



# Улучшенная функция протокола связующего дерева - защита BPDU Portfast

---

## Содержание

### Общие сведения

#### Предварительные условия

Требования

Используемые компоненты

Условные обозначения

#### Описание функции

Рисунок 1

Рисунок 2

#### Настройка

#### Мониторинг

Выходные данные команды

#### Дополнительные сведения

---

## Общие сведения

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 данного документа специфических требований нет.

### Используемые компоненты

Следующие версии ПО включили в себя защиту STP PortFast BPDU:

- ОС Catalyst (CatOS) версии 5.4.1 для платформ Catalyst 4500/4000 (Supervisor Engine II), 5500/5000, 6500/6000, 2926, 2926G, 2948G и 2980G;
- Программное обеспечение Cisco IOS® выпуска 12.0(7)XE для платформ Catalyst 6500/6000;
- Программное обеспечение Cisco IOS выпуска 12.1(8a)EW для Catalyst 4500/4000 Supervisor Engine III;
- Программное обеспечение Cisco IOS выпуска 12.1(12c)EW для Catalyst 4500/4000 Supervisor Engine IV;
- Программное обеспечение Cisco IOS выпуска 12.0(5)WC5 для серии Catalyst 2900XL и 3500XL;
- Программное обеспечение Cisco IOS выпуска 12.1(11)AX для коммутаторов серии Catalyst 3750;
- Программное обеспечение Cisco IOS выпуска 12.1(14)AX для коммутаторов Catalyst 3750 Metro;
- Программное обеспечение Cisco IOS выпуска 12.1(19)EA1 для коммутаторов серии Catalyst 3560;

- Программное обеспечение Cisco IOS выпуска 12.1(4)EA1 для коммутаторов серии Catalyst 3550;
- Программное обеспечение Cisco IOS выпуска 12.1(11)AX для коммутаторов серии Catalyst 2970;
- Программное обеспечение Cisco IOS выпуска 12.1(12c)EA1 для коммутаторов серии 2955;
- Программное обеспечение Cisco IOS выпуска 12.1(6)EA2 для коммутаторов серии Catalyst 2950;
- Программное обеспечение Cisco IOS выпуска 12.1(11)EA1 для коммутаторов Long-Reach Ethernet (LRE) Catalyst 2950;
- Программное обеспечение Cisco IOS выпуска 12.1(13)AY для коммутаторов серии Catalyst 2940.

**Примечание.** Функция STP PortFast защиты BPDU *не* является доступной для коммутаторов серии Catalyst 8500, 2948G-L3 или 4908G-L3.

Информация, содержащаяся в данном документе, была получена в специально созданных лабораторных условиях. Все устройства, описанные в данном документе, начинали работу с очищенной (стандартной) конфигурацией. При работе с реально функционирующей сетью необходимо полностью осознавать возможные результаты использования всех команд.

## Условные обозначения

См. "Технические рекомендации Cisco. Условные обозначения" для получения дополнительной информации об условных обозначениях, встречающихся в данном документе.

