Усиление протокола STP с помощью функций защиты от петель и обнаружения отклонений BPDU

Содержание

Введение

Протокол STP разрешает физически избыточные топологии в древовидные топологии без петель. Самая большая проблема протокола STP заключается в том, что некоторые отказы оборудования могут вызывать сбой этого протокола. Такой сбой приводит к образованию петель пересылки (или петель STP). Петли STP вызывают серьезные перебои в работе сети.

В данном документе описана функция защиты от петель STP, предназначенная для повышения стабильности сетей уровня 2 (L2). Здесь также описывается функция обнаружения потери BPDU. Функция обнаружения потери BPDU представляет собой средство диагностики, которое создает сообщения системного журнала, если пакеты BPDU не получены в надлежащий срок.

Предварительные условия

Требования

В данном документе предполагается, что читатель знаком с принципами работы протокола STP. С принципами работы протокола STP можно ознакомиться в документе Общее описание протокола STP и его настройка на коммутаторах Catalyst.

Используемые компоненты

Содержимое данного документа не ограничивается определенными версиями оборудования и программного обеспечения.

Условные обозначения

Подробное описание условных обозначений, используемых в документах, см. в документе Cisco Technical Tips Conventions (Условные обозначения, используемые в технической документации Cisco).

Доступность функций

CatOS

- Функция защиты от петель STP была впервые реализована в CatOS версии 6.2.1 программы Catalyst для платформ Catalyst 4000 и Catalyst 5000 и в версии 6.2.2 для платформы Catalyst 6000.
- Функция обнаружения потери BPDU впервые реализована в CatOS версии 6.2.1 программы Catalyst для платформ Catalyst 4000 и Catalyst 5000 и в версии 6.2.2 для платформы Catalyst 6000.

Cisco IOS®

- Функция защиты от петель STP впервые реализована в ПО Cisco IOS выпуска 12.1(12c)EW для коммутаторов Catalyst 4500 и в ПО Cisco IOS выпуска 12.1(11b)EX для Catalyst 6500.
- Функция обнаружения потери BPDU не поддерживается коммутаторами Catalyst с системным ПО Cisco IOS.

Краткое описание ролей портов протокола STP

Для внутренних целей протокол STP каждому порту моста (или коммутатора) назначает роль на основе конфигурации, топологии, относительного положения порта в топологии и других факторов. Роль порта определяет поведение порта с точки зрения протокола STP. В зависимости от назначенной роли порт либо отправляет, либо принимает пакеты BPDU протокола STP и пересылает или блокирует трафик данных. В следующем списке приведено краткое описание каждой роли порта STP.

- *Назначенный.* Для каждого соединения (сегмента) выбирается один назначенный порт. Назначенный порт — это порт, ближайший к корневому мосту. Этот порт отправляет пакеты BPDU по этому соединению (сегменту) и пересылает трафик на корневой мост. В сети с топологией сходимости STP все назначенные порты находятся в состоянии пересылки STP.
- *Корневой.* У моста может быть только один корневой порт. Корневой порт — это порт, ведущий к корневому мосту. В сети с топологией сходимости STP корневой порт находится в состоянии пересылки STP.
- *Альтернативный.* Альтернативные порты ведут к корневому мосту, но не являются корневыми портами. Альтернативные порты поддерживают состояние блокировки STP.
- *Резервный.* Это особый случай, когда два или более портов одного моста (коммутатора) связаны между собой напрямую или через общий носитель. В этом случае один порт

является назначенным, а остальные порты блокируются. Такой порт имеет роль резервного.

Защита от петель STP

Описание функции

Функция защиты от петель STP обеспечивает дополнительную защиту от петель пересылки на уровне 2 (петель STP). Петля STP образуется, когда заблокированный порт STP в избыточной топологии ошибочно переходит в состояние пересылки. Обычно причина этого в том, что один из портов физически избыточной топологии (не обязательно заблокированный порт STP) перестает получать пакеты BPDU протокола STP. Работа протокола STP зависит от непрерывного приема и передачи пакетов BPDU на основе роли порта. Назначенный порт передает пакеты BPDU, а неназначенный порт получает пакеты BPDU.

Когда один из портов в физически избыточной топологии перестает принимать пакеты BPDU, протокол STP считает такую топологию как топологию без петель. В итоге заблокированный порт из альтернативного или резервного порта превращается в назначенный и переходит в состояние пересылки. В такой ситуации образуется петля.

