Администрирование локальных сетей

Лабораторная работа №10

Скандарова Полина Юрьевна

Содержание

[Цель работы 1](#_Toc195923378)

[Выполнение лабораторной работы 1](#_Toc195923379)

[Самостоятельная работа 4](#_Toc195923380)

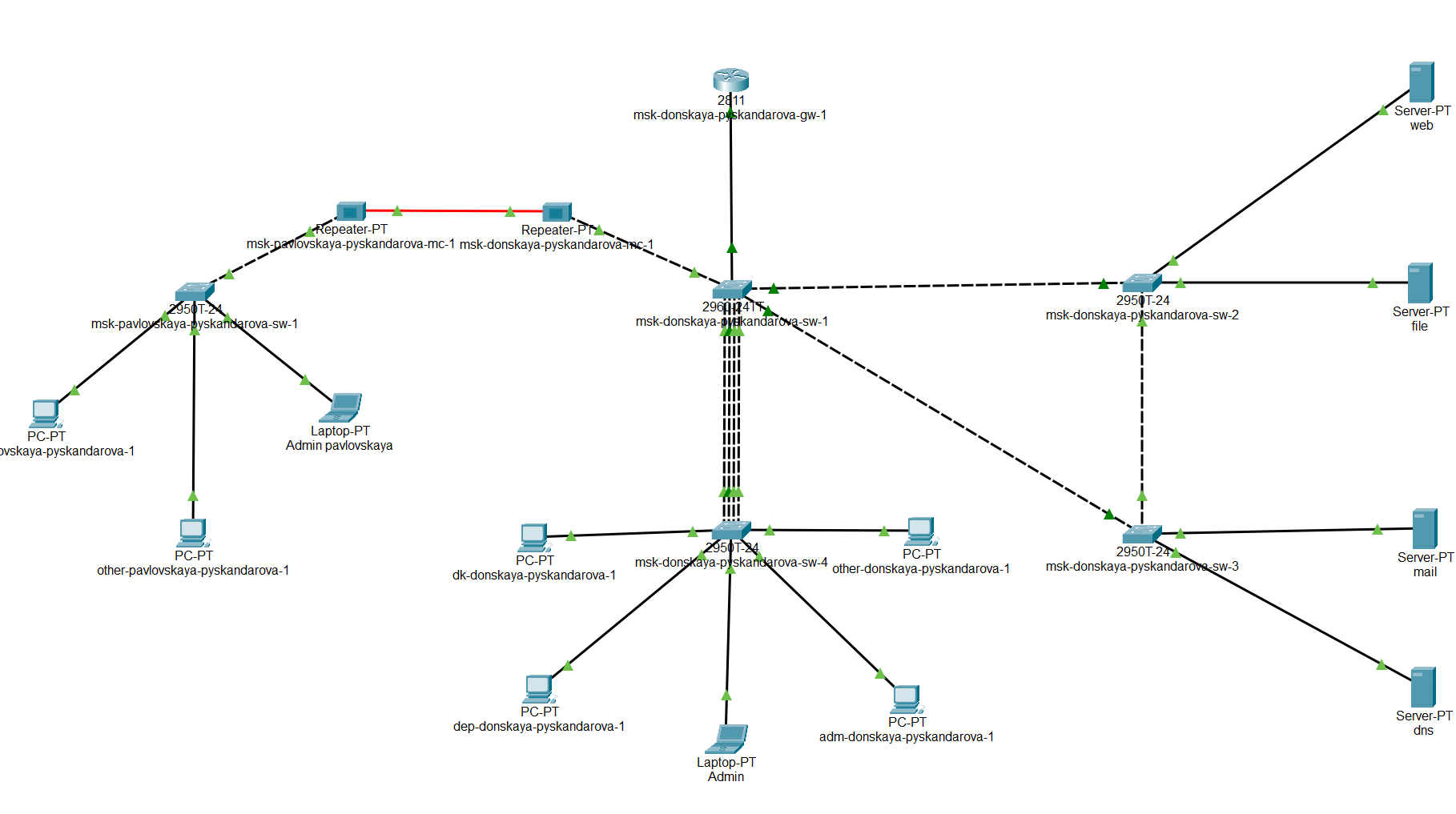
[Выводы 5](#_Toc195923381)

