

Лабораторная работа. Настройка Rapid PVST+, PortFast и BPDU Guard

Топология

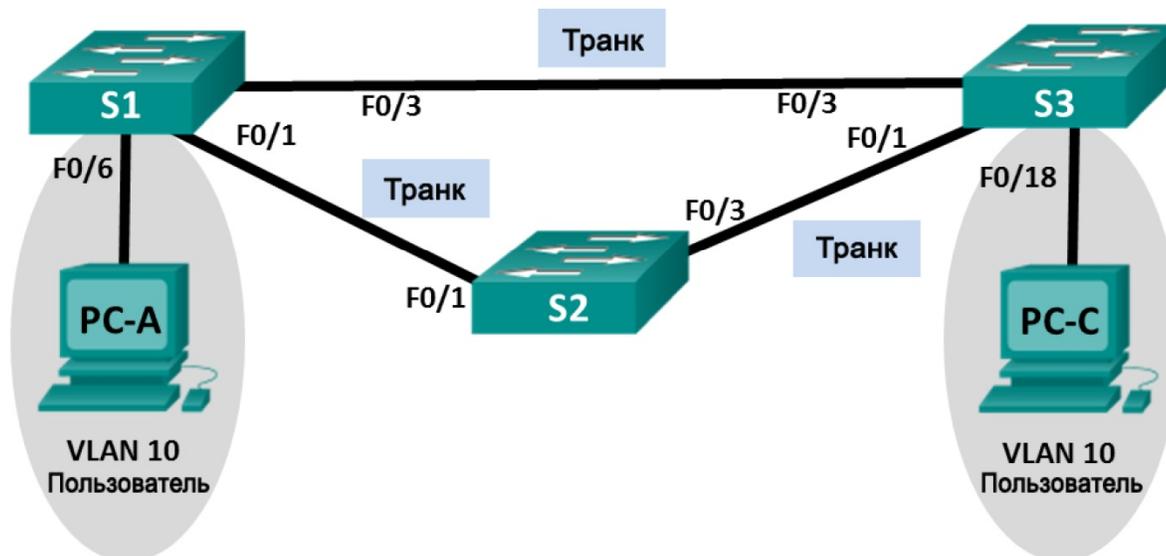


Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети
S1	VLAN 99	192.168.1.11	255.255.255.0
S2	VLAN 99	192.168.1.12	255.255.255.0
S3	VLAN 99	192.168.1.13	255.255.255.0
PC-A	NIC	192.168.0.2	255.255.255.0
PC-C	NIC	192.168.0.3	255.255.255.0

Назначения сети VLAN

VLAN	Имя
10	Пользователь
99	Management (Руководство)

Задачи

Часть 1. Создание сети и настройка базовых параметров устройств

Часть 2. Настройка сетей VLAN, native VLAN и транковых каналов

Часть 3. Настройка корневого моста и проверка сходимости PVST+

Часть 4. Настройка Rapid PVST+, PortFast, BPDU guard и проверка сходимости

Исходные данные/сценарий

Протокол spanning-tree для VLAN (PVST) является проприетарным протоколом Cisco. По умолчанию коммутаторы Cisco используют протокол PVST. Rapid PVST+ (IEEE 802.1w) является усовершенствованной версией PVST+ и обеспечивает более быстрые вычисления протокола spanning-tree и более быструю сходимость после изменений топологии 2 уровня. Rapid PVST+ определяет три состояния порта: отбрасывание, обучение и пересылка, а также представляет ряд нововведений в целях оптимизации производительности сети.

В этой лабораторной работе вам предстоит настроить основной и вспомогательный корневые мосты, изучить сходимость PVST+, настроить Rapid PVST+ и сравнить его сходимость с PVST+. Кроме того, необходимо будет настроить пограничные порты для немедленного перехода в состояние пересылки с помощью PortFast, а также заблокировать пересылку BPDU из пограничных портов, используя BPDU guard.

