Усиление функции защиты Portfast BPDU для протокола STP

Содержание

Введение

Данный документ описывает такую функциональную возможность, как защита блока данных протокола моста (BPDU) PortFast. Эта функциональная возможность - одно из улучшений протокола связующего дерева (STP), созданных Cisco. Данная функциональность повышает надежность, управляемость и безопасность коммутируемой сети.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

Эти версии программного обеспечения представили защиту BPDU STP portfast:

- Версия программного обеспечения 5.4.1 Операционной системы Catalyst (CatOS) для Catalyst 4500/4000 (Supervisor Engine II), 5500/5000, 6500/6000, 2926, 2926G, 2948G, и 2980G платформы
- Релиз 12.0 Программного обеспечения Cisco IOS (7) XE для платформ Catalyst 6500/6000
- Cisco IOS Software Release 12.1 (8a) EW для Supervisor Engine III Catalyst 4500/4000

- Cisco IOS Software Release 12.1 (12c) EW для Supervisor Engine IV Catalyst 4500/4000
- Cisco IOS Software Release 12.0 (5) WC5 для Catalyst 2900XL и серии 3500XL
- Программное обеспечение Cisco IOS версии 12.2(11)AX для коммутаторов серии Catalyst 3750
- Программное обеспечение Cisco IOS версии 12.1(14)AX для коммутаторов Catalyst 3750 Metro
- Программное обеспечение Cisco IOS версии 12.1(19)EA1 для коммутаторов серии Catalyst 3560
- Cisco IOS Software Release 12.1 (4) EA1 для Коммутаторов серии Catalyst 3550
- Программное обеспечение Cisco IOS версии 12.2(11)AX для коммутаторов Catalyst 2970 Series
- Программное обеспечение Cisco IOS версии 12.1 (12c) EA1 для коммутаторов серии Catalyst 2955
- Cisco IOS Software Release 12.1 (6) EA2 для Коммутаторов серии Catalyst 2950
- Программное обеспечение Cisco IOS версии 12.1(11)EA1 для коммутаторов Long-Reach Ethernet (LRE) Catalyst 2950
- Программное обеспечение Cisco IOS версии 12.1(13)AY для коммутаторов серии Catalyst 2940

Примечание: Защита BPDU STP portfast не доступна для серии Catalyst 8500, 2948G-L3 или коммутаторов 4908G-L3.

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Условные обозначения

Дополнительные сведения об условных обозначениях см. в документе Условные обозначения технических терминов Cisco.

Описание функции

STP перенастраивает ячеистую топологию в свободную от петель древоподобную структуру. При включении канала в порту моста, в данном порту осуществляется вычисление STP. Результатом вычисления станет переход порта в состояние пересылки или блокировки. Этот результат зависит от положения порта в сети и параметров STP. Вычисление и переходный период занимают, как правило, от 30 до 50 секунд. В течение этого времени данные пользователя через порт не проходят. За этот период время ожидания некоторых пользовательских приложений может истечь.

Для немедленного перехода порта в состояние пересылки активизируйте функцию STP PortFast. Portfast переводит порт в режим пересылки STP сразу после включения канала. При этом порт все еще участвует в STP. Таким образом, если порт должен являться частью цикла, он в конечном итоге переходит в режим блокировки STP.

Так как данный порт участвует в STP, какое-то устройство может взять на себя функцию корневого моста и повлиять на активную STP топологию. Для осуществления функции корневого моста, данное устройство должно подключиться к порту и запустить STP с

