Лабораторная работа №4
Принцип работы протокола покрывающего дерева STP

Цель работы: исследовать принцип работы протокола STP; сравнить процесс конвергенции протоколов STP и RSTP.

По ходу выполнения работы необходимо сформировать отчёт:

1. Название работы.
2. Цель работы.
3. Схема топологии сети.
4. Набор используемых команд.
5. Вывод о скорости сходимости протокола STP.
6. Вывод о скорости сходимости протокола RSTP.

После выполнения работы необходимо ответить на контрольные вопросы (к защите).

Теоретическая часть

Для повышения надежности сети часто используют избыточные соединения между коммутаторами. Но эта избыточность может стать причиной следующих проблем:

- петли 2-го уровня;
- широковещательный шторм;
- дублирование одноадресных фреймов.

STP (Spanning Tree Protocol – протокол покрывающего дерева) - протокол второго уровня, позволяющий в сети с избыточными соединениями использовать только один логический путь, блокируя избыточные пути, которые могут привести к образованию петель.

В случае если один из участков пути будет недоступен, протокол STP вычислит новый путь и разблокирует один из заблокированных участков.

STP использует алгоритм покрывающего дерева Spanning Tree Algorithm (STA), чтобы определить, какой из портов коммутатора перевести в заблокированное состояние. Для этого STA определяет один из коммутаторов, как root bridge (корневой узел) и использует его как точку отсчета для расчета всех путей. После того, как root bridge выбран, STA рассчитывает кратчайший путь к root bridge. Каждый коммутатор использует STA, чтобы определить, какой порт блокировать. Пока STA выбирает кратчайшие пути, коммутатор не имеет возможности передавать данные по сети. Для определения кратчайшего пути STA использует стоимость пути. Стоимость пути рассчитывается исходя из скоростей всех портов на протяжении пути. Сумма стоимостей участков в пути составляет стоимость пути. Если есть больше чем один путь, STA выбирает путь с меньшей стоимостью. Когда STA определил, какие пути оставить доступными, он назначает роли портам коммутаторов.

Таблица 1. Скорость передачи и стоимость пути

Скорость передачи	Стоимость (802.1D-1998)	Стоимость (802.1W-2001)
4 Мбит/с	250	5 000 000
10 Мбит/с	100	2 000 000
16 Мбит/с	62	1 250 000
100 Мбит/с	19	200 000
1 Гбит/с	4	20 000
2 Гбит/с	3	10 000
10 Гбит/с	2	2 000

Роли портов

Root (корневые) порты – порты некорневых коммутаторов, через которые проходит трафик в сторону корневого коммутатора. Может быть только один корневой порт у коммутатора. MAC адреса источника фреймов, полученные на этот порт, заносятся в таблицу MAC адресов коммутатора.

Designated (назначенные) порты – могут быть и у корневых, и у некорневых коммутаторов. У корневых – это все порты. У некорневых – все некорневые порты, через которые разрешена передача трафика. В одном сегменте сети может быть только один назначенный порт. MAC адреса источника фреймов, полученные на эти порты, заносятся в таблицу MAC адресов коммутатора.

Non-designated (неназначенные) порты – порты, которые находятся в состоянии блокировки. Трафик через них запрещен.

Disabled (отключенные) порты – порты, которые выключены администратором командой **shutdown.**

Процесс выбора root bridge

Все коммутаторы в сети принимают участие в выборах. Для этого они обмениваются сообщениями BPDU (Bridge Protocol Data Unit). Эти сообщения содержат bridge ID и root ID.

Bridge ID - идентификатор текущего коммутатора.

Root ID - идентификатор корневого коммутатора.

После загрузки коммутатор каждые 2 секунды начинает отправлять BPDU-сообщение. Изначально root ID в сообщении равен локальному bridge ID. После того, как коммутатор принимает BPDU сообщение, он сравнивает root ID из сообщения со своим root ID. Если root ID из сообщения будет меньше, он заменяет свой root ID. Затем коммутатор начинает передавать BPDU сообщения с новым root ID. В конце концов, все BPDU сообщения, передаваемые коммутаторами, будут содержать наименьший root ID. Коммутатор с этим bridge ID и будет root bridge.