# Цель работы

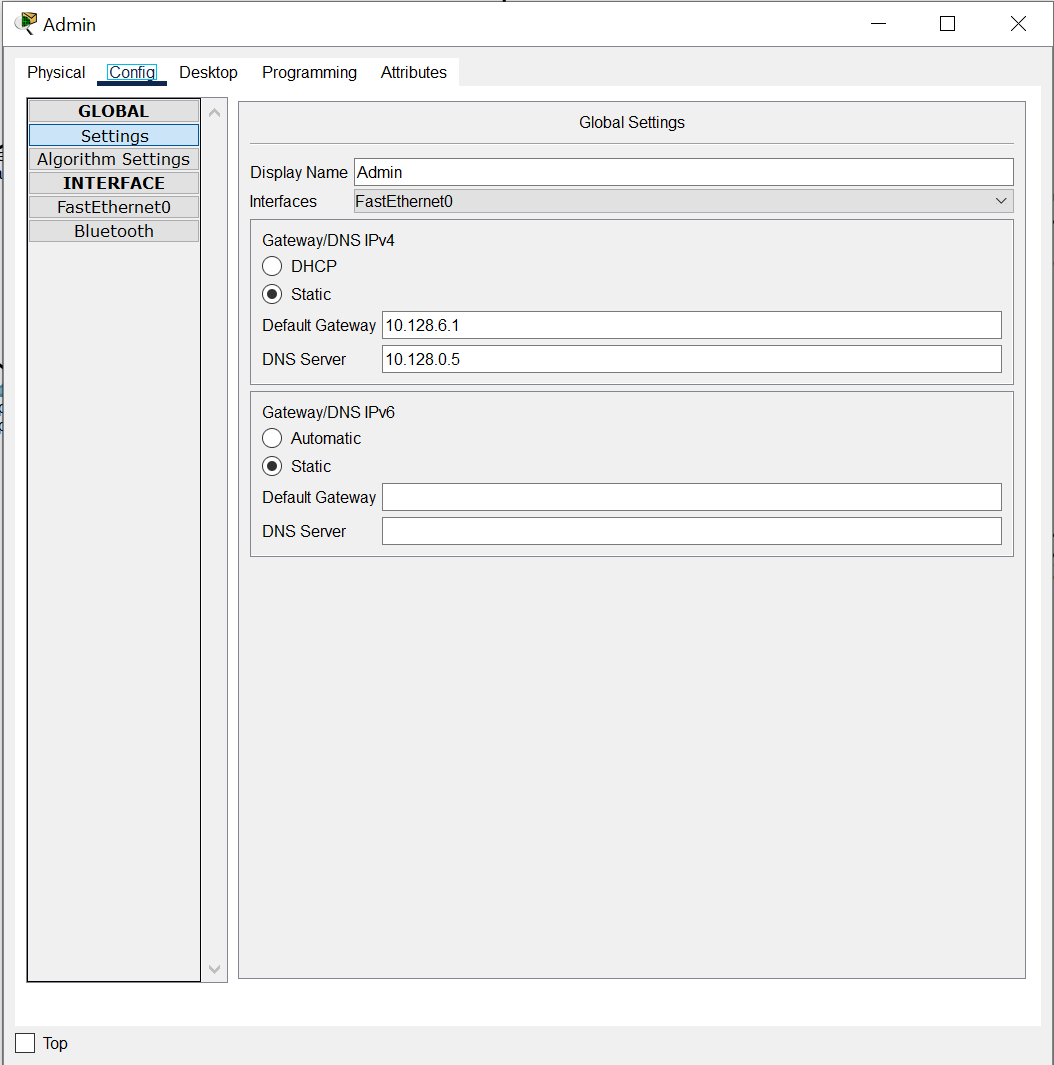
Освоить настройку прав доступа пользователей к ресурсам сети.