Функция защиты от петель выполняет дополнительные проверки. Если пакеты BPDU больше не принимаются неназначенным портом, а защита от петель включена, то такой порт переводится в состояние блокировки вследствие возможности петли STP, а не в состояние прослушивания, самообучения (learning) или пересылки. Без функции защиты от петель порт принимает роль назначенного порта. Порт переходит в состояние пересылки STP и формирует петлю.

Когда защита от петель блокирует несогласованный порт, в журнале регистрируется следующее сообщение:

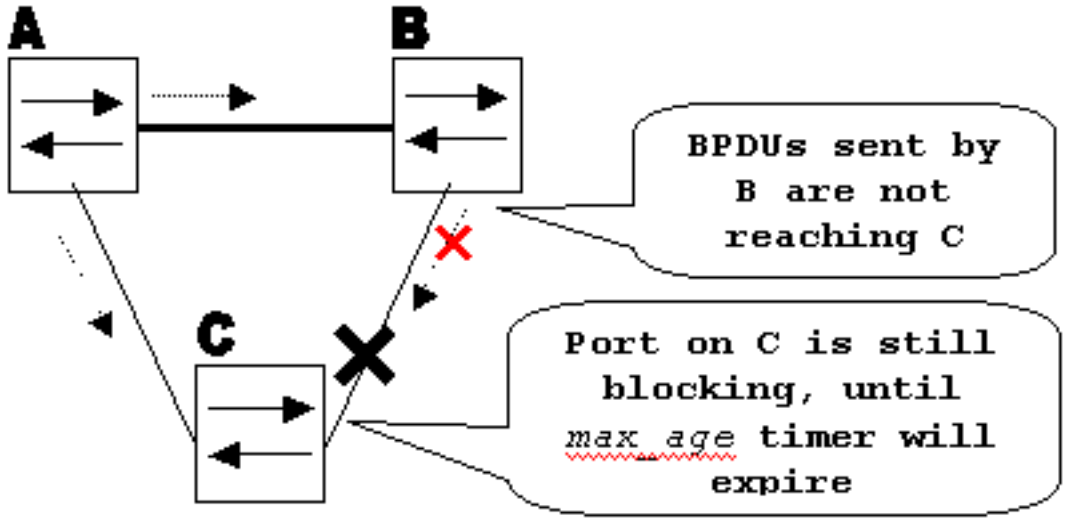
- CatOS
- Cisco IOS

Когда пакет BPDU принимается портом в состоянии блокировки вследствие возможности петли STP, этот порт переходит в другое состояние STP. Согласно полученному блоку BPDU это значит, что восстановление выполнено автоматически и вмешательство не требуется. После восстановления в журнале регистрируется следующее сообщение:

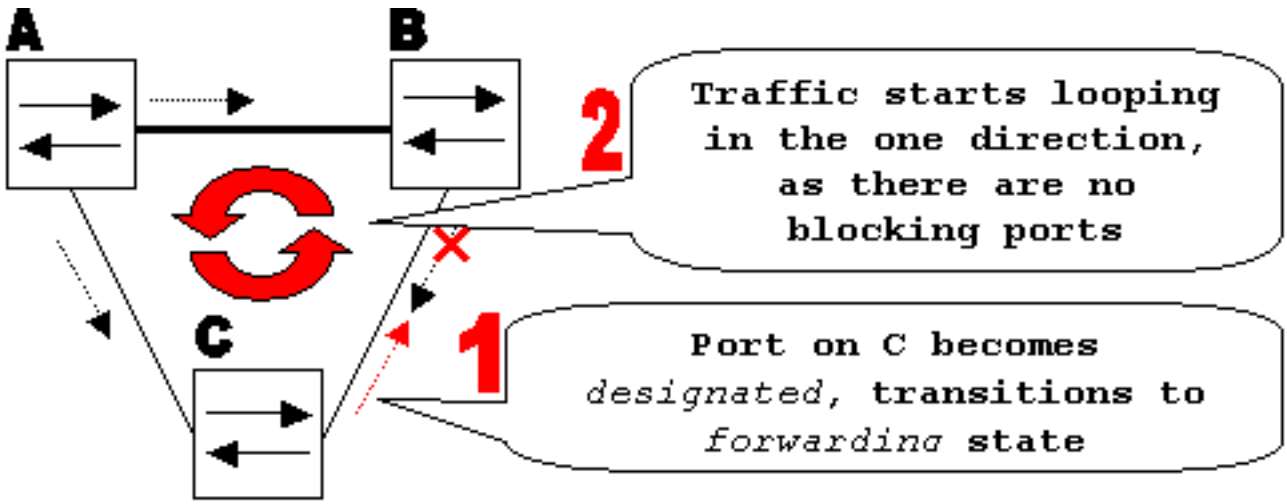
- CatOS
- Cisco IOS

Чтобы проиллюстрировать это поведение, рассмотрим следующий пример.

