Отчёт по лабораторной работе №10

дисциплина: Администрирование локальных сетей

Студент: Кузнецова София Вадимовна

Содержание

# Цель работы

Изучить возможности протокола STP и его модификаций по обеспечению отказоустойчивости сети, агрегированию интерфейсов и перераспределению нагрузки между ними.

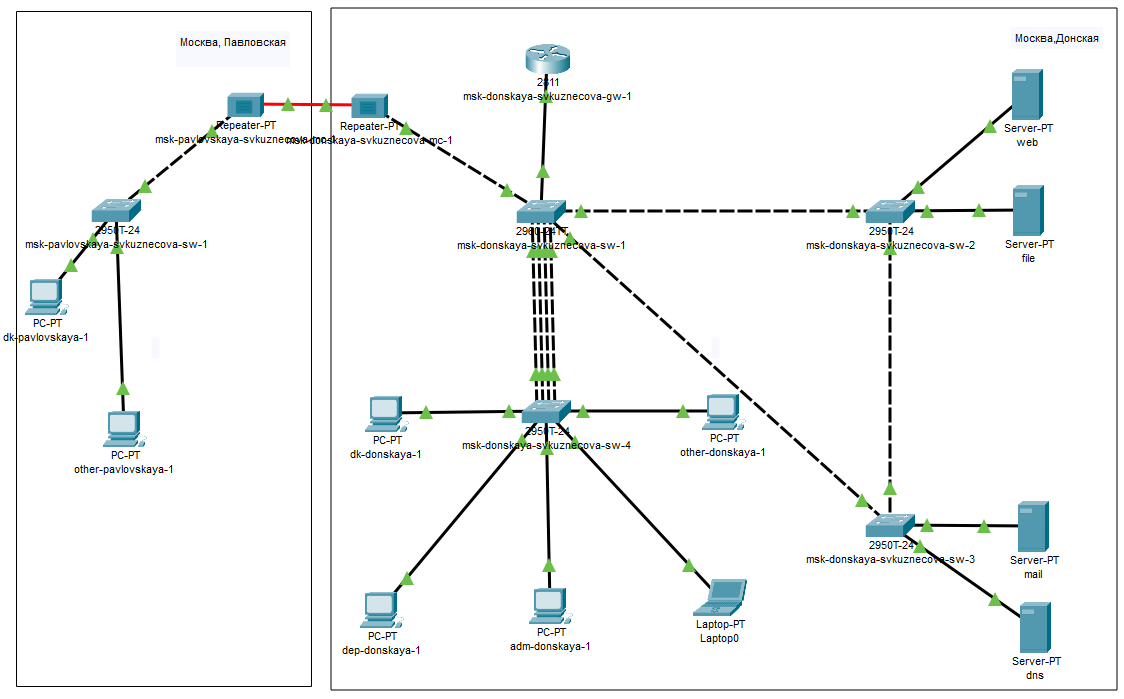
# Выполнение лабораторной работы

Откроем проект с названием lab\_PT-09.pkt и сохраним под названием lab\_PT-10.pkt. После чего откроем его для дальнейшего редактирования.

