Отчет по лабораторной работе №9

Дисциплина: Администрирование локальных сетей

Лобанова Полина Иннокентьевна

Содержание

# 1 Цель работы

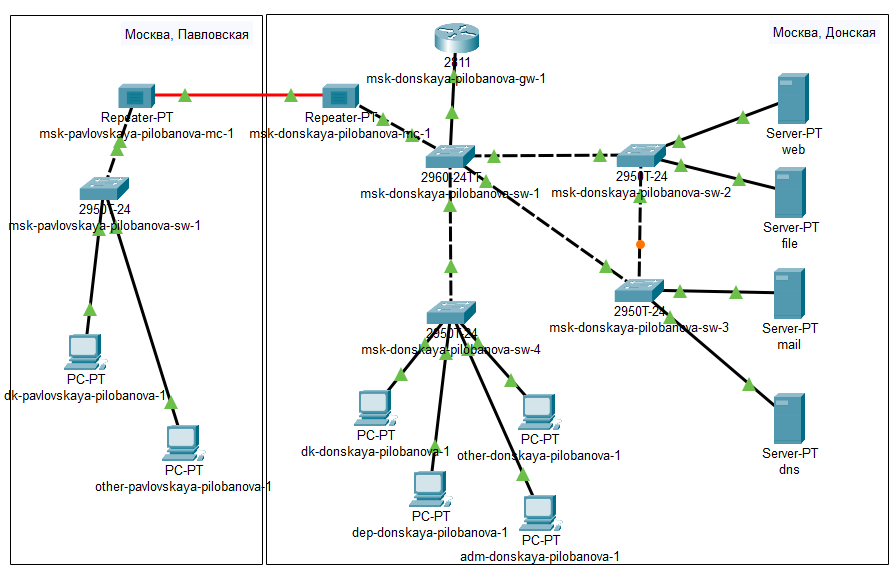
Изучение возможностей протокола STP и его модификаций по обеспечению отказоустойчивости сети, агрегированию интерфейсов и перераспределению нагрузки между ними.

# 2 Задание

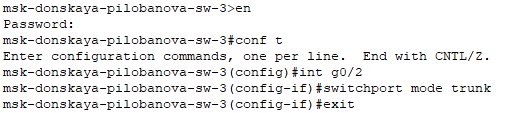
1. Сформируйте резервное соединение между коммутаторами msk-donskayasw-1 и msk-donskaya-sw-3.
2. Настройте балансировку нагрузки между резервными соединениями.
3. Настройте режим Portfast на тех интерфейсах коммутаторов, к которым подключены серверы.
4. Изучите отказоустойчивость резервного соединения.
5. Сформируйте и настройте агрегированное соединение интерфейсов Fa0/20 – Fa0/23 между коммутаторами msk-donskaya-sw-1 и msk-donskaya-sw-4.
6. При выполнении работы необходимо учитывать соглашение об именовании.

# 3 Выполнение лабораторной работы

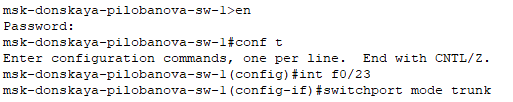
1. Сформировала резервное соединение между коммутаторами msk-donskayasw-1 и msk-donskaya-sw-3. Для этого заменила соединение между коммутаторами msk-donskaya-sw-1 (Gig0/2) и msk-donskaya-sw-4 (Gig0/1) на соединение между коммутаторами msk-donskaya-sw-1 (Gig0/2) и msk-donskaya-sw-3 (Gig0/2); сделала порт на интерфейсе Gig0/2 коммутатора msk-donskaya-sw-3 транковым; соединение между коммутаторами msk-donskaya-sw-1 и msk-donskayasw-4 сделала через интерфейсы Fa0/23, не забыв активировать их в транковом режиме.