Изначально, после загрузки все порты коммутатора находятся в блокированном состоянии. По умолчанию - в течение 20 секунд (для диаметра сети 7). Они только передают и принимают BPDU.

Определение лучшего пути к root bridge

В BPDU сообщениях кроме bridge ID и root ID передается также стоимость пути к root ID. После того, как root bridge был выбран, STA начинает процесс определения наилучшего пути к корневому мосту со всех направлений в широковещательном домене. Информация о путях определяется путем суммирования индивидуальных стоимостей портов на пути от коммутатора назначения до root bridge.

По умолчанию, стоимость портов коммутаторов следующая:

10 Гб/с - 2
1 Гб/с - 4
100 Мб/с - 19
10 Мб/с - 100

Для каждого порта можно задать стоимость вручную командой:

S1(config-if)#**spanning-tree cost *cost***

Для отмены ручной настройки стоимости порта используется команда:

S1(config-if)#**no spanning-tree cost**

После подсчета стоимостей всех путей, выбирается путь с наименьшей стоимостью, а все резервные пути блокируются. Для проверки стоимостей портов, а также стоимости пути к root bridge используется команда:

S1#**show spanning-tree**

Для вывода более детальной информации используется команда:

S1#**show spanning-tree detail**

Bridge ID

Поле bridge ID в BPDU состоит из трех частей.

Bridge Priority - приоритет коммутатора при выборе root bridge. Может изменяться от 1 до 65536. По умолчанию равен 32768. Чем меньше значение, тем больше приоритет.

Extended System ID - номер VLAN'а. Используется в PVST. Добавляется к Bridge Priority для вычисления приоритета.

MAC Address. Когда все коммутаторы в сети сконфигурированы с одинаковыми приоритетом (Bridge Priority) и номером Extended System ID, решающим фактором при выборе root bridge будет MAC адрес. Коммутатор с наименьшим MAC адресом будет выбран как root bridge.

Бывают случаи, когда необходимо, чтобы конкретный коммутатор был корневым. Для этого меняется приоритет коммутатора. Сделать это можно двумя способами.

1. Командой

S1(config)#**spanning-tree vlan *vlan-id* root primary**

коммутатору будет присвоен приоритет 24576 или на 4096 меньший, чем самый меньший обнаруженный приоритет в сети. Это будет основной корневой коммутатор.

Командой

S1(config)#**spanning-tree vlan *vlan-id* root secondary**

коммутатору будет присвоен приоритет 28672. Это будет запасной корневой коммутатор. Он станет корневым, если основной корневой станет недоступен и начнутся новые выборы, при условии, что у остальных коммутаторов приоритет установлен по умолчанию.

2. Командой

S1(config)#**spanning-tree vlan *vlan-id priority value***

Этим способом можно назначать конкретные значения приоритетов.

Определение роли порта

Выбор корневого порта. Коммутатор сравнивает стоимости всех возможных путей к корневому коммутатору. Порт коммутатора, у которого самая низкая стоимость пути, автоматически становится корневым. Если два и более портов имеют одинаковую стоимость пути, выбирается порт, имеющий больший приоритет. Если приоритеты тоже одинаковые, выбирается порт, имеющий наименьший номер (port ID). Приоритет порта настраивается командой S1(config-if)#**spanning-tree *port-priority value*.** Диапазон от 0 до 240 с шагом 16. По умолчанию равен 128.

Выбор назначенных и неназначенных портов. Корневой коммутатор автоматически определяет все свои порты как назначенные. На некорневых коммутаторах этот выбор происходит после выбора корневого порта. Выбор происходит на каждом сегменте. Коммутатор смотрит сообщение BPDU, приходящее на порт и решает: если bridge ID у него меньше, чем у соседа, порт становится назначенным, а если больше - неназначенным.

Проверить роли портов и их приоритеты можно командой S1#**show spanning-tree**

Состояния порта

Порты коммутатора при работе протокола STP могут находиться в пяти состояниях:

Blocking (заблокированный) - неназначенный порт не участвует в процессе пересылки фреймов. Но передает и принимает BPDU.

