Отчёт по лабораторной работе №10

Дисциплина: Администрирование локальных сетей

Выполнил: Танрибергенов Эльдар

Содержание

# 1 Цель работы

Освоить настройку прав доступа пользователей к ресурсам сети.

# 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. Проверить правильность действия установленных правил доступа.
3. Выполнить задание для самостоятельной работы по настройке прав доступа администратора сети на Павловской.

# 3 Выполнение лабораторной работы

1. В рабочей области проекта подсоединил ноутбук к порту 24 коммутатора msk-donskaya-sw-4 (рис. 1) и присвоил ему статический адрес 10.128.6.200 (рис. 2), указав в качестве gateway-адреса 10.128.6.1 и адреса DNS-сервера 10.128.0.5 (рис. 3).

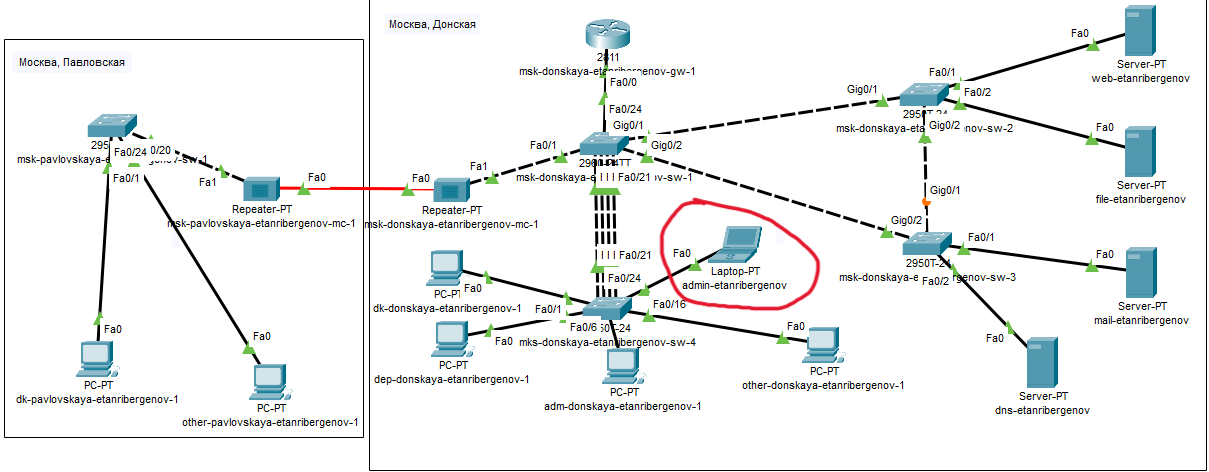


Рис. 1: Размещение ноутбука администратора в сети other-donskaya-1

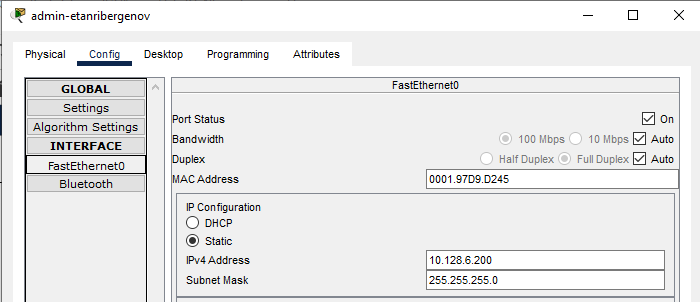


Рис. 2: Присвоение статического ip-адреса ноутбука

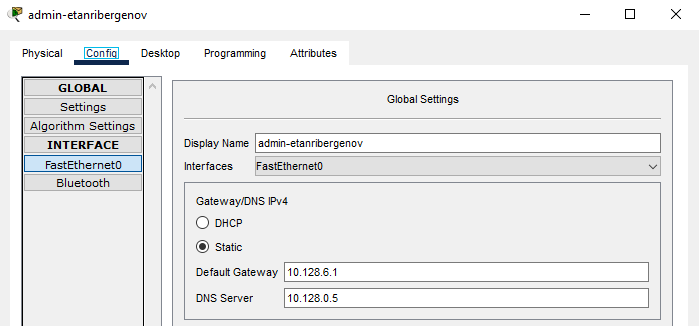


Рис. 3: Указание адресов шлюза и DNS-сервера

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

Создал список контроля доступа с названием servers-out (так как предполагается ограничить доступ в конкретные подсети и по отношению к маршрутизатору это будет исходящий трафик); указал (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.