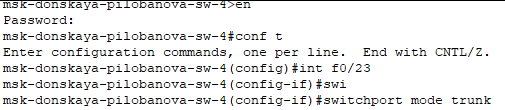
*Логическая схема локальной сети с резервным соединением*



*Активация портов в транковом режиме*

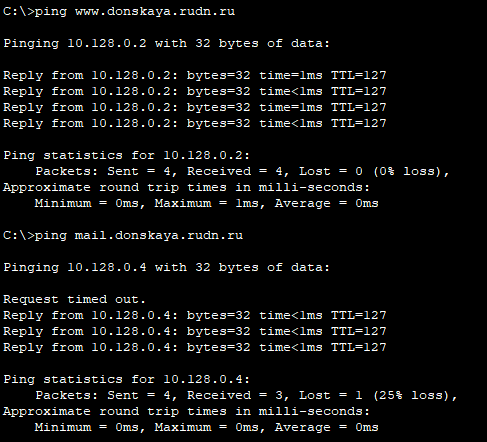


*Активация портов в транковом режиме*

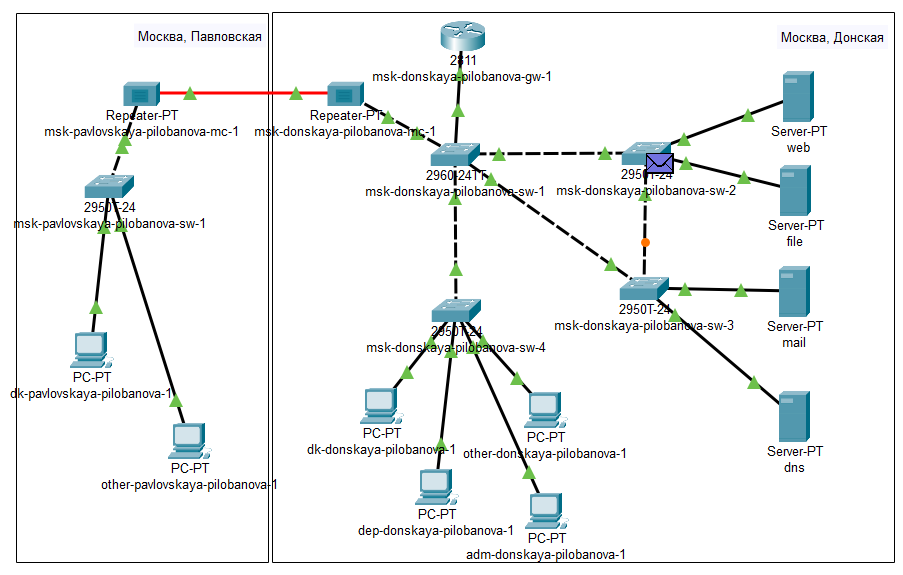


*Активация портов в транковом режиме*

1. С оконечного устройства dk-donskaya-1 пропинговала серверы mail и web. В режиме симуляции проследила движение пакетов ICMP. Убедилась, что движение пакетов происходит через коммутатор msk-donskaya-sw-2.

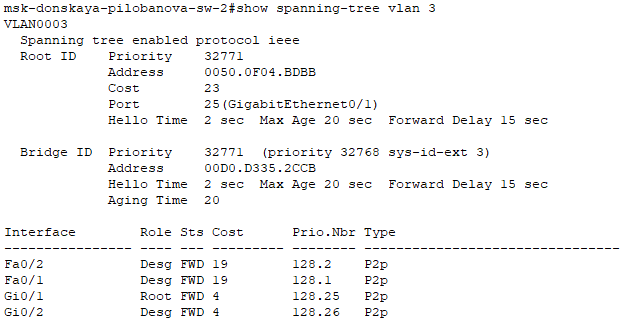


*Пингование*



*Режим симуляции*

1. На коммутаторе msk-donskaya-sw-2 посмотрела состояние протокола STP для vlan 3.



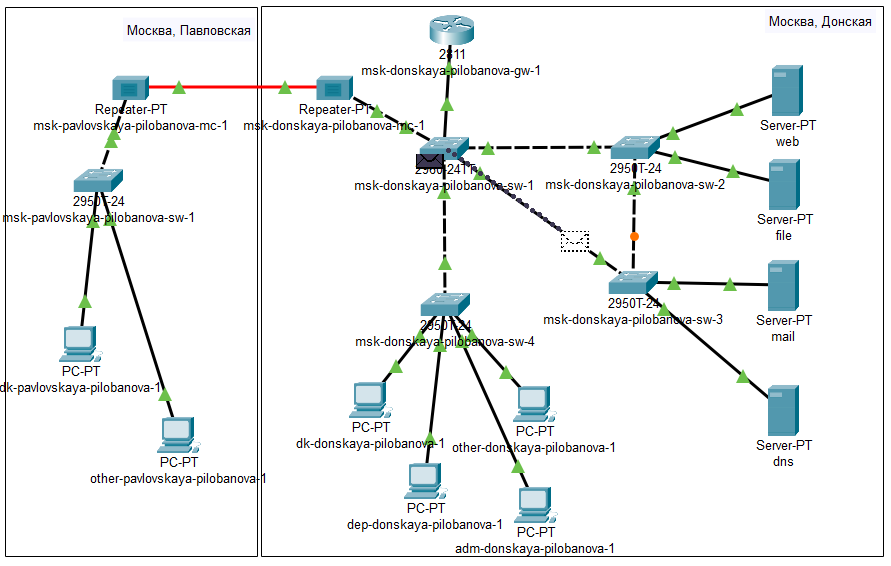
*Информация, связанная с протоколом STP*