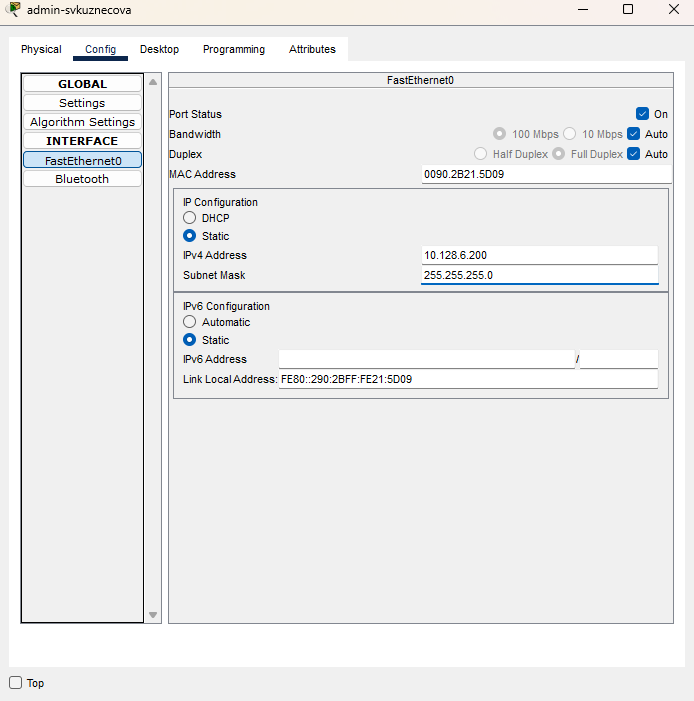
Открытие проекта lab_PT-10.pkt

Открытие проекта lab\_PT-10.pkt

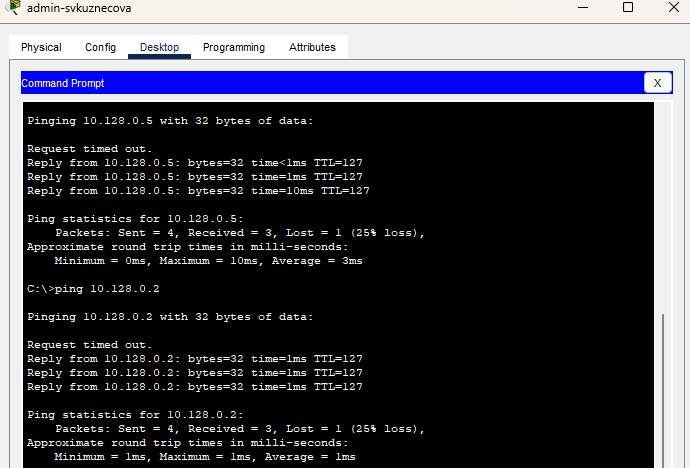
В рабочей области проекта подключим ноутбук администратора с именем admin к сети к other-donskaya-1 с тем, чтобы разрешить ему потом любые действия, связанные с управлением сетью. Для этого подсоединим ноутбук к порту 24 коммутатора msk-donskaya-svkuznecova-sw-4 и присвоим ему статический адрес 10.128.6.200, указав в качестве gateway-адреса 10.128.6.1 и адреса DNS-сервера 10.128.0.5. После чего пропингуем. Права доступа пользователей сети будем настраивать на маршрутизаторе msk- donskaya-svkuznecova-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.



Подсоединение ноутбука к порту 24 коммутатора msk-donskaya-svkuznecova-sw-4 и изменение названия

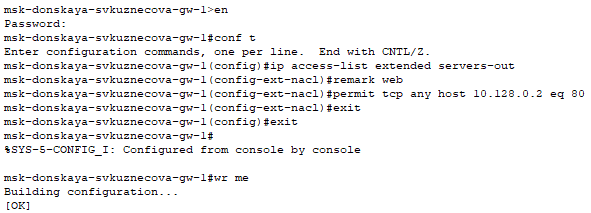


Присвоение оконечному устройству статического адреса 10.128.6.200, gateway-адреса 10.128.6.1 и адреса DNS-сервера 10.128.0.5



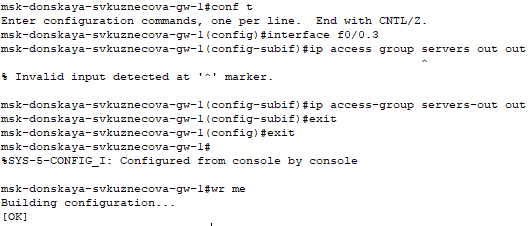
Проверка (пингуем с admin-svkuznecova 10.128.0.2 и 10.128.0.5)

Далее настроим доступ к web-серверу по порту tcp 80. Здесь: 1. Создадим список контроля доступа с названием servers-out (так как предполагается ограничить доступ в конкретные подсети и по отношению к маршрутизатору это будет исходящий трафик); 2. Укажем (в качестве комментария-напоминания remark web), что ограничения предназначены для работы с web-сервером; 3. Дадим 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.