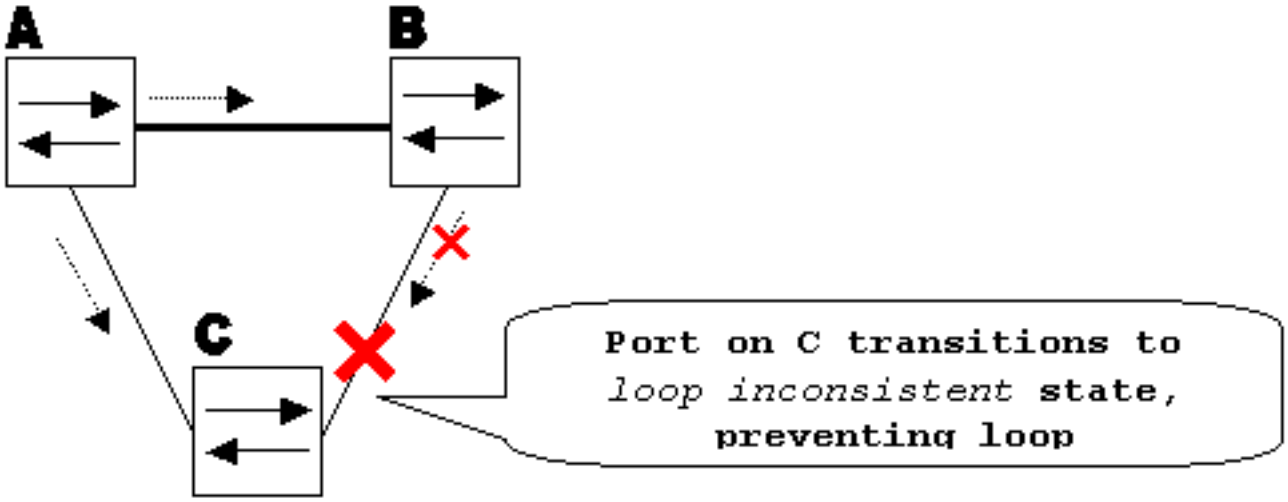
Коммутатор A является корневым коммутатором. Коммутатор C не получает пакеты BPDU от коммутатора B из-за сбоя однонаправленного соединения между коммутатором B и коммутатором C.



Без защиты от петель заблокированный порт STP на коммутаторе C переходит в состояние прослушивания STP по истечении времени, задаваемого таймером max_age, а затем переходит в состояние пересылки через промежуток, равный удвоенному значению forward_delay. В такой ситуации образуется петля.



Когда функция защиты от петель включена, после обнуления таймера max_age заблокированный порт на коммутаторе C переходит в состояние блокировки вследствие возможности петли STP. Порт в состоянии блокировки вследствие возможности петли STP не предает пользовательский трафик, поэтому петля не образуется. (Состояние блокировки вследствие возможности петли фактически эквивалентно состоянию блокировки.)