1. В качестве корневого коммутатора STP настроила коммутатор mskdonskaya-sw-1.

Настройка корневого коммутатаора

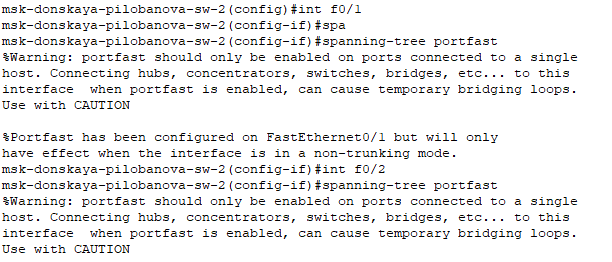
*Настройка корневого коммутатаора*

1. Используя режим симуляции, убедилась, что пакеты ICMP пойдут от хоста dk-donskaya-1 до mail через коммутаторы msk-donskaya-sw-1 и mskdonskaya-sw-3, а от хоста dk-donskaya-1 до web через коммутаторы msk-donskaya-sw-1 и msk-donskaya-sw-2.

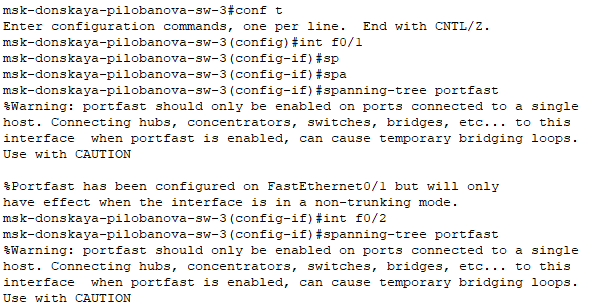


*Режим симуляции*

1. Настроила режим Portfast на тех интерфейсах коммутаторов, к которым подключены серверы.

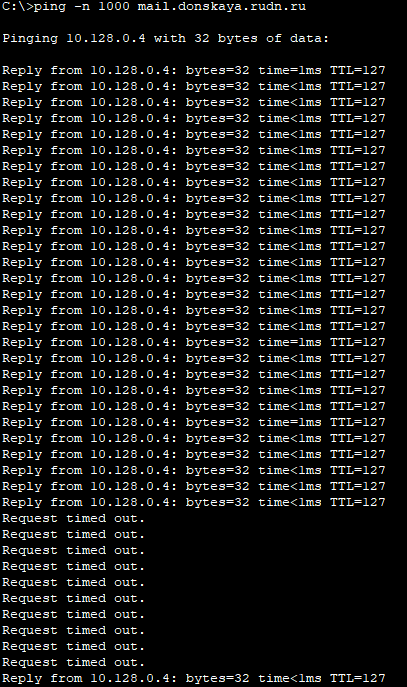


*Настройка режима Portfast*



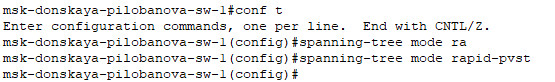
*Настройка режима Portfast*

1. Изучила отказоустойчивость протокола STP и время восстановления соединения при переключении на резервное соединение. Для этого использовала команду ping -n 1000 mail.donskaya.rudn.ru на хосте dk-donskaya-1, а разрыв соединения обеспечила переводом соответствующего интерфейса коммутатора в состояние shutdown.

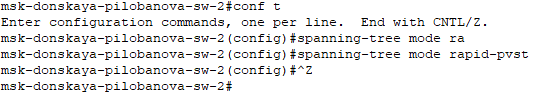


*Пингование*

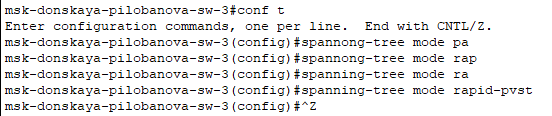
1. Переключила коммутаторы режим работы по протоколу Rapid PVST+.