# Выполнение лабораторной работы

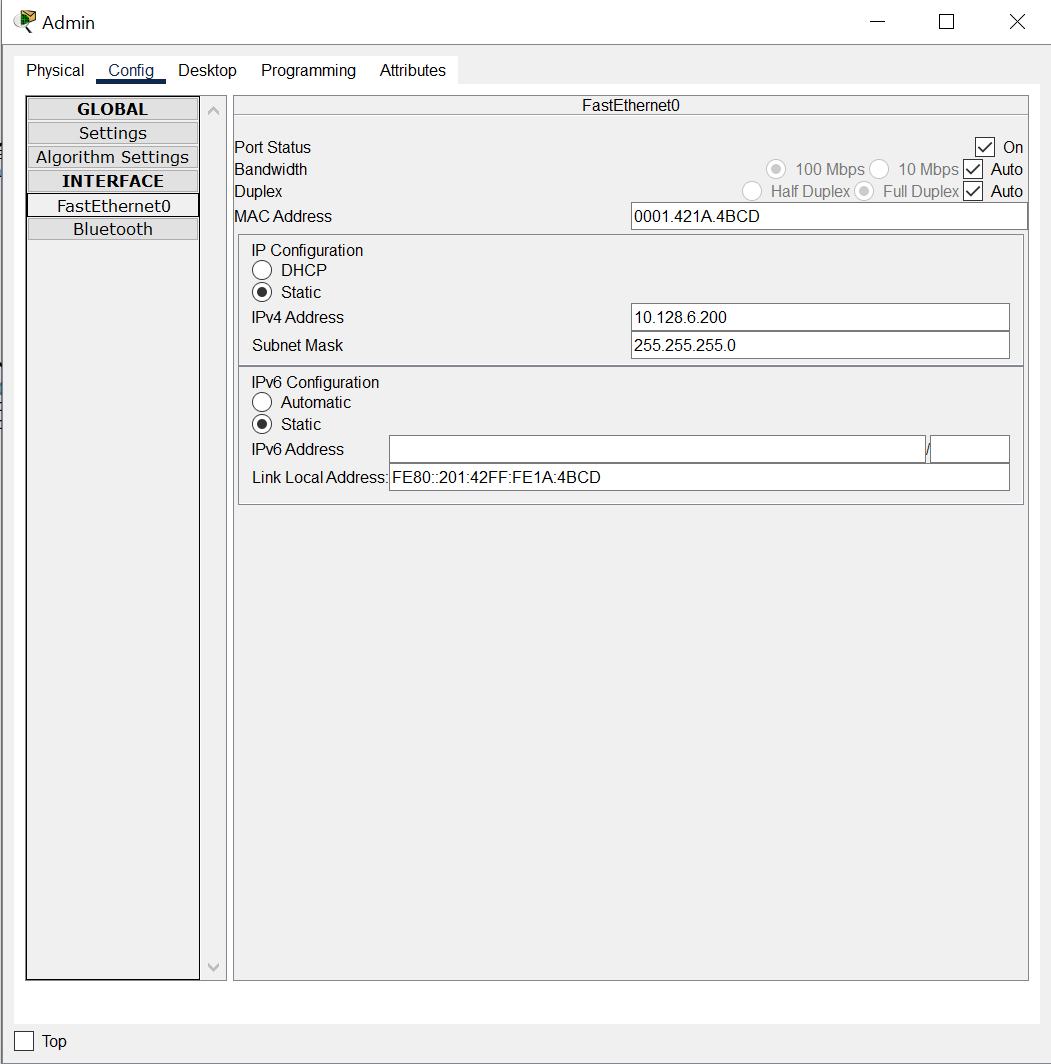
В рабочей области проекта подключаю ноутбук администратора с именем admin к сети к other-donskaya-1 с тем, чтобы разрешить ему потом любые действия, связанные с управлением сетью. (рис. [-@fig:001]) Для этого подсоединяю ноутбук к порту 24 коммутатора msk-donskaya-sw-4 и присваиваю ему статический адрес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



*Добавленные DNS и gateway адреса*

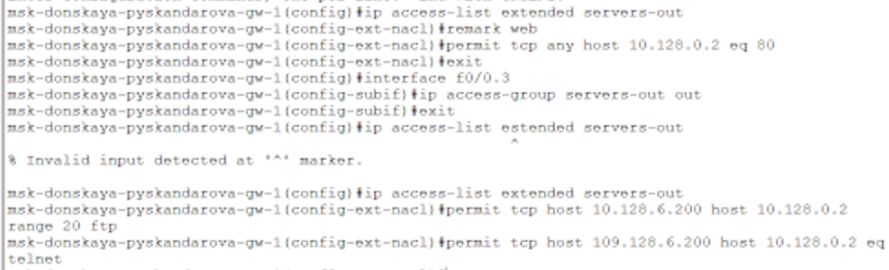


*Добавленный статический IP-адрес*

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).