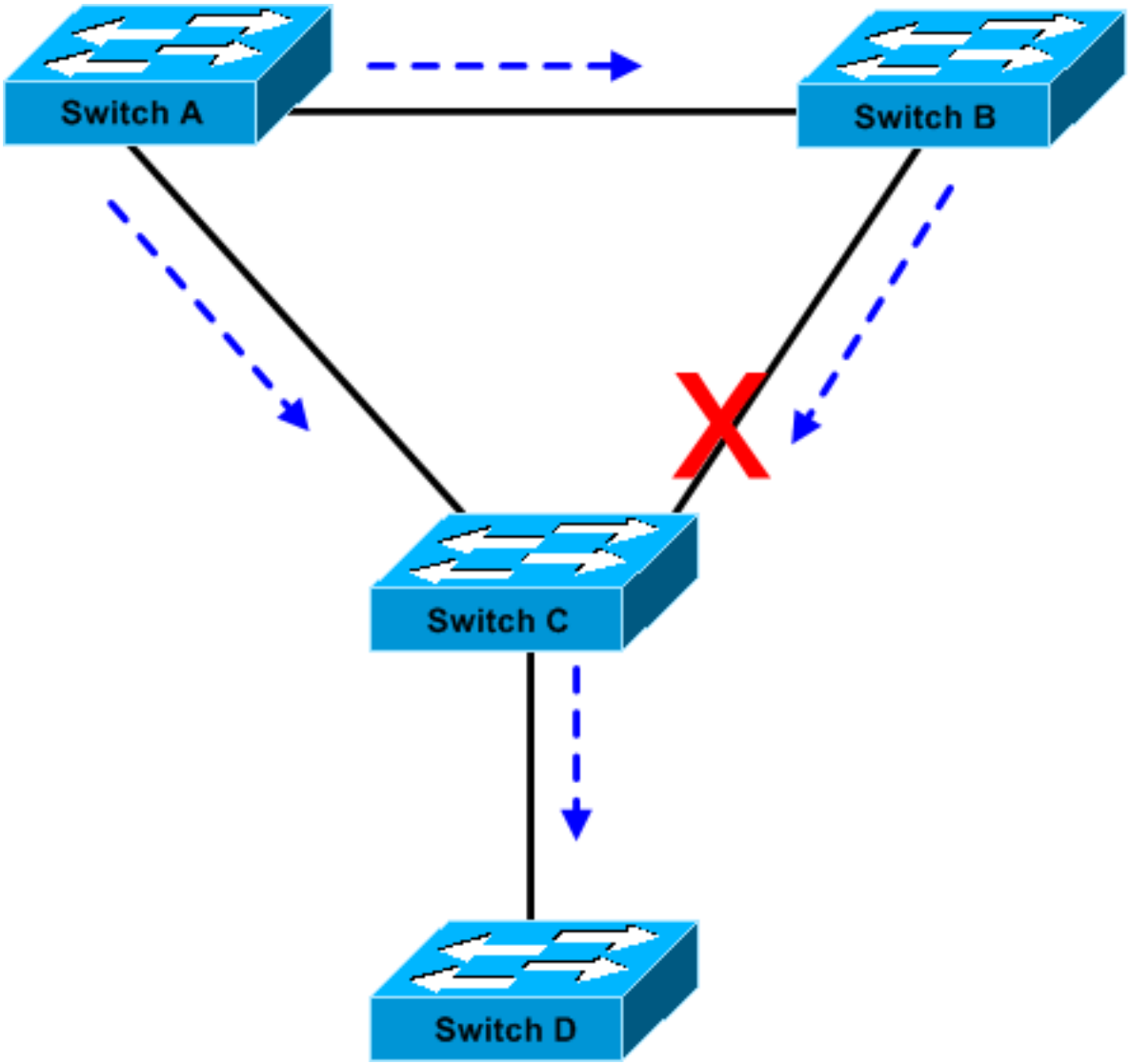
приоритетом моста более низким, чем у текущего корневого моста. Если другое устройство таким образом берет на себя функцию корневого моста, оно приводит сеть в условно оптимальное состояние. Это представляет собой простую форму атаки на сеть типа "отказ в обслуживании" (DoS). Временное введение и последующее удаление STP устройств с низким (0) приоритетом моста приводит к постоянному пересчету STP.