Примечание. В данной лабораторной работе содержится минимальный набор команд, необходимых для настройки. Список требуемых команд приведен в приложении А. Проверьте свои знания: настройте устройства, не обращаясь к информации, приведённой в приложении.

Примечание. В лабораторной работе используются коммутаторы Cisco Catalyst 2960s под управлением ОС Cisco IOS 15.0(2), (образ lanbasek9). Допускается использование других моделей коммутаторов и других версий ОС Cisco IOS. В зависимости от модели устройства и версии Cisco IOS доступные команды и их результаты могут отличаться от приведённых в описании лабораторных работ.

Примечание. Убедитесь, что прежние настройки коммутаторов были удалены, и они не содержат конфигурации загрузки. Если вы не уверены в этом, обратитесь к инструктору.

Необходимые ресурсы:

- 3 коммутатора (Cisco 2960 под управлением ОС Cisco IOS 15.0(2), (образ lanbasek9) или аналогичная модель);
- 2 ПК (под управлением ОС Windows 7, Vista или XP с программой эмуляции терминала, например Tera Term);
- консольные кабели для настройки устройств Cisco IOS через порты консоли;
- кабели Ethernet, расположенные в соответствии с топологией.

Часть 1: Создание сети и настройка базовых параметров устройств

В первой части вам предстоит настроить топологию сети и настроить базовые параметры, такие как IP-адреса интерфейсов, статическая маршрутизация, доступ к устройствам и пароли.

Шаг 1: Подключите кабели в сети в соответствии с топологией.

Шаг 2: Настройте узлы ПК.

Шаг 3: Выполните инициализацию и перезагрузку коммутаторов.

Шаг 4: Настройте базовые параметры каждого коммутатора.

- а. Отключите поиск DNS.
- б. Присвойте имена устройствам в соответствии с топологией.
- в. Установите **cisco** в качестве пароля консоли и виртуального терминала VTU и включите вход по паролю.

- d. Назначьте **class** в качестве зашифрованного пароля доступа к привилегированному режиму EXEC.
- e. Настройте **logging synchronous**, чтобы сообщения от консоли не могли прерывать ввод команд.
- f. Отключите все порты коммутатора.
- g. Сохраните текущую конфигурацию в загрузочную конфигурацию.

Часть 2: Настройка сетей VLAN, native VLAN и транковых каналов

В части 2 рассматриваются создание сетей VLAN, назначения сетям VLAN портов коммутатора, настройка транковых портов и изменение native VLAN для всех коммутаторов.

Примечание. Команды, необходимые для выполнения заданий второй части лабораторной работы, приведены в приложении А. Чтобы проверить свои знания, попробуйте настроить сети VLAN, native VLAN и транковые каналы, не обращаясь к приложению.

Шаг 1: Создайте сети VLAN.

Используйте соответствующие команды, чтобы создать сети VLAN 10 и 99 на всех коммутаторах. Присвойте сети VLAN 10 имя **User**, а сети VLAN 99 — имя **Management**.

```
S1(config)# vlan 10
S1(config-vlan)# name User
S1(config-vlan)# vlan 99
S1(config-vlan)# name Management
```

```
S2(config)# vlan 10
S2(config-vlan)# name User
S2(config-vlan)# vlan 99
S2(config-vlan)# name Management
```

```
S3(config)# vlan 10
S3(config-vlan)# name User
S3(config-vlan)# vlan 99
S3(config-vlan)# name Management
```

Шаг 2: Переведите пользовательские порты в режим доступа и назначьте сети VLAN.

Для интерфейса F0/6 S1 и интерфейса F0/18 S3 включите порты, настройте их в качестве портов доступа и назначьте их сети VLAN 10.

Шаг 3: Настройте транковые порты и назначьте их сети native VLAN 99.

Для портов F0/1 и F0/3 на всех коммутаторах включите порты, настройте их в качестве транковых и назначьте их сети native VLAN 99.

Шаг 4: Настройте административный интерфейс на всех коммутаторах.

Используя таблицу адресации, настройте на всех коммутаторах административный интерфейс с соответствующим IP-адресом.