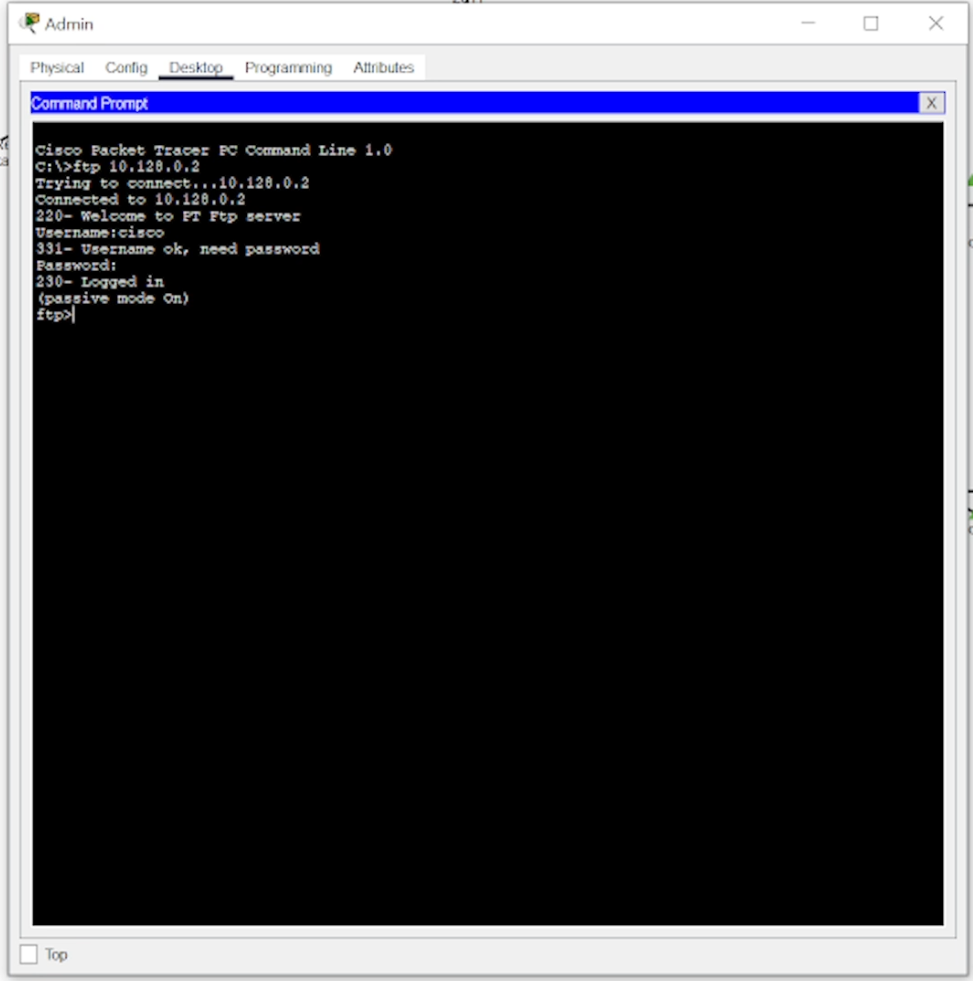
Настройка доступа к web-серверу по порту tcp 80: msk −donskaya −gw −1# configure terminal msk −donskaya −gw −1( config )#ip access −list extended servers −out msk −donskaya −gw −1( config −ext −nacl)# remark web msk −donskaya −gw −1( config −ext −nacl)# permit tcp any host 10.128.0.2 eq 80 Здесь: создан 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