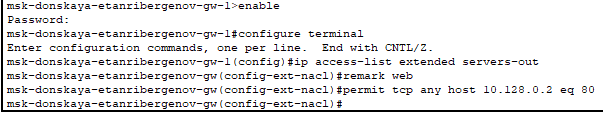


Рис. 4: Настройка доступа к web-серверу по порту http (tcp 80)

1. Добавление списка управления доступом к интерфейсу:

К интерфейсу f0/0.3 подключил список прав доступа servers-out и применил к исходящему трафику (out) (рис. 5). Проверил, что доступ к web-серверу есть через протокол HTTP (введя в строке браузера хоста ip-адрес web-сервера) (рис. 6). При этом команда ping демонстрирует недоступность web-сервера как по имени, так и по ip-адресу web-сервера (рис. 7).

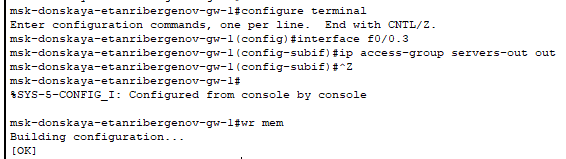


Рис. 5: Подключение списка прав доступа к интерфейсу и применение к исходящему трафику

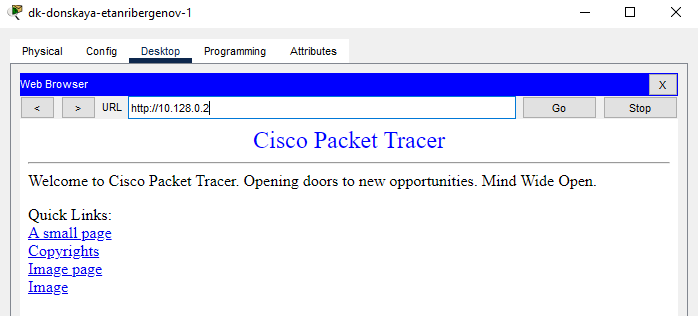


Рис. 6: Проверка доступа к web-серверу через протокол HTTP

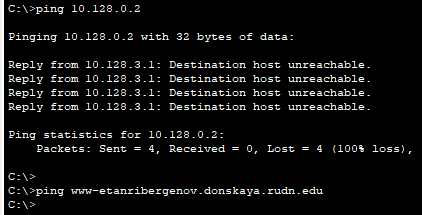


Рис. 7: Проверка недоступности web-сервера по команде ping

1. Дополнительный доступ для администратора по протоколам Telnet и FTP:

В список контроля доступа servers-out добавил 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. 8). Убедился, что с узла с ip-адресом 10.128.6.200 есть доступ по протоколу FTP. Для этого в командной строке устройства администратора ввёл ftp 10.128.0.2, а затем по запросу имя пользователя cisco и пароль cisco (рис. 9).

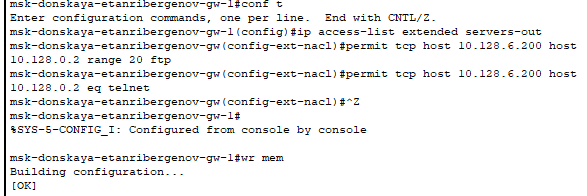


Рис. 8: Добавление разрешения устройству администратору на доступ на web-сервер по протоколам FTP и telnet

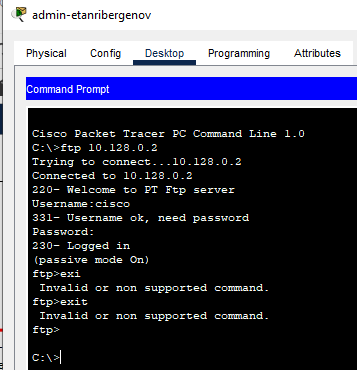


Рис. 9: Проверка доступа администратора к web-серверу по протоколу FTP

Попробовал провести аналогичную процедуру с другого устройства сети. Убедился, что доступ запрещён.

