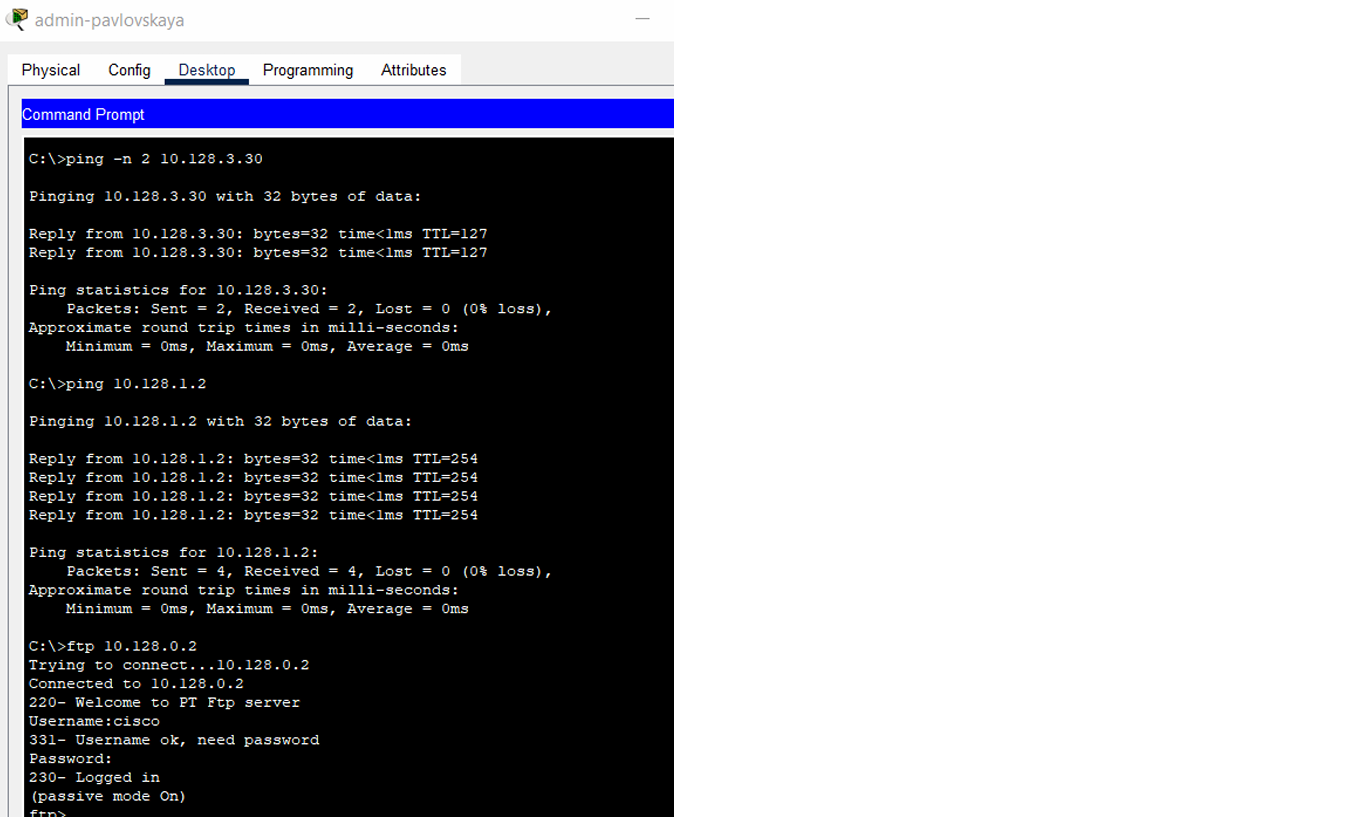


Рис. 22: Проверка корректности настроенного доступа

# 5 Выводы

Освоил настройку прав доступа пользователей к ресурсам сети

# 6 Контрольные вопросы

1. Как задать действие правила для конкретного протокола?

Например, permit tcp any host 10.128.0.4 eq pop3.

1. Как задать действие правила сразу для нескольких портов?

Для этого нужна команда interface range.

1. Как узнать номер правила в списке прав доступа?

С помощью команды show access-lists.

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

Команда access-list <номер в списке> permit.

# 7 Список литературы

1. 802.1D-2004 - IEEE Standard for Local and Metropolitan Area Networks. Media Access Control (MAC) Bridges : тех. отч. / IEEE. — 2004. — С. 1—
2. — DOI: 10.1109/IEEESTD.2004.94569. — URL: http://ieeexplore. ieee.org/servlet/opac?punumber=9155.
3. 802.1Q - Virtual LANs. — URL: http://www.ieee802.org/1/pages/802. 1Q.html.
4. A J. Packet Tracer Network Simulator. — Packt Publishing, 2014. — ISBN 9781782170426. — URL: https://books.google.com/books?id= eVOcAgAAQBAJ&dq=cisco+packet+tracer&hl=es&source=gbs\_navlinks\_
5. Cotton M., Vegoda L. Special Use IPv4 Addresses : RFC / RFC Editor. — 01.2010. — С. 1—11. — № 5735. — DOI: 10.17487/rfc5735. — URL: https: //www.rfc-editor.org/info/rfc5735.
6. Droms R. Dynamic Host Configuration Protocol : RFC / RFC Editor. — 03.1997. — С. 1—45. — № 2136. — DOI: 10.17487/rfc2131. — URL: https: //www.ietf.org/rfc/rfc2131.txt%20https://www.rfc-editor.org/ info/rfc2131.
7. McPherson D., Dykes B. VLAN Aggregation for Efficient IP Address Allocation, RFC 3069. — 2001. — URL: http : / / www . ietf . org / rfc / rfc3069.txt.
8. Moy J. OSPF Version 2 : RFC / RFC Editor. — 1998. — С. 244. — DOI: 10. 17487/rfc2328. — URL: https://www.rfc-editor.org/info/rfc2328.
9. NAT Order of Operation. — URL: https://www.cisco.com/c/en/us/ support/docs/ip/network-address-translation-nat/6209-5.html.
10. NAT: вопросы и ответы / Сайт поддержки продуктов и технологий компании Cisco. — URL: https://www.cisco.com/cisco/web/support/ RU/9/92/92029\_nat-faq.html.
11. Neumann J. C. Cisco Routers for the Small Business A Practical Guide for IT Professionals. — Apress, 2009.