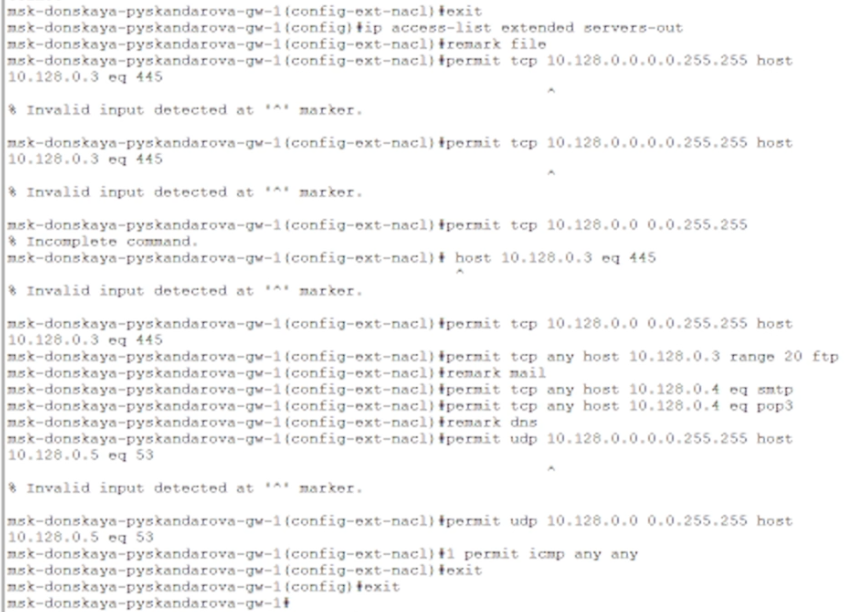
Создание списка контроля доступа с названием servers-out, подключение список прав доступа servers-out к интерфейсу f0/0.3 и применение к исходящему трафику (out), добавление правила, разрешающего устройству администратора с ip-адресом 10.128.6.200 доступ на web-сервер (10.128.0.2) по протоколам FTP и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



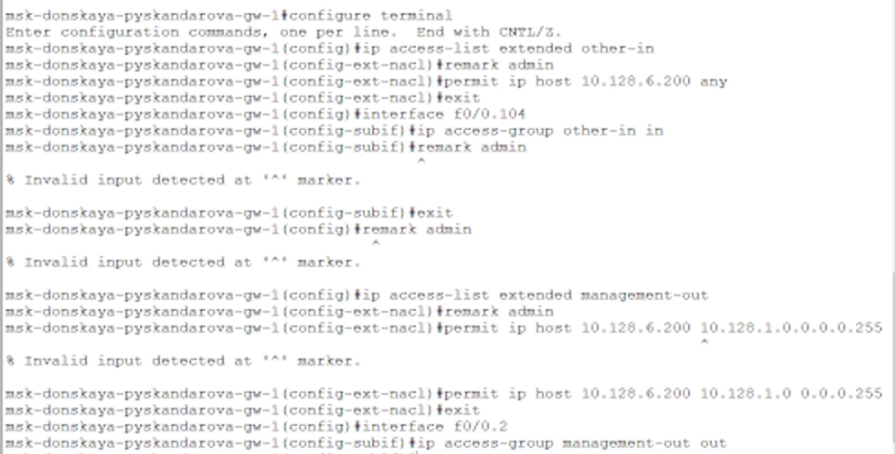
Всем узлам внутренней сети (10.128.0.0) разрешён доступ по протоколу SMB (работает через порт 445 протокола TCP) к каталогам общего пользования, любым узлам разрешён доступ к file-серверу по протоколу FTP, всем разрешён доступ к почтовому серверу по протоколам POP3 и SMTP, правило разрешения для icmp-запросов 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])