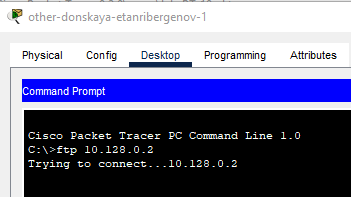


Рис. 10: Проверка доступа другого устройства сети к web-серверу по протоколу FTP

1. Настройка доступа к файловому серверу:

В списке контроля доступа servers-out указал (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).

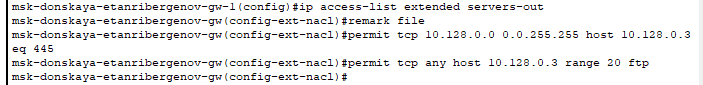


Рис. 11: Настройка доступа к файловому серверу

1. Настройка доступа к почтовому серверу:

В списке контроля доступа servers-out указал (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.

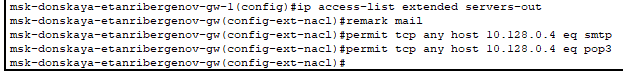


Рис. 12: Настройка доступа к почтовому серверу

1. Настройка доступа к DNS-серверу:

В списке контроля доступа servers-out указал (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 (рис. 13). Проверил доступность web-сервера (через браузер) по имени (рис. 14).

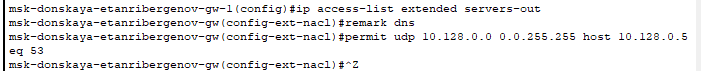


Рис. 13: Настройка доступа к DNS-серверу

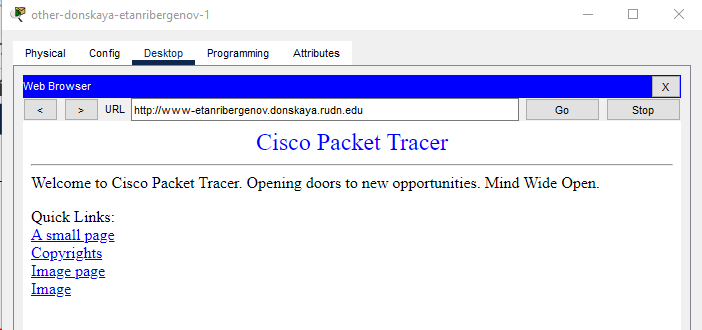


Рис. 14: Проверка доступа к DNS-серверу

1. Разрешение icmp-запросов:

Разрешение icmp-запросов всем узлам в сети

Рис. 15: Разрешение icmp-запросов всем узлам в сети

Явно указал порядок размещения правил — правило разрешения для icmp-запросов добавил в начало списка контроля доступа (рис. 16).

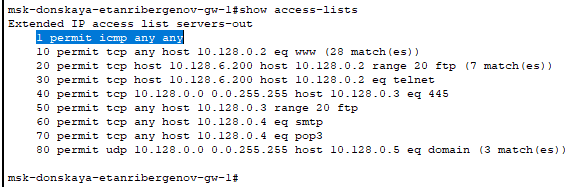


Рис. 16: Проверка размещения правила первым в списке

Проверил, что icmp-запросы доступны (рис. 17).