Новая функция STP PortFast защиты BPDU позволяет разработчикам сетей устанавливать границы домена STP и сохранять предсказуемость активной топологии. Устройства, находящиеся в сети после портов с включенной функцией STP PortFast, не могут повлиять на топологию STP. При приеме BPDU операция защиты BPDU отключает порт, работающий в режиме PortFast. Защита BPDU переводит порт в состояние отключения в результате ошибки и выводит на консоль сообщение. Например, сообщение может быть следующим:

```
2000 May 12 15:13:32 %SPANTREE-2-RX_PORTFAST:Received BPDU on PortFast enable port.
Disabling 2/1
2000 May 12 15:13:32 %PAGP-5-PORTFROMSTP:Port 2/1 left bridge port 2/1
```

Рассмотрим следующий пример:

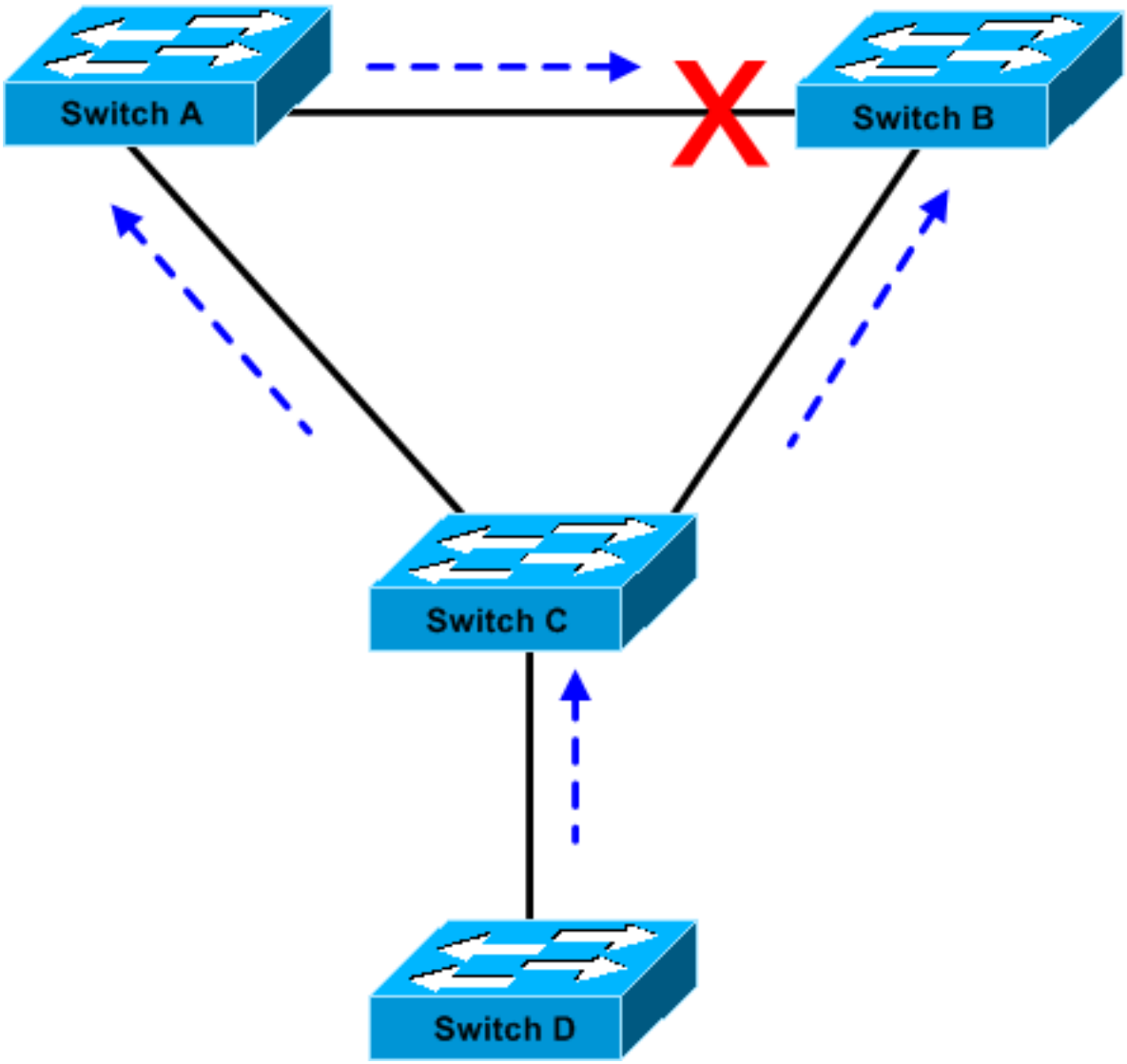
Рисунок 1



Мост A имеет приоритет 8192 и является корневым для VLAN. Мост B имеет приоритет, равный 16384, и является резервным корневым мостом для той же сети VLAN. Мосты A и B, соединенные каналом Gigabit Ethernet, образуют ядро сети. Мост C является коммутатором

доступа и имеет работающий в режиме PortFast порт, подключающий его к устройству D. Если стандартными являются другие параметры STP, то порт моста C, соединяющий его с мостом B, находится в состоянии блокировки STP. Устройство D (ПК) не является частью STP. Пунктирные стрелки указывают поток протокольных информационных единиц моста STP.