Listening (прослушивание) - порт принимает и передает только BPDU.

Learning (изучение) - порт готовится к началу пересылки фреймов. Порт принимает и передает BPDU, а также изучает MAC адреса из фреймов, приходящих на него.

Forwarding (пересылка) - порт принимает, передает и изучает MAC адреса из фреймов, приходящих на него.

Disabled - порт отключен администратором командой shutdown.

Таймеры BPDU

Время, в течение которого порт находится в различных состояниях, зависит от таймеров BPDU. Только корневой коммутатор может рассылать сообщения по сети, которые настраивают таймеры. Существуют следующие таймеры изменения состояний:

Hello time - время между посылками сообщений BPDU на порт. По умолчанию равно 2 секунды. Можно изменять от 1 до 10 секунд.

Forward delay (задержка перед передачей) - время, в течение которого порт находится в каждом из состояний listening и learning. По умолчанию - 15 секунд. Можно изменить от 4 до 30 секунд.

Maximum age - время, в течение которого порт хранит информацию, полученную вместе с последним BPDU. По умолчанию - 20 секунд. Может изменяться от 6 до 40 секунд.

Изменять таймеры напрямую не рекомендуется. Таймеры по умолчанию установлены для сети с диаметром, равным 7. Поэтому, если администратор решит изменить время сходимости сети, лучше использовать команду задания диаметра сети. Коммутатор сам подстроит все таймеры.

S1(config)#**spanning-tree vlan *vlan id* root primary *diameter value***

Технология Cisco PortFast

Для портов, к которым подключены не коммутаторы, конечные устройства (компьютеры, телефоны и др.), для быстрого перехода в состояние передачи (без прохода через состояния listening и learning), Cisco разработала технологию PortFast. Устройство, подключенное к порту с включенным PortFast, сразу может передавать данные.

Для включения используется команда: S1(config-if)#**spanning-tree portfast.**

Для выключения - S1(config-if)#**no spanning-tree portfast.**

Проверка включения режима PortFast на интерфейсе: S1#**show running-config.**

Изменение топологии STP

После того, как выборы корневого коммутатора завершились, и произошло назначение ролей портам коммутатора, все коммутаторы, за исключением корневого, прекращают генерацию своих BPDU. Только корневой коммутатор генерирует BPDU и рассылает их на широковещательный адрес. Все остальные - только ретранслируют его.

При изменении топологии коммутатор, который это обнаружил, отправляет специальное сообщение BPDU, которое называется TCN (topology change notification), через корневой порт в направлении корневого коммутатора. Некорневые коммутаторы, которые принимают это сообщение, ретранслируют его через свой корневой порт, а также отправляют назад подтверждение о получении - TCA (topology change acknowledgement).

После того, как корневой коммутатор получил TCN, он сначала отправляет назад TCA. А затем широковещательно отправляет BPDU с установленным флагом TC (topology change). Таким образом, все коммутаторы сети узнают об изменении топологии сети и увеличивают время Maximum age до 35 секунд по умолчанию.

Варианты и модификации STP

Per-VLAN spanning tree protocol (PVST) – проприетарный (частный, собственный) протокол Cisco. Использует для организации транков свой протокол ISL. Связующее дерево строится отдельно для каждой VLAN. Это дает возможность балансировать трафик на 2-м уровне. Для PVST разработаны расширения настройки портов BackboneFast, UplinkFast и PortFast.

Per-VLAN spanning tree protocol plus (PVST+) – проприетарный протокол Cisco. Разработан для поддержки транкового протокола IEEE 802.1Q. Поддерживает все расширения PVST, а также введены дополнения BPDU guard и Root guard.

Rapid per-VLAN spanning tree protocol (rapid PVST+) – проприетарный протокол Cisco. основан на стандарте IEEE802.1w и имеет меньшее время сходимости по сравнению с STP. Поддерживает все расширения PVST и PVST+.

Rapid spanning tree protocol (RSTP) – общедоступный протокол. Включает расширения Cisco BackboneFast, UplinkFast и PortFast. Имеет меньшее время сходимости по сравнению с STP. Именно он сейчас и применяется. Т.е. STP = RSTP.