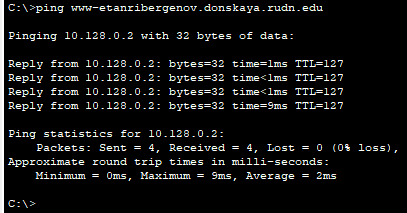


Рис. 17: Проверка доступности icmp-запросов в сети

1. Настройка доступа для сети Other (наложил ограничение на исходящий из сети Other трафик, который по отношению к маршрутизатору 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).

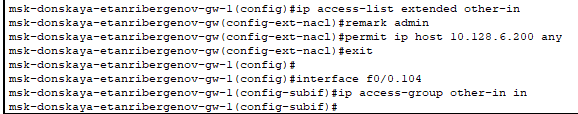


Рис. 18: Настройка доступа для сети other

1. Настройка доступа администратора к сети сетевого оборудования:

В списке контроля доступа management-out указал (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).

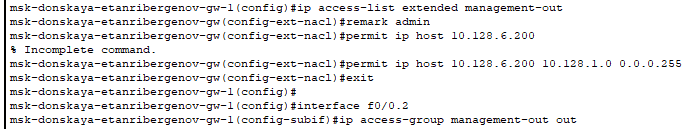


Рис. 19: Настройка доступа администратора к сети сетевого оборудования

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

Проверил правильность работы установленных правил доступа, попытавшись получить доступ с устройства из сети other. Убедился, что доступ запрещён.

К серверу:

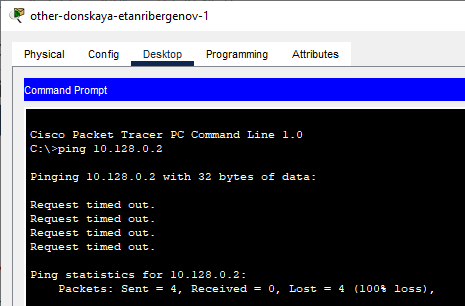


Рис. 20: Проверка доступа к web-серверу устройства из сети other

К сетевому оборудованию:

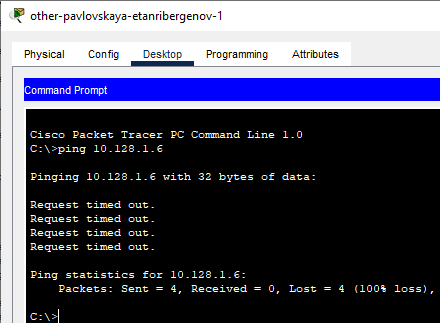


Рис. 21: Проверка доступа к сетевому оборудованию устройства из сети other

Проверил правильность работы установленных правил доступа, попытавшись получить доступ с устройства администатора. Убедился, что доступ разрешён.

К серверу:

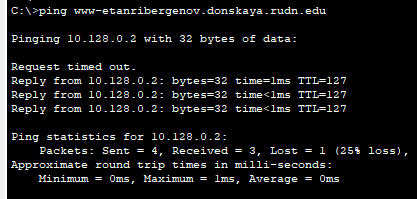


Рис. 22: Проверка доступа администратора к сети сетевого оборудования

К сетевому оборудованию:

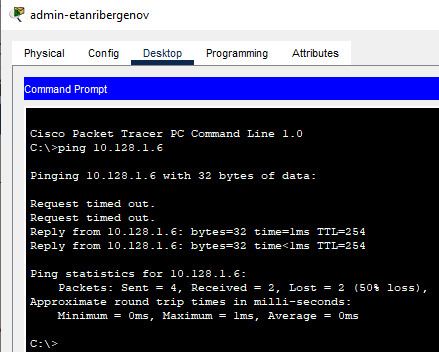


Рис. 23: Проверка доступа администратора к сети сетевого оборудования

1. Разрешил администратору из сети Other на Павловской действия, аналогичные действиям администратора сети Other на Донской.