Шаг 5: Проверка конфигураций и возможности подключения.

Используйте команду **show vlan brief** на всех коммутаторах, чтобы убедиться в том, что все сети VLAN внесены в таблицу VLAN и назначены правильные порты.

Используйте команду **show interfaces trunk** на всех коммутаторах, чтобы проверить транковые интерфейсы.

Используйте команду **show running-config** на всех коммутаторах, чтобы проверить все остальные конфигурации.

Какие настройки используются для режима протокола spanning-tree на коммутаторах Cisco?

Проверьте подключение между PC-A и PC-C. Удалось ли выполнить эхо-запрос? _____

Если эхо-запрос выполнить не удалось, следует выполнять отладку до тех пор, пока проблема не будет решена.

Примечание. Для успешной передачи эхо-запросов может потребоваться отключение брандмауэра.

Часть 3: Настройка корневого моста и проверка сходимости PVST+

В части 3 вам предстоит определить корневой мост по умолчанию в сети, назначить основной и вспомогательный корневые мосты и использовать команду **debug** для проверки сходимости PVST+.

Примечание. Команды, необходимые для выполнения заданий третьей части лабораторной работы, приведены в приложении А. Проверьте свои знания: попробуйте настроить корневой мост, не обращаясь к приложению.

Шаг 1: Определите текущий корневой мост.

С помощью какой команды пользователи определяют состояние протокола spanning-tree коммутатора Cisco Catalyst для всех сетей VLAN? Запишите команду в строке ниже.

Выполните команду на всех трех коммутаторах, чтобы ответить на следующие вопросы:

Примечание. На каждом коммутаторе доступно три экземпляра протокола spanning-tree. По умолчанию на коммутаторах Cisco используется конфигурация STP PVST+, которая позволяет создавать отдельный экземпляр протокола spanning-tree для каждой сети VLAN (VLAN 1 и все остальные настроенные пользователем сети VLAN).

Какой приоритет моста используется для коммутатора S1 в сети VLAN 1? _____

Какой приоритет моста используется для коммутатора S2 в сети VLAN 1? _____

Какой приоритет моста используется для коммутатора S3 в сети VLAN 1? _____

Какой коммутатор является корневым мостом? _____

Почему этот коммутатор выбран в качестве корневого моста?

Шаг 2: Настройте основной и вспомогательный корневые мосты для всех существующих сетей VLAN.

При выборе корневого моста (коммутатора) по MAC-адресу может образоваться условно оптимальная конфигурация. В этой лабораторной работе вам необходимо настроить коммутатор S2 в качестве корневого моста и коммутатор S1 — в качестве вспомогательного корневого моста.

- Настройте коммутатор S2 в качестве основного корневого моста для всех существующих сетей VLAN. Запишите команду в строке ниже.
-

- b. Настройте коммутатор S1 в качестве вспомогательного корневого моста для всех существующих сетей VLAN. Запишите команду в строке ниже.

Используйте команду **show spanning-tree** для ответа на следующие вопросы:

Какой приоритет моста используется для коммутатора S1 в сети VLAN 1? _____

Какой приоритет моста используется для коммутатора S2 в сети VLAN 1? _____

Какой интерфейс в сети находится в состоянии блокировки?

Шаг 3: Измените топологию 2 уровня и проверьте сходимось.

Чтобы проверить сходимось PVST+, необходимо создать изменение топологии 2 уровня, используя команду **debug** для отслеживания событий протокола spanning-tree.