Multiple STP (MSTP) - общедоступный протокол. Позволяет строить связующие деревья для нескольких VLAN. Т.е. позволяет уменьшать количество деревьев на коммутаторе. Предусматривает несколько путей для переадресации трафика и позволяет балансировать нагрузку.

PVST+

Это проприетарный протокол Cisco. Он строит связующие деревья для каждой VLAN и позволяет блокировать порты для каждой VLAN в отдельности. Поэтому более экономично используется полоса пропускания каждого порта (не простаивает).

Соответственно и настраивать приоритеты для коммутаторов и портов можно для каждой VLAN. Например, для половины VLAN корневым коммутатором настраивается один коммутатор, а для второй половины - другой.

Но надо помнить, что если не настраивать приоритеты, все коммутаторы сети для всех VLAN будут принимать решения о корневом коммутаторе, основываясь на MAC-адресах коммутаторов. И никакой балансировки нагрузки не будет.

Настройки по умолчанию на коммутаторах Cisco:

Состояние - включено для VLAN1

Вариант протокола - PVST+ (Rapid PVST+ и MSTP отключены)

Приоритет коммутатора - 32768

Приоритет порта (при STP на основе портов) - 128

Стоимость портов - 10 Гб/с - 2, 1 Гб/с - 4, 100 Мб/с - 19, 10 Мб/с - 100

Приоритет порта (при STP на основе VLAN) - 128

Таймеры - Hello time: 2 с, Forward-delay time: 15 с, Maximum-aging time: 20 с, Transmit hold count: - 6 BPDU

Порядок настройки:

1. Выбираем коммутаторы, которые будут основными и резервными корневыми коммутаторами для каждой VLAN.

2. Конфигурируем эти коммутаторы:

S1(config)#**spanning-tree vlan *vlan-ID* root primary**

S2(config)#**spanning-tree vlan *vlan-ID* root secondary**

Также можно настроить приоритеты коммутаторов командой

S1(config)#**spanning-tree vlan *vlan-ID* priority *priority*** - где приоритет можно назначать в диапазоне от 0 до 61440 с шагом 4096. Коммутатор с более низким приоритетом и будет корневым.

Проверка настроенного протокола для активных интерфейсов осуществляется командой:

S2#**show spanning tree active**

RSTP

Это развитие протокола STP. Большинство параметров не изменилось. Изменились лишь роли портов и их состояния. Из-за этого значительно уменьшилось время сходимости сети.

В RSTP, если коммутатор не принял три подряд BPDU (по умолчанию 6 секунд), считается, что связь потеряна.

Edge Port - граничный порт относительно STP дерева. Это порт, к которому никогда не был подключен другой коммутатор, а подключены конечные устройства. То есть порт сразу же переходит в режим пересылки. Режим работы порта в этой роли похож на режим PortFast, но отличается тем, что порт при получении первого же BPDU становится STP портом.

Состояния портов:

В отличие от STP, RSTP определяет всего три состояния портов коммутаторов:

Discarding (отброс фреймов) - состояние, в котором порт не передает данные. По аналогии с STP, это Blocking, Listening и Disabled состояния.

Learning (изучение) - так же, как и в STP.

Forwarding - так же, как и в STP.

Роли портов:

Корневой порт - порт некорневого коммутатора, имеющий лучшую стоимость для достижения корневого коммутатора. Для каждого некорневого коммутатора может быть только один. В стабильной сетевой топологии находится в состоянии Forwarding.

Назначенный порт - все порты корневого коммутатора. А также только по одному порту на сегмент, связывающий некорневые коммутаторы. В стабильной сетевой топологии находится в состоянии Forwarding.

Альтернативный порт - порт, предлагающий альтернативный путь к корневому коммутатору. Находится в состоянии Discarding.

Конфигурирование Rapid-PVST+

S1(config)#**spanning-tree mode rapid-pvst**
S1(config)#**interface *interface-id***
S1(config-if)#**spanning-tree link-type point-to-point**
S1#**clear spanning-tree detected-protocols**

Практическая часть

1. Построить сеть в соответствии с топологией на рис. 1 в Cisco Packet Tracer. Зарисовать схему в отчет.