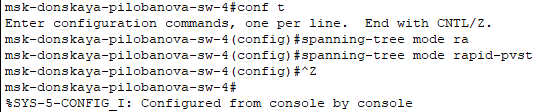
*Режим работы по протоколу Rapid PVST+*



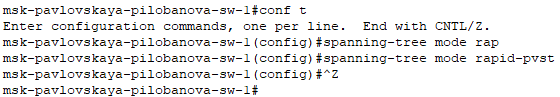
*Режим работы по протоколу Rapid PVST+*



*Режим работы по протоколу Rapid PVST+*

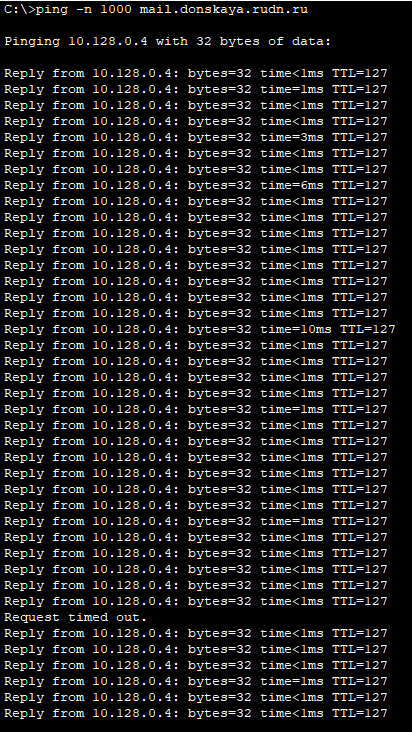


*Режим работы по протоколу Rapid PVST+*



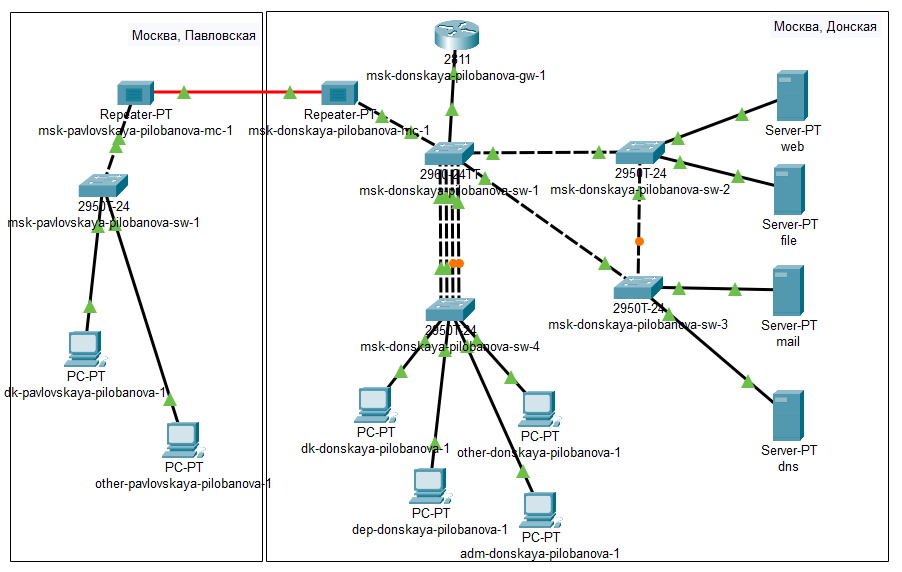
*Режим работы по протоколу Rapid PVST+*

1. Изучила отказоустойчивость протокола Rapid PVST+ и время восстановления соединения при переключении на резервное соединение.