- a. Выполните команду **debug spanning-tree events** в привилегированном режиме на коммутаторе S3.

```
S3# debug spanning-tree events
Spanning Tree event debugging is on
```

- b. Измените топологию, отключив интерфейс F0/1 на коммутаторе S3.

```
S3(config)# interface f0/1
```

```
S3(config-if)# shutdown
```

```
*Mar 1 00:58:56.225: STP: VLAN0001 new root port Fa0/3, cost 38
*Mar 1 00:58:56.225: STP: VLAN0001 Fa0/3 -> listening
*Mar 1 00:58:56.225: STP[1]: Generating TC trap for port FastEthernet0/1
*Mar 1 00:58:56.225: STP: VLAN0010 new root port Fa0/3, cost 38
*Mar 1 00:58:56.225: STP: VLAN0010 Fa0/3 -> listening
*Mar 1 00:58:56.225: STP[10]: Generating TC trap for port FastEthernet0/1
*Mar 1 00:58:56.225: STP: VLAN0099 new root port Fa0/3, cost 38
*Mar 1 00:58:56.225: STP: VLAN0099 Fa0/3 -> listening
*Mar 1 00:58:56.225: STP[99]: Generating TC trap for port FastEthernet0/1
*Mar 1 00:58:56.242: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed
state to down
*Mar 1 00:58:56.242: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed
state to down
*Mar 1 00:58:58.214: %LINK-5-CHANGED: Interface FastEthernet0/1, changed state to
administratively down
*Mar 1 00:58:58.230: STP: VLAN0001 sent Topology Change Notice on Fa0/3
*Mar 1 00:58:58.230: STP: VLAN0010 sent Topology Change Notice on Fa0/3
*Mar 1 00:58:58.230: STP: VLAN0099 sent Topology Change Notice on Fa0/3
*Mar 1 00:58:59.220: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1,
changed state to down
*Mar 1 00:59:11.233: STP: VLAN0001 Fa0/3 -> learning
*Mar 1 00:59:11.233: STP: VLAN0010 Fa0/3 -> learning
*Mar 1 00:59:11.233: STP: VLAN0099 Fa0/3 -> learning
*Mar 1 00:59:26.240: STP[1]: Generating TC trap for port FastEthernet0/3
*Mar 1 00:59:26.240: STP: VLAN0001 Fa0/3 -> forwarding
*Mar 1 00:59:26.240: STP[10]: Generating TC trap for port FastEthernet0/3
*Mar 1 00:59:26.240: STP: VLAN0010 sent Topology Change Notice on Fa0/3
*Mar 1 00:59:26.240: STP: VLAN0010 Fa0/3 -> forwarding
```

```
*Mar 1 00:59:26.240: STP[99]: Generating TC trap for port FastEthernet0/3
*Mar 1 00:59:26.240: STP: VLAN0099 Fa0/3 -> forwarding
*Mar 1 00:59:26.248: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed
state to up
*Mar 1 00:59:26.248: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed
state to up
```

Примечание. Прежде чем продолжить, исходя из выходных данных команды **debug** убедитесь, что все сети VLAN на интерфейсе F0/3 перешли в состояние пересылки, после чего используйте команду **no debug spanning-tree events**, чтобы остановить вывод данных командой **debug**.

Через какие состояния портов проходит каждая сеть VLAN на интерфейсе F0/3 в процессе схождения сети?

Используя временную метку из первого и последнего сообщений отладки STP, рассчитайте время (округляя до секунды), которое потребовалось для схождения сети. **Рекомендация.** Формат временной метки сообщений отладки: чч.мм.сс.мс

Часть 4: Настройка Rapid PVST+, PortFast, BPDU Guard и проверка СХОДИМОСТИ

В части 4 вам предстоит настроить Rapid PVST+ на всех коммутаторах. Вам необходимо будет настроить функции PortFast и BPDU guard на всех портах доступа, а затем использовать команду **debug** для проверки сходимости Rapid PVST+.

Примечание. Команды, необходимые для выполнения заданий в четвертой части, приведены в приложении А. Проверьте свои знания. Для этого попробуйте настроить Rapid PVST+, PortFast и BPDU guard, не обращаясь к материалам в приложении.

Шаг 1: Настройте Rapid PVST+.

- Настройте S1 для использования Rapid PVST+. Запишите команду в строке ниже.

- Настройте S2 и S3 для Rapid PVST+.