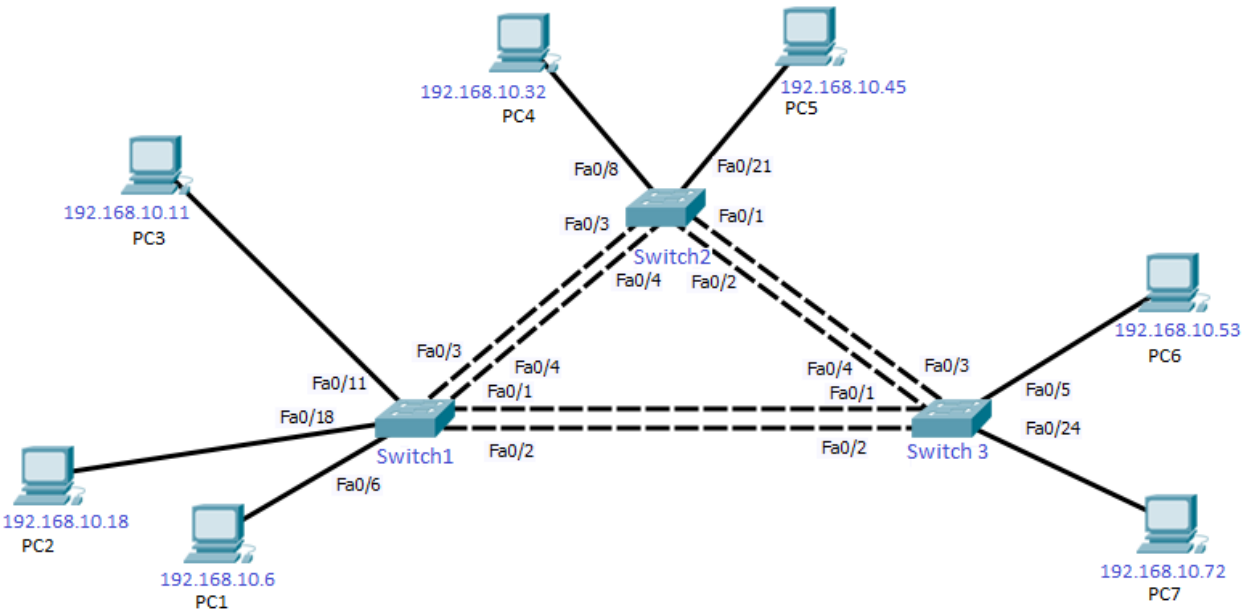

Рис. 1. Топология сети для задания

2. Изучение принципа работы протокола покрывающего дерева

Проследить за работой протокола STP с помощью режима симуляции.

Замените режим реального времени на режим симуляции (смените вкладку Realtime на Simulation). В фильтре укажите только STP пакеты (помощью Show All/None и Edit Filters, отметить STP). Проследите прохождение пакетов в режиме Simulation (с помощью кнопки Capture/Forward) и каким образом формируется покрывающее дерево.

3. Базовая конфигурация оборудования

- Настроить hostname (задать имя коммутатору).
- Отключить DNS lookup (при ошибке в командах не обращается к списку команд).
- Установить пароль для EXEC mode (пароль зашифрованный **cisco**).
- Установить пароль для console (пароль незашифрованный **cisco**).
- Установить пароль для 6 vty (для подключения через telnet пароль незашифрованный **cisco**).
- Сохранить текущую конфигурацию.

Код базовой конфигурации (настраивается на каждом коммутаторе с изменением **hostname S1**, **S2**, **S3**):