## 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.

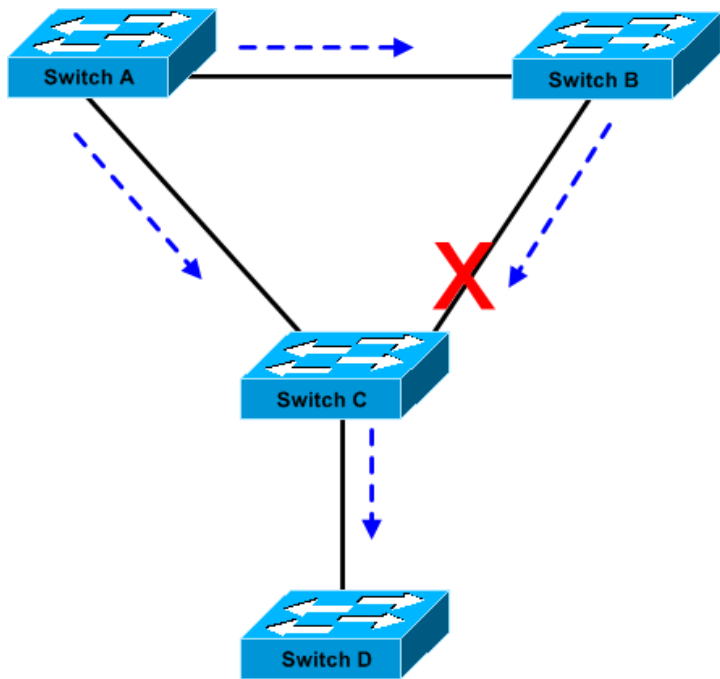
Так как данный порт участвует в STP, какое-то устройство может взять на себя функцию корневого моста и повлиять на активную STP топологию. Для осуществления функции корневого моста, данное устройство должно подключиться к порту и запустить STP с приоритетом моста более низким, чем у текущего корневого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

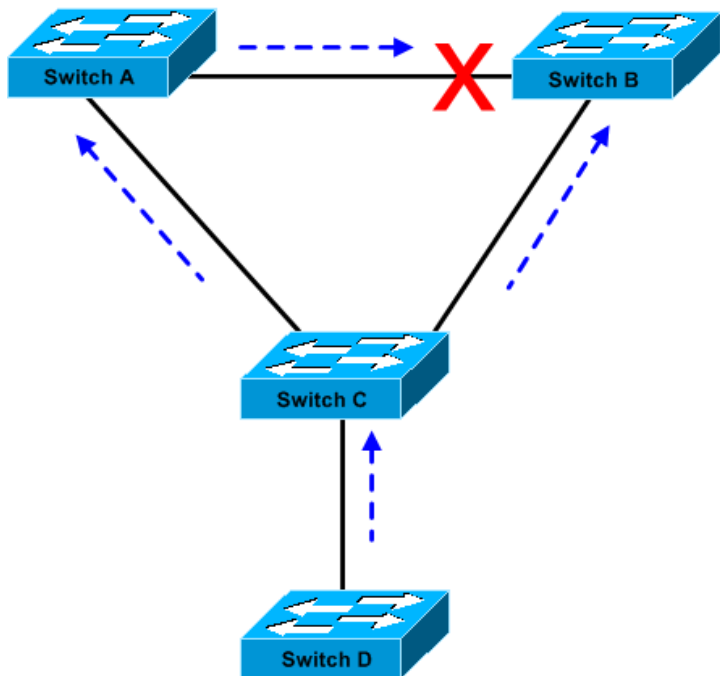
Рассмотрим следующий пример:

## Рисунок 1



Мост А имеет приоритет 8192 и является корневым для VLAN. Мост В имеет приоритет 16384 и является резервным корневым мостом для той же сети VLAN. Мосты А и В, соединенные каналом Gigabit Ethernet, образуют ядро сети. Мост С является коммутатором доступа и имеет работающий в режиме PortFast порт, подключающий его к устройству D. Если стандартными являются другие параметры STP, то порт моста С, соединяющий его с мостом В, находится в состоянии блокировки STP. Устройство D (ПК) не является частью STP. Пунктирные стрелки обозначают направление потока STP BPDU.

**Рисунок 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. Эта функция отключает порт в тот самый момент, когда мост С получает STP BPDU от устройства D.

# Настройка

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:** По умолчанию время ожидания составляет 300 секунд, а функция отключения по таймауту ожидания отключена.

# Мониторинг

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

## Выходные данные команды

## 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 коммутации LAN](#)
- [Техническая поддержка и документация - Cisco Systems](#)

---

© 1992-2010 Cisco Systems, Inc. Все права защищены.

---

Дата генерации PDF файла: Jan 05, 2010

---

<http://www.cisco.com/support/RU/customer/content/9/92091/65.shtml>

---