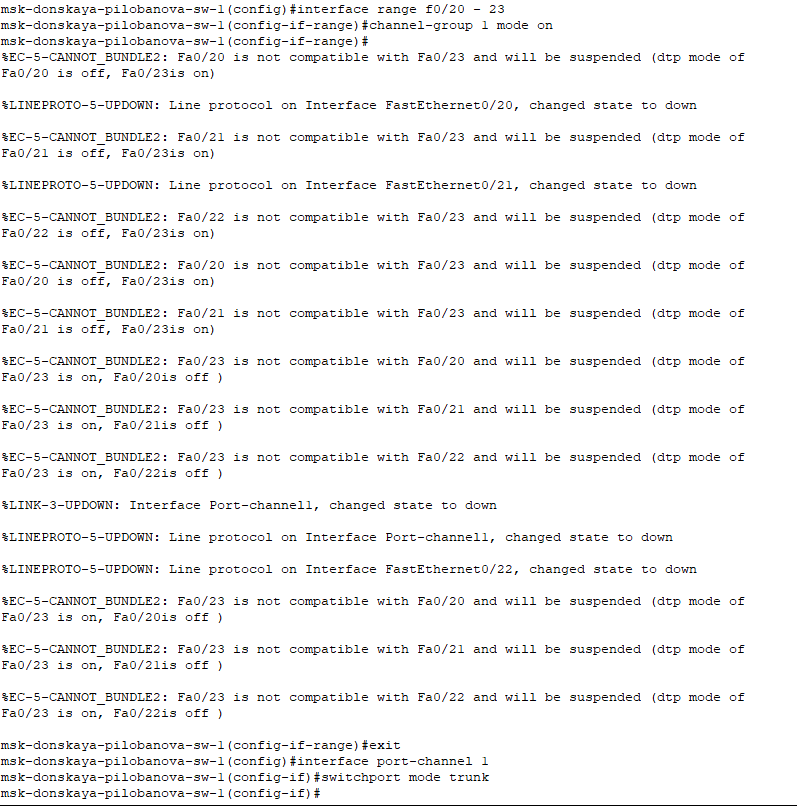
*Пингование*

1. Сформировала агрегированное соединение интерфейсов Fa0/20 – Fa0/23 между коммутаторами msk-donskaya-sw-1 и msk-donskaya-sw-4.

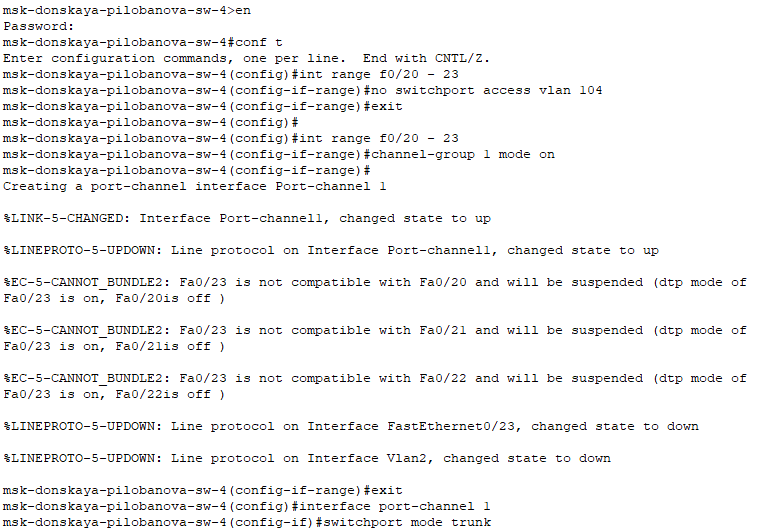


*Логическая схема локальной сети с агрегированным соединением*

1. Настроила агрегирование каналов (режим EtherChannel).



*Настройка агрегирования каналов*



*Настройка агрегирования каналов*

# 4 Выводы

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

# 5 Контрольные вопросы

1. Какую информацию можно получить, воспользовавшись командой определения состояния протокола STP для VLAN (на корневом и не на корневом устройстве)? Приведите примеры вывода подобной информации на устройствах.

Команда для получения информации о состоянии STP зависит от используемого вендора оборудования. Наиболее распространенные команды:

Cisco IOS: show spanning-tree vlan <vlan\_id> или show spanning-tree detail (для всей сети).

Вывод команды show spanning-tree vlan <vlan\_id> покажет информацию о:

Root Bridge: MAC-адрес корневого моста для данной VLAN. Root Path Cost: Стоимость пути до корневого моста. Bridge ID: ID моста (MAC-адрес + приоритет) данного устройства. Порты: Состояние портов (Forwarding, Blocking, Listening, Learning) для данной VLAN на этом устройстве. Role: Роль порта (RootPort, Designated Port, Alternate Port, Backup Port).

1. При помощи какой команды можно узнать, в каком режиме, STP или Rapid PVST+, работает устройство? Приведите примеры вывода подобной информации на устройствах.

Для определения режима STP (STP или Rapid PVST+) на Cisco IOS используется команда:

show spanning-tree

В выводе этой команды будет указан используемый протокол STP (например, “Rapid PVST+”).