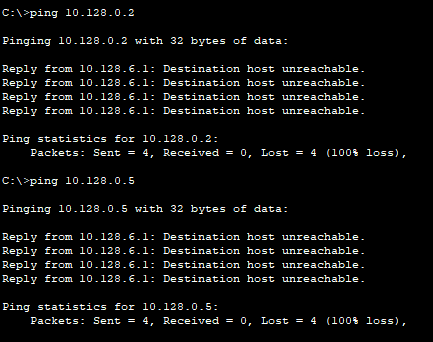


Настройка доступа к web-серверу по порту tcp 80

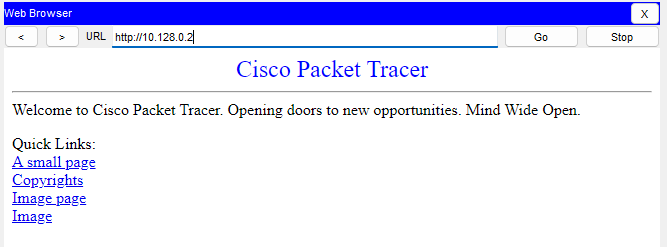
Добавление списка управления доступом к интерфейсу. Здесь: - К интерфейсу f0/0.3 подключаем список прав доступа serversout и примяем к исходящему трафику (out). Проверим, что доступ к web-серверу есть через протокол HTTP (введя в строке браузера хоста ip-адрес web-сервера). При этом команда ping будет демонстрировать недоступность web-сервера как по имени, так и по ip-адресу web-сервера.



Добавление списка управления доступом к интерфейсу

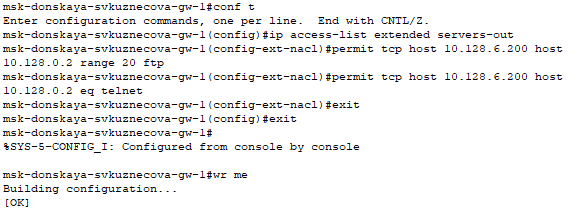


Проверка демонстрации недоступности web-сервера как по имени, так и по ip-адресу web-сервера.

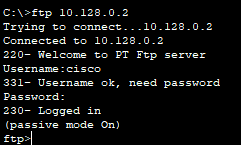


Проверка доступа к web-серверу есть через протокол HTTP (введя в строке браузера хоста ip-адрес web-сервера)

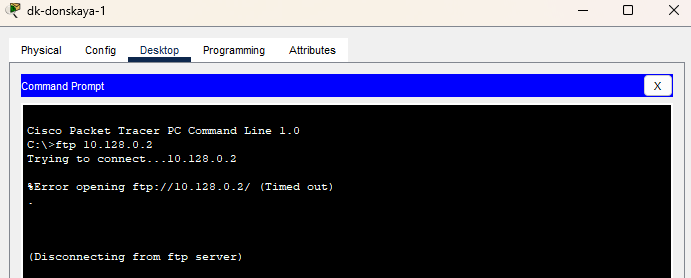
Настроим дополнительный доступ для администратора по протоколам Telnet и FTP. Здесь: - В список контроля доступа servers-out добавим правило, разрешающее устройству администратора с ip-адресом 10.128.6.200 доступ на web-сервер (10.128.0.2) по протоколам FTP и telnet. Убедимся, что с узла с ip-адресом 10.128.6.200 есть доступ по протоколу FTP. Для этого в командной строке устройства администратора введём ftp 10.128.0.2, а затем по запросу имя пользователя cisco и пароль cisco. Попробуем провести аналогичную процедуру с другого устройства сети. Попробуем убедиться, что доступ будет запрещён.