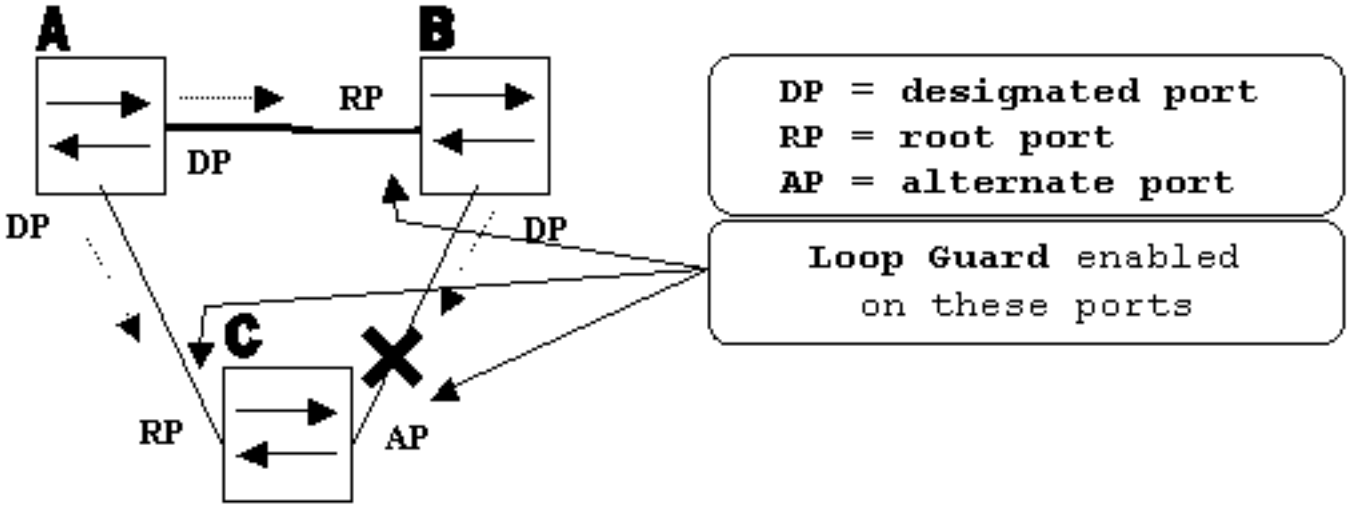


Замечания по настройке

Функция защиты от петель включается для каждого порта отдельно. Однако поскольку функция защиты от петель блокирует порт на уровне STP, она блокирует несогласованные порты для каждой VLAN по отдельности (поскольку протокол STP настроен отдельно для каждой VLAN). Значит, если пакеты BPDU не принимаются на магистральном порту только одной отдельной VLAN, то блокируется только эта VLAN (переводится в состояние блокировки вследствие возможности петли STP). По этой же причине, если эта функция включена в интерфейсе EtherChannel, блокируется весь канал отдельной VLAN, а не только одно соединение (так как EtherChannel с точки зрения протокола STP является одним логическим портом).

На каких портах должна быть включена защита от петель? Наиболее очевидный ответ: на заблокированных портах. Однако это не совсем верно. Защита от петель должна быть включена на неназначенных портах (точнее, на корневых и альтернативных портах) для всех возможных комбинаций активных топологий. Поскольку защита от петель не устанавливается для каждой VLAN по отдельности, один и тот же (магистральный) порт может быть назначенным в одной сети VLAN (VLAN) и неназначенным в другой. Следует также учитывать возможные сценарии перехода на другой ресурс при сбое.

Рассмотрим следующий пример.



По умолчанию защита от петель отключена. Для включения защиты от петель используется следующая команда:

- CatOS
  set spantree guard loop <mod/port>

  ```
  Console> (enable) set spantree guard loop 3/13
  Enable loopguard will disable rootguard if it's currently enabled on the port(s).
  Do you want to continue (y/n) [n]? y
  Loopguard on port 3/13 is enabled.
  ```
- Cisco IOS
  spanning-tree guard loop

  ```
  Router(config)#interface gigabitEthernet 1/1
  Router(config-if)#spanning-tree guard loop
  ```

Начиная с версии 7.1(1) ПО Catalyst (CatOS), защита от петель может включаться глобально на всех портах. Фактически защита от петель включается на всех соединениях "точка-точка". Соединение "точка-точка" определяется по состоянию дуплексной передачи соединения. Если настроен полнодуплексный режим, соединение считается соединением "точка-точка". Еще можно настроить или переопределить глобальные настройки для каждого порта по отдельности.