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname S1
S1(config)#enable secret class
S1(config)#no ip domain-lookup
S1(config)#line console 0
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#line vty 0 5
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#end
%SYS-5-CONFIG_I: Configured from console by console
S1#copy running-config startup-config
```

Destination filename [startup-config]? **[Enter]**
Building configuration...
[OK]

4. Настроить сетевые интерфейсы персональных компьютеров

Настроить сетевые интерфейсы PC1-PC7 в соответствии с планом адресации (табл.2). Используя команду ping, убедится в наличии связи между компьютерами.

Таблица 2. План адресации

Device	Interface	IP Address	Subnet Mask
PC1	**NIC**	**192.168.10.6**	**255.255.255.0**
PC2	**NIC**	**192.168.10.18**	**255.255.255.0**
PC3	**NIC**	**192.168.10.11**	**255.255.255.0**
PC4	**NIC**	**192.168.10.32**	**255.255.255.0**
PC5	**NIC**	**192.168.10.45**	**255.255.255.0**
PC6	**NIC**	**192.168.10.53**	**255.255.255.0**
PC7	**NIC**	**192.168.10.72**	**255.255.255.0**

5. Изучить конфигурацию Spanning Tree

- При помощи команды **show spanning-tree** проверить текущую конфигурацию **STP**

S1#**show spanning-tree**

S2#**show spanning-tree**

S3#**show spanning-tree**

Выяснить различия между позициями коммутаторов. Записать, какой из них является корневым (***This bridge is the root***).

6. Изучить процесс конвергенции STP

- Наблюдать за индикацией портов: выяснить, какой порт является заблокированным STP (оранжевый), какой – рабочим (зелёный) (например, рис. 2).

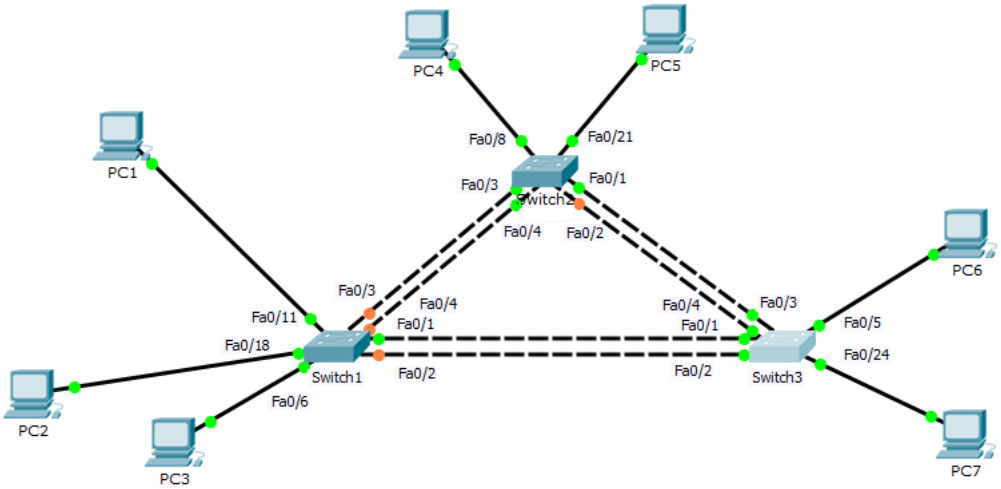

Рис. 2. Сеть с индикацией портов

- На некорневом коммутаторе необходимо отключить корневой порт, исходя из индикации на схеме (сразу же возвращаемся к схеме) засечь время, пока покрывающее дерево не перестроится и какой-нибудь другой порт (с оранжевой индикацией) станет рабочим (индикатор станет зелёным), то есть отметить время сходимости сети. Записать в отчёт примерное время сходимости сети.