- Проверьте конфигурации с помощью команды **show running-config | include spanning-tree mode**.

```
S1# show running-config | include spanning-tree mode
spanning-tree mode rapid-pvst
```

```
S2# show running-config | include spanning-tree mode
spanning-tree mode rapid-pvst
```

```
S3# show running-config | include spanning-tree mode
spanning-tree mode rapid-pvst
```

Шаг 2: Настройте PortFast и BPDU Guard на портах доступа.

PortFast является функцией протокола spanning-tree, которая переводит порт в состояние пересылки сразу после его включения. Эту функцию рекомендуется использовать при подключении узлов, чтобы они могли начать обмен данными по сети VLAN немедленно, не дожидаясь протокола spanning-tree.

Чтобы запретить портам, настроенным с использованием PortFast, пересылать кадры BPDU, которые могут изменить топологию протокола spanning-tree, можно включить функцию BPDU guard. После получения BPDU функция BPDU Guard отключает порт, настроенный с помощью функции PortFast.

- a. Настройте F0/6 на S1 с помощью функции PortFast. Запишите команду в строке ниже.

- b. Настройте F0/6 на S1 с помощью функции BPDU Guard. Запишите команду в строке ниже.

- c. Глобально настройте все нетранковые порты на коммутаторе S3 с помощью функции PortFast. Запишите команду в строке ниже.

- d. Глобально настройте все нетранковые порты на коммутаторе S3 с помощью функции BPDU. Запишите команду в строке ниже.

Шаг 3: Проверьте сходимость Rapid PVST+.

- a. Выполните команду **debug spanning-tree events** в привилегированном режиме на коммутаторе S3.
b. Измените топологию, отключив интерфейс F0/1 на коммутаторе S3.

```
S3(config)# interface f0/1
S3(config-if)# no shutdown
*Mar 1 01:28:34.946: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up
*Mar 1 01:28:37.588: RSTP(1): initializing port Fa0/1
*Mar 1 01:28:37.588: RSTP(1): Fa0/1 is now designated
*Mar 1 01:28:37.588: RSTP(10): initializing port Fa0/1
*Mar 1 01:28:37.588: RSTP(10): Fa0/1 is now designated
*Mar 1 01:28:37.588: RSTP(99): initializing port Fa0/1
*Mar 1 01:28:37.588: RSTP(99): Fa0/1 is now designated
*Mar 1 01:28:37.597: RSTP(1): transmitting a proposal on Fa0/1
*Mar 1 01:28:37.597: RSTP(10): transmitting a proposal on Fa0/1
*Mar 1 01:28:37.597: RSTP(99): transmitting a proposal on Fa0/1
*Mar 1 01:28:37.597: RSTP(1): updt roles, received superior bpdu on Fa0/1
*Mar 1 01:28:37.597: RSTP(1): Fa0/1 is now root port
*Mar 1 01:28:37.597: RSTP(1): Fa0/3 blocked by re-root
*Mar 1 01:28:37.597: RSTP(1): synced Fa0/1
*Mar 1 01:28:37.597: RSTP(1): Fa0/3 is now alternate
*Mar 1 01:28:37.597: RSTP(10): updt roles, received superior bpdu on Fa0/1
*Mar 1 01:28:37.597: RSTP(10): Fa0/1 is now root port
*Mar 1 01:28:37.597: RSTP(10): Fa0/3 blocked by re-root
*Mar 1 01:28:37.597: RSTP(10): synced Fa0/1
*Mar 1 01:28:37.597: RSTP(10): Fa0/3 is now alternate
*Mar 1 01:28:37.597: RSTP(99): updt roles, received superior bpdu on Fa0/1
```

```
*Mar 1 01:28:37.605: RSTP(99): Fa0/1 is now root port
*Mar 1 01:28:37.605: RSTP(99): Fa0/3 blocked by re-root
*Mar 1 01:28:37.605: RSTP(99): synced Fa0/1
*Mar 1 01:28:37.605: RSTP(99): Fa0/3 is now alternate
*Mar 1 01:28:37.605: STP[1]: Generating TC trap for port FastEthernet0/1
*Mar 1 01:28:37.605: STP[10]: Generating TC trap for port FastEthernet0/1
*Mar 1 01:28:37.605: STP[99]: Generating TC trap for port FastEthernet0/1
*Mar 1 01:28:37.622: RSTP(1): transmitting an agreement on Fa0/1 as a response to a
proposal
*Mar 1 01:28:37.622: RSTP(10): transmitting an agreement on Fa0/1 as a response to a
proposal
*Mar 1 01:28:37.622: RSTP(99): transmitting an agreement on Fa0/1 as a response to a
proposal
*Mar 1 01:28:38.595: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1,
changed state to up
```