Настроим дополнительный доступ для администратора по протоколам Telnet и FTP

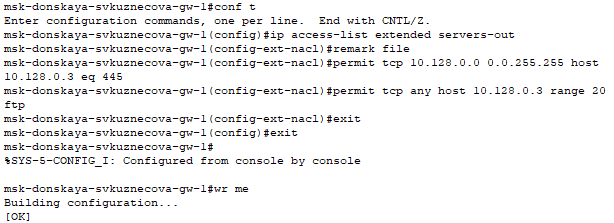


Проверка доступа с узла 10.128.6.200 по протоколу FЕP



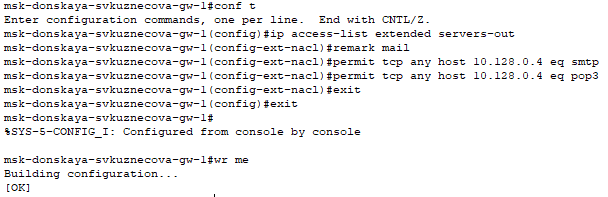
Проверка доступа с устройства dk-donskaya-1 по протоколу FTP (доступ запрещён)

Настроим доступа к файловому серверу. Здесь: 1. В списке контроля доступа servers-out укажем (в качестве комментария-напоминания remark file), что следующие ограничения предназначены для работы с file-сервером; 2. Всем узлам внутренней сети (10.128.0.0) разрешим доступ по протоколу SMB (работает через порт 445 протокола TCP) к каталогам общего пользования; 3. Любым узлам разрешим доступ к file-серверу по протоколу FTP. Запись 0.0.255.255 — обратная маска (wildcard mask).



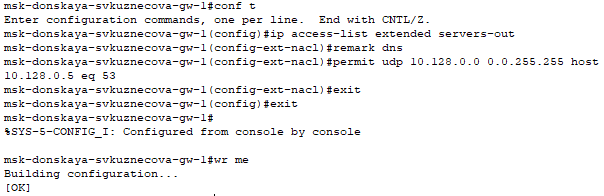
Настройка доступа к файловому серверу

Теперь настроим доступа к почтовому серверу. Здесь: 1. В списке контроля доступа servers-out укажем (в качестве комментария-напоминания remark mail), что следующие ограничения предназначены для работы с почтовым сервером; 2. Всем разрешим доступ к почтовому серверу по протоколам POP3 и SMTP.

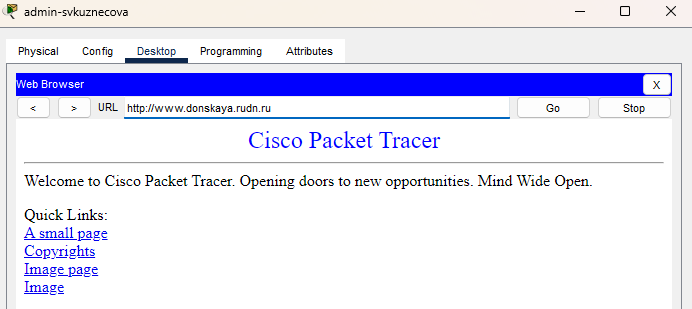


Настройка доступа к почтовому серверу

Настройим доступа к DNS-серверу. Здесь: 1. В списке контроля доступа servers-out укажем (в качестве комментария-напоминания remark dns), что следующие ограничения пред назначены для работы с DNS-сервером; 2. Всем узлам внутренней сети разрешим доступ к DNS-серверу через UDP-порт 53.