Применение команды msk−donskaya−gw−1# show access−lists

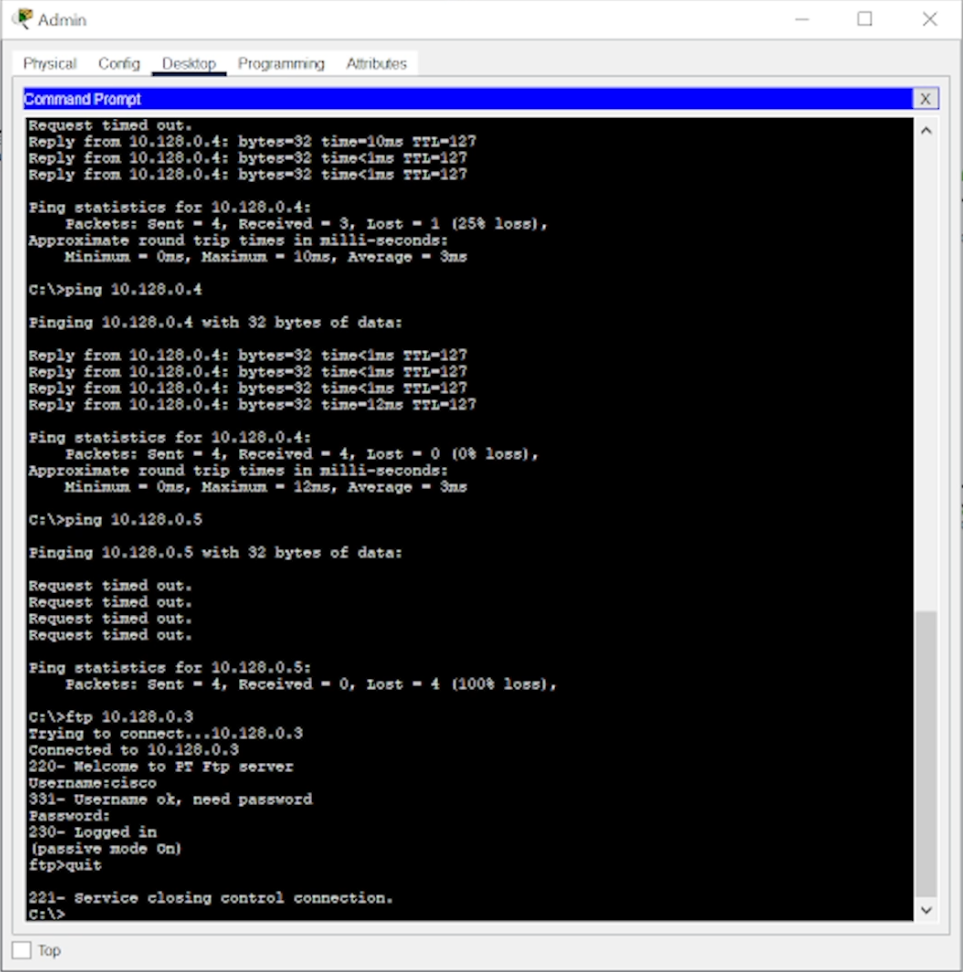
Настройка доступа для сети Other (требуется наложить ограничение на исходящий из сети Other трафик, который по отношению к маршрутизатору msk-donskaya-gw-1 является входящим трафиком): msk −donskaya −gw −1# configure terminal msk −donskaya −gw −1( config )#ip access −list extended other −in msk −donskaya −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 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]).



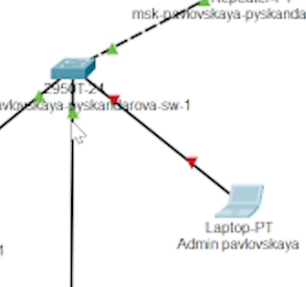
Даётся разрешение устройству с адресом 10.128.6.200 на любые действия (any), к интерфейсу f0/0.104 подключается список прав доступа other-in и применяется к входящему трафику (in), устройству администратора с адресом 10.128.6.200 разрешён доступ к сети сетевого оборудования (10.128.1.0), к интерфейсу f0/0.2 подключается список прав доступа management-out и применяется к исходящему трафику (out)

# Самостоятельная работа

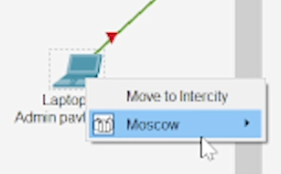
Проверяю корректность установленных правил доступа, попытавшись получить доступ по различным протоколам с разных устройств сети к подсети серверов и подсети сетевого оборудования (рис. [-@fig:009]).