Используя временную метку из первого и последнего сообщений отладки RSTP, рассчитайте время, которое потребовалось для схождения сети.

Вопросы на закрепление

1. В чем заключается главное преимущество Rapid PVST+?

2. Каким образом настройка порта с помощью функции PortFast обеспечивает более быстрое схождение?

3. Какую защиту обеспечивает функция BPDU Guard?

Приложение А. Команды настройки коммутатора

Коммутатор S1

```
S1(config)# vlan 10
S1(config-vlan)# name User
S1(config-vlan)# vlan 99
S1(config-vlan)# name Management
S1(config-vlan)# exit
S1(config)# interface f0/6
S1(config-if)# no shutdown
S1(config-if)# switchport mode access
S1(config-if)# switchport access vlan 10
S1(config-if)# interface f0/1
```

```
S1(config-if)# no shutdown
S1(config-if)# switchport mode trunk
S1(config-if)# switchport trunk native vlan 99
S1(config-if)# interface f0/3
S1(config-if)# no shutdown
S1(config-if)# switchport mode trunk
S1(config-if)# switchport trunk native vlan 99
S1(config-if)# interface vlan 99
S1(config-if)# ip address 192.168.1.11 255.255.255.0
S1(config-if)# exit
S1(config)# spanning-tree vlan 1,10,99 root secondary
S1(config)# spanning-tree mode rapid-pvst
S1(config)# interface f0/6
S1(config-if)# spanning-tree portfast
S1(config-if)# spanning-tree bpduguard enable
```

Коммутатор S2

```
S2(config)# vlan 10
S2(config-vlan)# name User
S2(config-vlan)# vlan 99
S2(config-vlan)# name Management
S2(config-vlan)# exit
S2(config)# interface f0/1
S2(config-if)# no shutdown
S2(config-if)# switchport mode trunk
S2(config-if)# switchport trunk native vlan 99
S2(config-if)# interface f0/3
S2(config-if)# no shutdown
S2(config-if)# switchport mode trunk
S2(config-if)# switchport trunk native vlan 99
S2(config-if)# interface vlan 99
S2(config-if)# ip address 192.168.1.12 255.255.255.0
S2(config-if)# exit
S2(config)# spanning-tree vlan 1,10,99 root primary
S2(config)# spanning-tree mode rapid-pvst
```

Коммутатор S3

```
S3(config)# vlan 10
S3(config-vlan)# name User
S3(config-vlan)# vlan 99
S3(config-vlan)# name Management
S3(config-vlan)# exit
S3(config)# interface f0/18
S3(config-if)# no shutdown
S3(config-if)# switchport mode access
```

```
S3(config-if)# switchport access vlan 10
S3(config-if)# spanning-tree portfast
S3(config-if)# spanning-tree bpduguard enable
S3(config-if)# interface f0/1
S3(config-if)# no shutdown
S3(config-if)# switchport mode trunk
S3(config-if)# switchport trunk native vlan 99
S3(config-if)# interface f0/3
S3(config-if)# no shutdown
S3(config-if)# switchport mode trunk
S3(config-if)# switchport trunk native vlan 99
S3(config-if)# interface vlan 99
S3(config-if)# ip address 192.168.1.13 255.255.255.0
S3(config-if)# exit
S3(config)# spanning-tree mode rapid-pvst
```