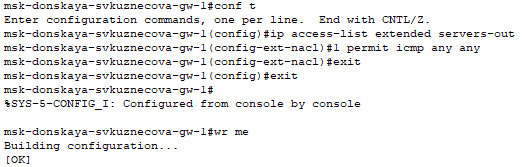


Настройка доступа к DNS-серверу

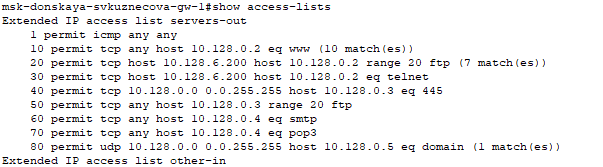


Проверка доступности web-сервера(через браузер) по имени

Разрешим icmp-запросов. Здесь: - Демонстрируем явное управление порядком размещения правил правило разрешения для icmp-запросов добавляется в начало списка контроля доступа. Посмотрим номера строк правил в списке контроля доступа.

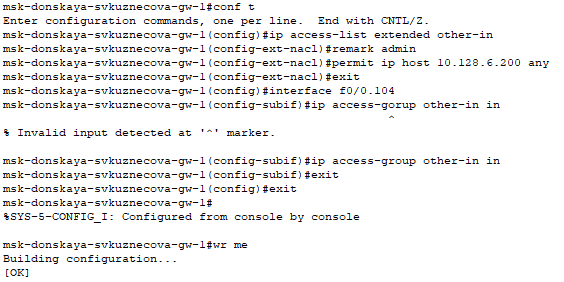


Разрешим icmp-запросов



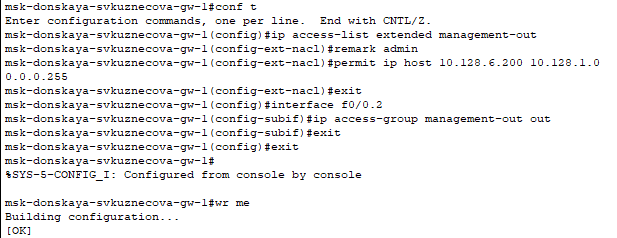
Просмотр номеров строк правил в списке контроля доступа

Теперь настроим 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): 1. В списке контроля доступа other-in укажем, что следующие правила относятся к администратору сети; 2. Даём разрешение устройству с адресом 10.128.6.200 на любые действия (any); 3. К интерфейсу f0/0.104 подключаем список прав доступа other-in и применяеем к входящему трафику (in).



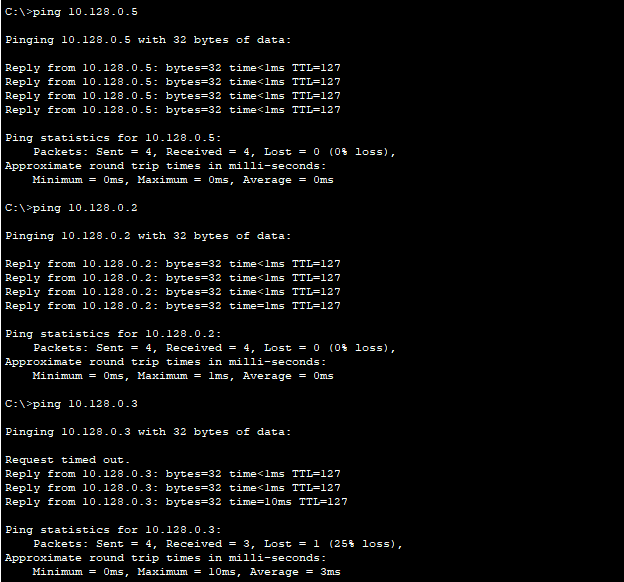
Настройка доступа для сети Other

Настроим доступ администратора к сети сетевого оборудования.Здесь: 1. 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); 2. К интерфейсу f0/0.2 подключаем список прав доступа management-out и применяем к исходящему трафику (out).