Проверка доступа к разным серверам с устройства администратора

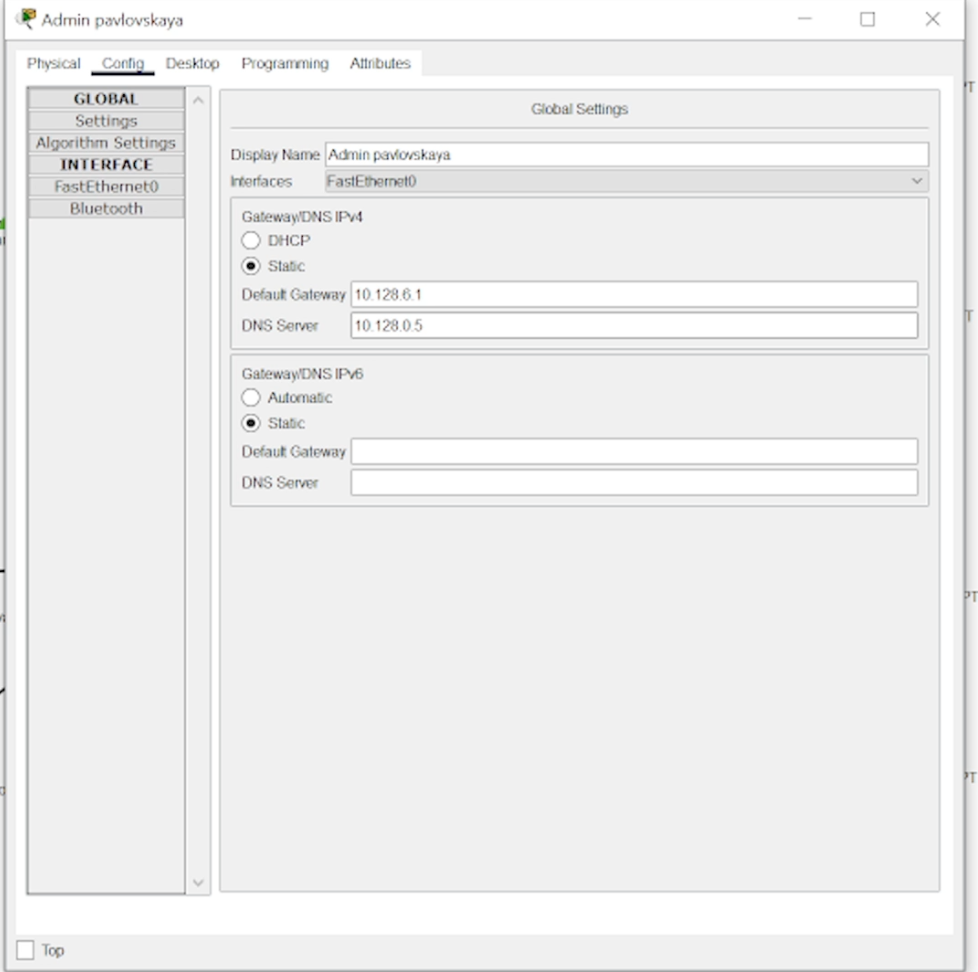
Разрешите администратору из сети Other на Павловской действия, аналогичные действиям администратора сети Other на Донской. При дополнении схемы ноутбуком администратора на Павловской у меня сначала произошли трудности с соединением, но я исправила их, перенеся ноутбук с Донской, где он сначала появился, 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])