Разместил ноутбук администратора на территории Павловская и соединил с 23 портом коммутатора msk-pavlovskaya-etanribergenov-sw-1:

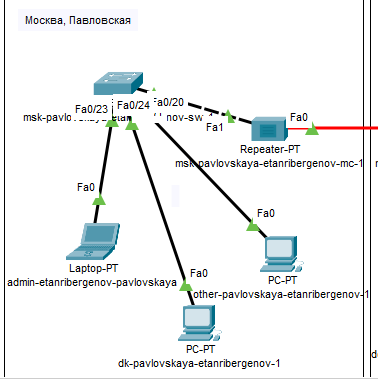


Рис. 24: Размещение ноутбука администратора на Павловской

Настроил интерфейс f0/23: задал ему принадлежность к vlan 104 (сеть other):

Настройка интерфейса коммутатора на Павловской

Рис. 25: Настройка интерфейса коммутатора на Павловской

Задал адреса шлюза и dns-сервера, а также его собственный статический ip-адрес:

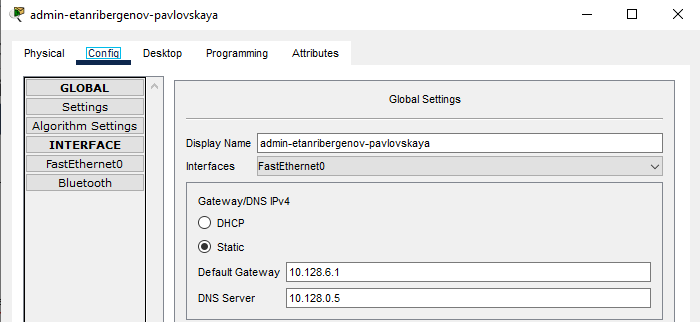


Рис. 26: IP-адреса шлюза и dns-сервера ноутбука администратора на Павловской

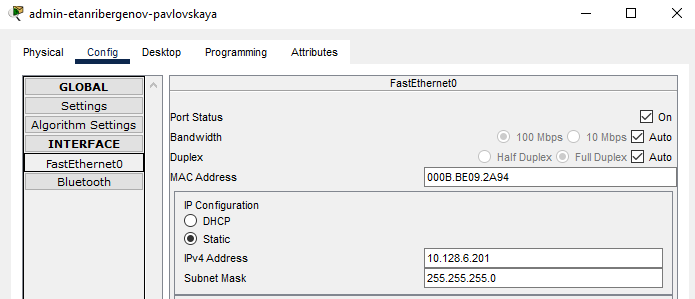


Рис. 27: IP-адрес ноутбука администратора на Павловской

Добавил правила (доступ по всем протоколам ко всем узлам сети и сетевому оборудованию) в списки доступа для узла администратора на Павловской:

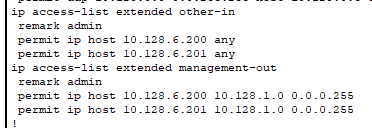


Рис. 28: Правила для администратора на Павловской в списках доступа

Проверка доступа узла администатора на Павловской к остальным узлам сети и сетевому оборудованию:

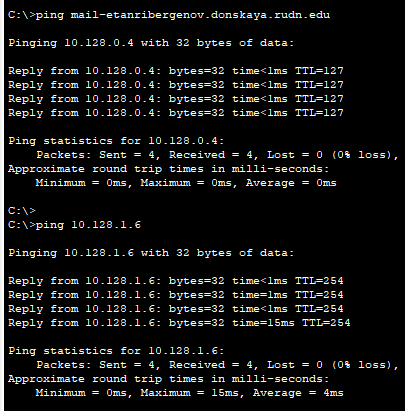


Рис. 29: Проверка правильности работы правил

# 4 Ответы на контрольные вопросы

1. Команда *permit <протокол> <кому> <куда> <порт>* задаёт правило для конкретного протокола.
2. Чтобы задать действие правила сразу для нескольких портов, можно написать сразу несколько протоколов.
3. Команда *show access-lists* выводит списки доступа с их порядковыми номерами.
4. Добавив перед правилом (перед словом permit/deny) число, можно изменить порядок применения правил в списке контроля доступа.

# 5 Выводы

Я освоил настройку прав доступа пользователей к ресурсам сети.