Чтобы включить защиту от петель глобально, выполните следующую команду:

- CatOS`Console> (enable) set spantree global-default loopguard enable`
- Cisco IOS`Router(config)#spanning-tree loopguard default`

Чтобы отключить защиту от петель, выполните следующую команду:

- CatOS`Console> (enable) set spantree guard none <mod/port>`
- Cisco IOS`Router(config-if)#no spanning-tree guard loop`

Чтобы отключить защиту от петель глобально, выполните следующую команду:

- CatOS`Console> (enable) set spantree global-default loopguard disable`
- Cisco IOS`Router(config)#no spanning-tree loopguard default`

Чтобы проверить состояние защиты от петель, выполните следующую команду:

- CatOS
  show spantree guard <mod/port>

  ```
  Console> (enable) show spantree guard 3/13
  Port                     VLAN Port-State    Guard Type
  ------------------------ ---- ------------- ----------
  3/13                     2    forwarding          loop
  Console> (enable)
  ```
- Cisco IOS
  show spanning-tree

  ```
  Router#show spanning-tree summary
  Switch is in pvst mode
  Root bridge for: none
  EtherChannel misconfig guard is enabled
  Extended system ID           is disabled
  Portfast Default             is disabled
  PortFast BPDU Guard Default  is disabled
  Portfast BPDU Filter Default is disabled
  Loopguard Default            is enabled
  ```

```
UplinkFast                    is disabled
BackboneFast                  is disabled
Pathcost method used          is short

Name                   Blocking Listening Learning Forwarding STP Active
---------------------- -------- --------- -------- ---------- ----------
Total                         0         0        0          0          0
```

Сравнение функций защиты от петель и UDLD

Защита от петель и UDLD (обнаружение однонаправленной связи) функционально пересекаются, частично из-за того, что обе эти функции защищают от сбоев протокола STP, вызванных однонаправленными соединениями. Однако эти функции различаются как функционально, так и по способу решения этой проблемы. В следующей таблице описываются функциональные возможности защиты от петель и UDLD:

Функция	Защита от петель	UDLD
Конфигурация	Для каждого порта	Для каждого порта
Возможность настройки действий	Для каждой VLAN	Для каждого порта
Автоматическое восстановление	Да	Да, с функцией тайм-аута состояния "err-disable"
Защита от сбоев STP, вызванных однонаправленными соединениями	Да, когда включена на всех корневых и альтернативных портах в избыточной топологии	Да, когда включена для всех соединений в избыточной топологии
Защита от сбоев STP, вызванных проблемами ПО (выделенный коммутатор не отправляет блоки BPDU)	Да	Нет
Защита от неправильных кабельных соединений.	Нет	Да

В зависимости от конкретных особенностей проекта можно выбрать функцию UDLD или защиту от петель. В отношении протокола STP наиболее заметное различие между этими двумя функциями заключается в отсутствии у UDLD защиты от сбоев STP, вызванных проблемами ПО. В результате выделенный коммутатор не отправляет пакеты BPDU. Однако сбои такого типа происходят (в десятки раз) реже, чем сбои, вызванные однонаправленными соединениями. В свою очередь, функция UDLD может быть более гибкой в случае однонаправленных соединений в EtherChannel. В этом случае UDLD отключает только неисправные соединения, а канал сохраняет работоспособность за счет

оставшихся соединений. При таком сбое защита от петель переводит порт в состоянии блокировки вследствие возможности петли, чтобы блокировать весь канал.

Кроме того, защита от петель не действует на совместно используемых соединениях и в ситуациях, когда с момента соединения соединение является однонаправленным. В последнем случае порт никогда не получает блоки BPDU и становится назначенным. Так как такое поведение может быть нормальным, этот случай не охватывается защитой от петель. Защиту от такого сценария предоставляет UDLD.

Как уже отмечено, самый высокий уровень защиты обеспечивается, когда включены функции UDLD и защиты от петель.

Взаимодействие защиты от петель с другими функциями STP

Защита корня дерева STP

Функции защиты корня дерева STP и защиты от петель являются взаимоисключающими. Защита корня дерева STP используется на назначенных портах и не разрешает порту изменять состояние. Защита от петель действует на неназначенных портах и разрешает порту становиться назначенным по истечении срока max_age. Защиту корня дерева STP нельзя включить для порта, на котором включена защита от петель. Когда для порта включается защита от петель, она отключает настроенную на этом порте защиту корня дерева STP.

Функции uplink fast и backbone fast

Функции uplink fast и backbone fast прозрачны для защиты от петель. Когда во время повторной конвергенции функция backbone fast пропускает max_age, это не вызывает срабатывание защиты от петель. Дополнительные сведения о функциях uplink fast и backbone fast см. в следующих документах:

- Общее описание и настройка функции Cisco uplink fast
- Общее описание и настройка функции backbone fast на коммутаторах Catalyst

PortFast и защита BPDU и динамическая виртуальная ЛС

Защиту от петель нельзя включить для портов, на которых включена функция PortFast. Так как защита BPDU действует на портах с включенной функцией portfast, к защите BPDU применяются некоторые ограничения. Защиту от петель нельзя включить на портах динамической виртуальной сети, так как на таких портах уже включена функция portfast.