В примере: на коммутаторе S1 для порта с ролью Root (в данном примере Fa0/1 – корневой порт, через который трафик идёт к корневому коммутатору) выполняется команда **shutdown** (рис. 3).

S1(config)#**interface fa0/1**
S1(config-if)#**shutdown**

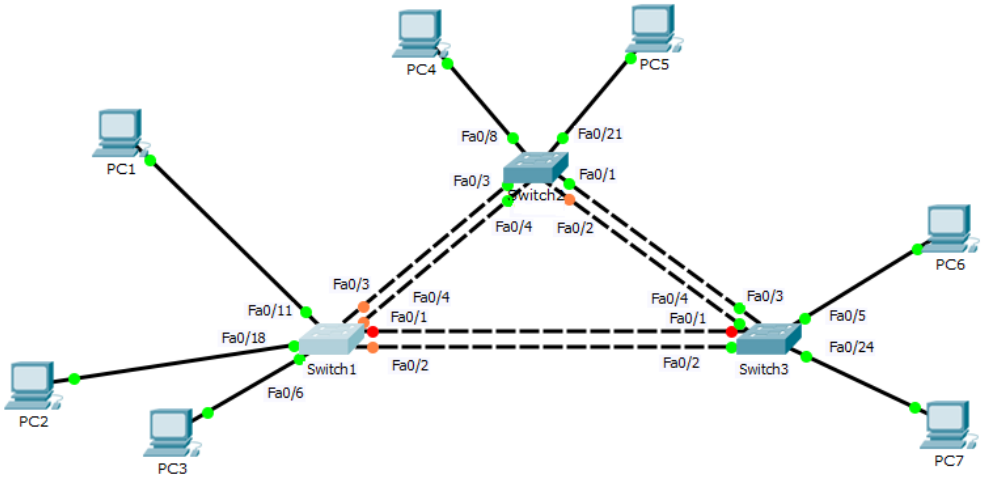

Рис. 3. Отключение корневого порта fa0/1 на Switch1

Восстановленная сеть показана на рис. 4.

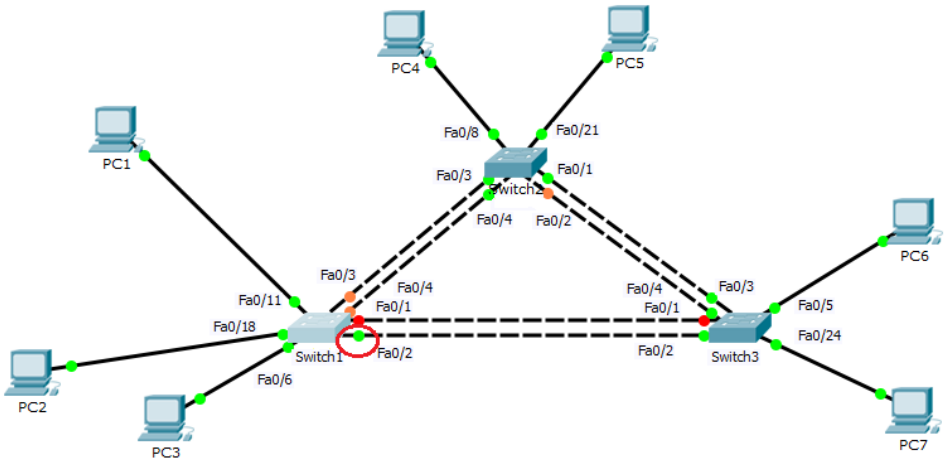

Рис. 4. Сеть с индикацией портов после восстановления сети (порт fa0/2 сменил индикацию с оранжевой на зелёную)

- После восстановления работоспособности сети необходимо вернуть предыдущее состояние порта командой **no shutdown**.

  S3(config-if)#**no shutdown**

7. Настроить на коммутаторах Rapid Spanning Tree Protocol

- На коммутаторах S1,S2 и S3 включить для spanning-tree режим rapid-pvst:

  S1(config)#**spanning-tree mode rapid-pvst**

  S2(config)#**spanning-tree mode rapid-pvst**

  S3(config)#**spanning-tree mode rapid-pvst**

- На коммутаторах S1, S2 и S3 настроить порты, к которым будут подключаться компьютеры, для использования в роли RSTP Edge –портов:

  S1(config)#**interface range fa0/5-24**
  S1(config-if-range)#**spanning-tree portfast**

  S2(config)#**interface range fa0/5-24**
  S2(config-if-range)#**spanning-tree portfast**

S3(config)#**interface range fa0/5-24**
S3(config-if-range)#**spanning-tree portfast**

8. Изучить процесс конвергенции RSTP

- Повторить пункт **6**. Записать в отчёт время сходимости для протокола RSTP.

Контрольные вопросы

1. Для чего используется технология PortFast?
2. Дать определение протоколу RSTP.
3. Определить роли портов (в протоколе STP) на Вашей сети.
4. Какие бывают виды и модификации протокола STP?
5. От чего защищает протокол STP в сетях Ethernet при наличии кольцевых топологий?