Рис. 2



На рисунке 2 устройство D становится частью STP. Например, на ПК запущено приложение, работающее на базе Linux. Если приоритет программного моста равен 0 или его приоритет ниже приоритета корневого моста, программный мост берет на себя функцию корневого. Канал Gigabit Ethernet, соединяющий два основных коммутатора, переходит в режим блокировки. Такой переход вызывает поток всех данных в этой VLAN через канал с пропускной способностью 100 Мбит/с. Если через ядро этой VLAN проходит больше данных, чем канал может вместить, некоторые кадры будут сброшены. Сброс кадров приводит к потере соединения.

Функция STP PortFast защиты BPDU предотвращает возникновение подобной ситуации. Функция отключает порт, как только мост C получает BPDU STP от устройства D.

!--- конфигурацию

Вы можете подключить или отключить функцию STP PortFast глобальной защиты BPDU, которая затронет все порты, имеющие функцию PortFast. По умолчанию защита BPDU STP отключена. Введите следующую команду для того, чтобы включить функцию STP PortFast защиты BPDU для коммутатора:

Команда CatOS

```
Console> (enable) set spantree portfast bpdu-guard enable

Spantree portfast bpdu-guard enabled on this switch.

Console> (enable)
```

Команда ПО Cisco IOS

```
CatSwitch-IOS(config)# spanning-tree portfast bpduguard
CatSwitch-IOS(config)
```

Когда защита BPDU STP отключает порт, порт остается выключенным до тех пор, пока его не включат вручную. Вы можете настроить порт таким образом, чтобы после перехода в состояние отключения в результате ошибки он включался автоматически. **Введите следующие команды, устанавливающие интервал времени ожидания при отключении в результате ошибки и включающие функцию времени ожидания:**

Команды CatOS

```
Console> (enable) set errdisable-timeout interval 400

Console> (enable) set errdisable-timeout enable bpdu-guard
```

Команды ПО Cisco IOS

```
CatSwitch-IOS(config)# errdisable recovery cause bpduguard

CatSwitch-IOS(config)# errdisable recovery interval 400
```

Примечание: Интервал времени ожидания по умолчанию составляет 300 секунд и, по умолчанию, функция timeout (таймаут) отключена.

Мониторинг

Для того, чтобы проверить, включена ли эта функция, введите следующую команду:

Выходные данные команд

Команда CatOS

```
Console> (enable) show spantree summary
Root switch for vlans: 3-4.
Portfast bpdu-guard enabled for bridge.
Uplinkfast disabled for bridge.
Backbonefast disabled for bridge.

Summary of Connected Spanning Tree Ports By VLAN:

Vlan  Blocking Listening Learning Forwarding STP Active
```

```
----- -------- --------- -------- ---------- ----------

   1         0         0        0          1          1

   3         0         0        0          1          1

   4         0         0        0          1          1

  20         0         0        0          1          1


Blocking Listening Learning Forwarding STP Active

----- -------- --------- -------- ---------- ----------

Total        0         0        0          4          4

Console> (enable)
```

Команда ПО Cisco IOS

```
CatSwitch-IOS# show spanning-tree summary totals
Root bridge for: none.
PortFast BPDU Guard is enabled
UplinkFast is disabled
BackboneFast is disabled
Spanning tree default pathcost method used is short


Name                 Blocking Listening Learning Forwarding STP Active
-------------------- -------- --------- -------- ---------- ----------
  1 VLAN                  0         0         0         1          1

CatSwitch-IOS#
```

Дополнительные сведения

- Страницы поддержки продуктов LAN
- Страница поддержки коммутационных решений для локальной сети
- Cisco Systems – техническая поддержка и документация