Пример вывода (Cisco IOS):

Spanning tree information:  
 Protocol : Rapid-PVST+  
 Name : vlan10  
 Version : IEEE 802.1D-2004

1. Для чего и в каких случаях нужно настраивать режим Portfast?

Режим Portfast используется для ускорения сходимости STP на портах, которые напрямую подключены к конечным устройствам (рабочие станции, серверы), а не к другим коммутаторам. Это позволяет избежать состояния “blocking” для порта, сокращая время ожидания и повышая доступность.

Необходимо настраивать Portfast в случаях:

Подключение к конечным устройствам (PC, серверы, принтеры) Подключение к устройствам доступа (IP-телефоны, точки доступа) Когда требуется быстрая доступность порта.

Настройка (Cisco IOS):

interface <interface> spanning-tree portfast

1. В чем состоит принцип работы агрегированного интерфейса? Для чего он используется?

Агрегированный интерфейс (EtherChannel) объединяет несколько физических портов в один логический канал с более высокой пропускной способностью и избыточностью. Если один из физических портов выходит из строя, трафик автоматически перенаправляется по оставшимся портам.

Использование:

Увеличение пропускной способности между устройствами. Обеспечение избыточности и отказоустойчивости. Упрощение управления сетью за счет объединения нескольких физических портов в один логический.

1. В чём принципиальные отличия при использовании протоколов LACP (Link Aggregation Control Protocol), PAgP (Port Aggregation Protocol) и статического агрегирования без использования протоколов?

Все три метода – LACP, PAgP и статическое агрегирование – используются для объединения нескольких физических портов в один логический канал (EtherChannel), увеличивая пропускную способность и отказоустойчивость. Однако, они отличаются по способу настройки и управления этим каналом:

Статическое агрегирование: Администратор вручную настраивает агрегированный канал на обоих коммутаторах, указав, какие порты должны быть объединены. Это самый простой метод, но и наименее гибкий. Если один из портов в канале выходит из строя, администратор должен вручную восстановить конфигурацию. Нет автоматического обнаружения и согласования параметров канала между устройствами. Требуется идеальное соответствие конфигурации на обоих концах канала.

PAgP (Port Aggregation Protocol): Это протокол Cisco, который автоматически обнаруживает и согласовывает параметры агрегированного канала между двумя коммутаторами. Коммутаторы обмениваются сообщениями, чтобы определить, какие порты должны быть объединены и на каких условиях. PAgP предлагает лучшую гибкость и отказоустойчивость, чем статическое агрегирование, так как автоматически восстанавливает канал после сбоев. Однако, он работает только между устройствами Cisco, или устройствами, поддерживающими этот протокол.

LACP (Link Aggregation Control Protocol): Это стандартный протокол IEEE 802.3ad, который обеспечивает автоматическое обнаружение и согласование параметров агрегированного канала между коммутаторами разных производителей. Он более универсален, чем PAgP, так как совместим с большинством современных сетевых устройств. LACP также обеспечивает более продвинутые функции управления каналом, такие как балансировка нагрузки и отказоустойчивость. Он предоставляет больше возможностей для управления агрегированием, например, позволяет указывать, сколько портов использовать в канале.

1. При помощи каких команд можно узнать состояние агрегированного канала EtherChannel?

Команды для проверки состояния агрегированного канала EtherChannel зависят от используемой операционной системы сетевого оборудования. В качестве примера, рассмотрим команды для Cisco IOS:

show etherchannel summary: Эта команда предоставляет краткий обзор всех агрегированных каналов на коммутаторе, включая их состояние, активные порты, скорость и тип. Она показывает общий статус канала.

show etherchannel port-channel <номер\_канала>: Эта команда отображает подробную информацию о конкретном агрегированном канале, указанном его номером. Показывает информацию о портах, включенных в канал, их состояние, скорость и протокол агрегации.

show etherchannel statistics <номер\_канала>: Эта команда выводит статистическую информацию о конкретном канале, такую как количество переданных и принятых пакетов, ошибок и т.д. Помогает в диагностике проблем.

show interfaces status: Показывает состояние всех интерфейсов, включая порты, входящие в состав EtherChannel. Можно увидеть, к какому каналу принадлежит порт и его статус.

show interfaces <номер\_порта>: Показывает подробную информацию о конкретном порте, в том числе информацию о его принадлежности к EtherChannel.

# Список литературы