Совместно используемые соединения

Защиту от петель не следует включать на совместно используемых соединениях. Если защиту от петель включить на совместно используемых соединениях, то трафик от узлов, подключенных к общим сегментам, может блокироваться.

Множественные связующие деревья (MST)

Защита от петель правильно функционирует в среде MST.

Обнаружение потери BPDU

Функция защиты от петель должна правильно взаимодействовать с функцией обнаружения потери BPDU.

Обнаружение потери BPDU

Описание функции

Работа протокола STP сильно зависит от своевременного получение пакетов BPDU. При каждом сообщении hello_time message (по умолчанию каждые 2 секунды) корневой мост отправляет пакеты BPDU. Некорневые мосты не создают пакеты BPDU заново для каждого сообщения hello_time, а принимают пакеты BPDU, ретранслированные от корневого моста. Поэтому каждый некорневой мост должен получать пакеты BPDU в каждой VLAN для каждого сообщения hello_time. В некоторых случаях пакеты BPDU теряются или ЦП моста слишком занят, чтобы своевременно ретранслировать пакеты BPDU. Такие или другие проблемы могут вызвать запаздывание пакетов BPDU (если они вообще получаются). Эта проблема может нарушить стабильность топологии STP.

Обнаружение потери BPDU позволяет коммутатору отслеживать запаздывающие пакеты BPDU и уведомлять администратора с помощью сообщений системного журнала. Для каждого порта, для которого когда-либо было зафиксировано запаздывание (или искажение) пакета BPDU, функция обнаружения задержки сообщит о самой последней задержке с указанием ее длительности. Она также указывает максимальную длительность задержки блока BPDU для этого конкретного порта.

Чтобы защитить ЦП моста от перегрузки, сообщение системного журнала создается не при каждой задержке пакета BPDU. Частота создания сообщений ограничивается одним сообщением каждые 60 секунд. Однако если задержка BPDU превышает значение max_age, деленное на 2 (что по умолчанию равно 10 с), сообщение печатается немедленно.

Примечание: Обнаружения потери BPDU — это функция диагностики. При обнаружении задержки пакетов BPDU она отправляет сообщение системного журнала. Функция обнаружения потери BPDU не выполняет никаких других корректирующих действий.

Пример сообщения системного журнала, созданного функцией обнаружения потери BPDU:

show spanning-tree

```
Router#show spanning-tree summary
Switch is in pvst mode
Root bridge for: none
EtherChannel misconfig guard is enabled
Extended system ID           is disabled
Portfast Default             is disabled
PortFast BPDU Guard Default  is disabled
Portfast BPDU Filter Default is disabled
Loopguard Default            is enabled
UplinkFast                   is disabled
BackboneFast                 is disabled
Pathcost method used         is short

Name                   Blocking Listening Learning Forwarding STP Active
---------------------- -------- --------- -------- ---------- ----------
Total                         0         0        0          0          0
```

Замечания по настройке

Обнаружение потери BPDU настраивается для каждого коммутатора по отдельности. По умолчанию эта функция отключена. Чтобы включить обнаружение потери BPDU, выполните следующую команду:

```
Cat6k> (enable) set spantree bpdu-skewing enable
   Spantree bpdu-skewing enabled on this switch.
```

Чтобы просмотреть сведения об обнаружении задержки пакетов BPDU, воспользуйтесь командой **show spantree bpdu-skewing <*vlan*>|<*mod/port*>** как показано в следующем примере:

```
Cat6k> (enable) show spantree bpdu-skewing 1
Bpdu skewing statistics for vlan 1
Port Last Skew (ms) Worst Skew (ms) Worst Skew Time
------------- -------------- -------------- ------------------------
3/12 4000 4100 Mon Nov 19 2001, 16:36:04
```

Дополнительные сведения

- Усиление функции защиты корня дерева STP
- Усиление функции защиты Portfast BPDU для протокола STP
- Общее описание и настройка функции протокола ULDP
- Страницы поддержки продуктов для локальных сетей
- Страница поддержки для коммутаторов локальных сетей
- Техническая поддержка и документация — Cisco Systems