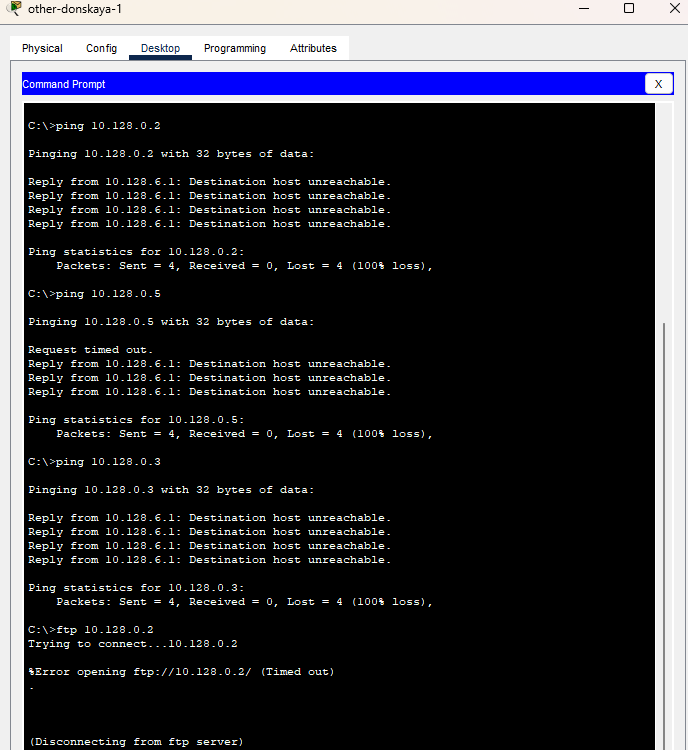


Настройка доступа администратора к сети сетевого оборудования

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

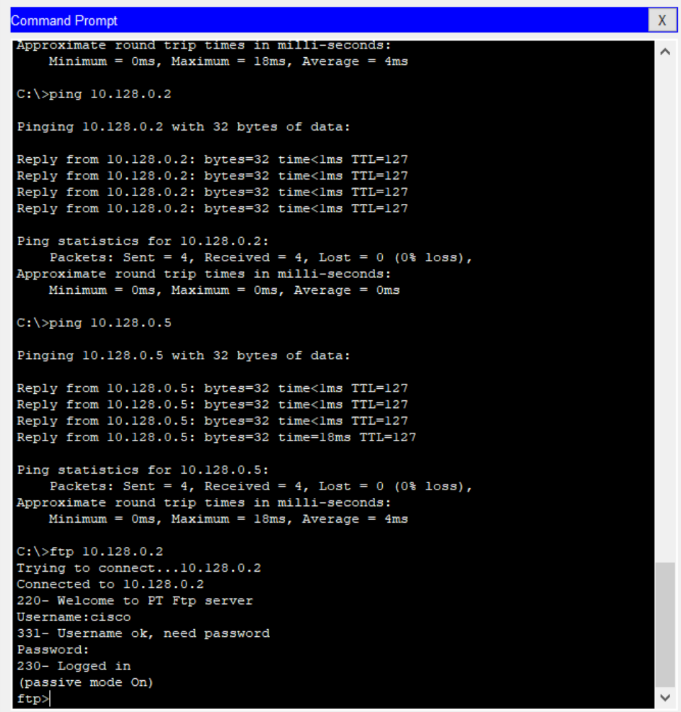


Проверка корректности установленных правил доступа с оконечного устройства admin-svkuznecova.



Проверка корректности установленных правил доступа с оконечного устройства other-donskaya-1.

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



Проверка разрешений администратора из сети Other на Павловской.

# Выводы

В ходе выполнения лабораторной работы мы освоили настройку прав доступа польНастройка доступа к web-серверу по порту tcp 80зователей к ресурсам сети.

# Ответы на контрольные вопросы

1. Как задать действие правила для конкретного протокола? – permit…
2. Как задать действие правила сразу для нескольких портов? - …range…
3. Как узнать номер правила в списке прав доступа? – show access-lists
4. Каким образом можно изменить порядок применения правил в списке контроля доступа? – ip access-list resequence…