**

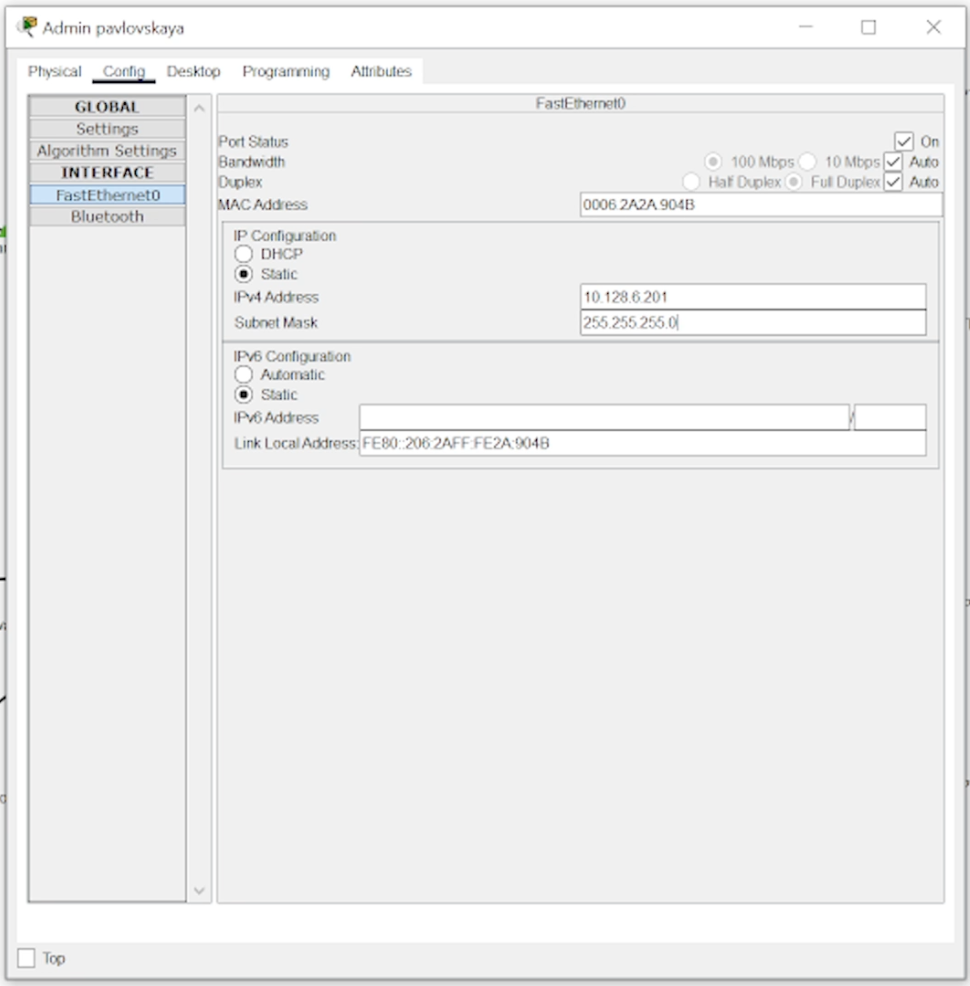
Проблемы с доступом у ноутбука



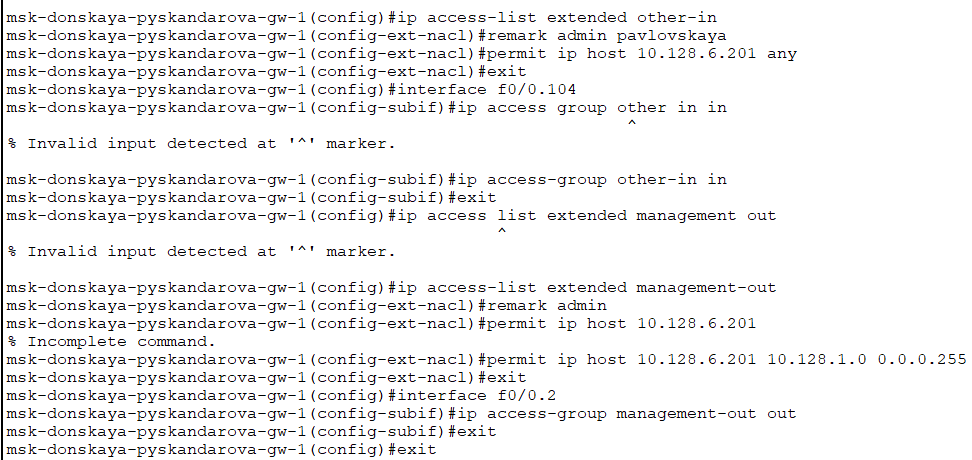
Исправление проблем с доступом



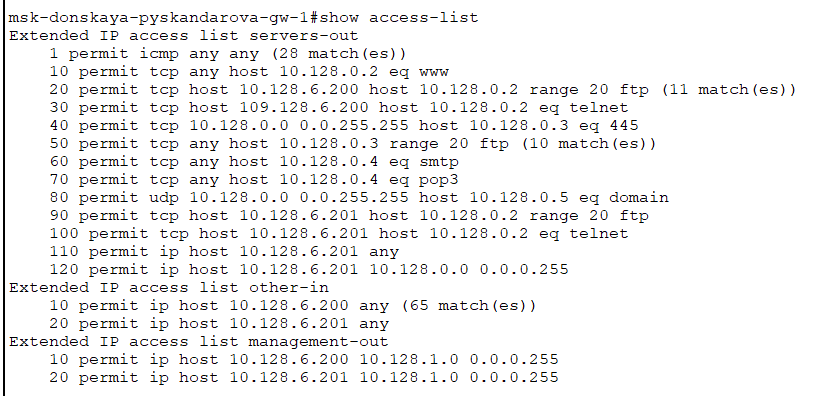
Добавленные DNS и gateway адреса



Добавленный статический IP-адрес



Настройка разрешений для ноутбука администратора на Павловской



Проверка списка разрешений

# Выводы

Освоена настройка прав доступа пользователей к ресурсам сети.