Ошибки протокола STP и соответствующие рекомендации по разработке

Содержание

Введение

В этом документе представлен список рекомендаций, которые помогут в построении безопасной сети с использованием мостов для коммутаторов Cisco Catalyst, использующих

Catalyst OS (CatOS) и программное обеспечение Cisco IOS®. В данном документе рассматриваются несколько общих причин неисправностей протокола связующего дерева (STP) и информация, которая поможет установить источник проблем. В документе также представлена примерная схема, которая поможет свести к минимуму количество проблем с STP и в которой легко устраняются неисправности.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

Настоящий документ не имеет жесткой привязки к каким-либо конкретным версиям программного обеспечения и оборудования.

Условные обозначения

Дополнительные сведения об условных обозначениях см. в документе Технические рекомендации Cisco. Условные обозначения.

Общие сведения

В этом документе не рассматриваются базовые операции STP. Описание работы STP можно просмотреть в следующем документе:

- Общие сведения и настройка протокола связующего дерева (STP) в коммутаторах Catalyst

В этом документе не рассматривается протокол Rapid STP (RSTP), определенный в IEEE 802.1w. Кроме того, в данном документе не рассматривается протокол MST (протокол множественных связующих деревьев), определенный в IEEE 802.1s. Более подробную информацию по протоколам RSTP и MST см. в следующей документации:

- Общие сведения о протоколе MSTP (протокол с несколькими связующими деревьями, 802.1s)
- Общие сведения о протоколе Rapid STP (802.1w)

Для более определенного документа Устранения проблем STP для Коммутаторов Catalyst, которые выполняют программное обеспечение Cisco IOS, обратитесь к документу, Устраняющему неполадки STP на Коммутаторе Catalyst Рабочая Cisco Интегрированный IOS (Режим работы в собственной системе команд).

Сбой Spanning Tree Protocol

Основная функция алгоритма связующего дерева (STA) заключается в отсечении петель, созданных резервными каналами связи в сетях с мостовыми подключениями. STP работает на уровне 2 модели взаимодействия открытых систем (OSI). При помощи BPDU (сообщения протокола моста), которыми обмениваются мосты, STP выбирает порты, которые

пересылают или блокируют трафик. В некоторых конкретных случаях может произойти сбой данного протокола и, в зависимости от схемы сети, решить данную проблему бывает очень сложно. В этой определенной области самая главная часть устранения неисправностей проводится еще до того, как возникнет проблема.

Сбой работы протокола STA обычно приводит к возникновению мостовой петли. Большинство клиентов, звонящих в центр технической поддержки Cisco по вопросам неисправностей с протоколом связующего дерева, подозревают в их происхождении наличие ошибок, однако ошибки редко являются причинами этих неисправностей. Даже если это проблема программного обеспечения, мостовая петля в среде STP все равно будет возникать из-за порта, который должен блокировать трафик, однако вместо этого он его пересылает.

Сходимость связующего дерева

Пример первоначального схождения связующего дерева можно просмотреть во flash-анимации работы протокола связующего дерева . В примере также разъясняется, почему заблокированный порт переходит в режим пересылки из-за избыточных потерь BPDU, что приводит к сбоям в работе протокола STA.

Остальная часть данного документа содержит список различных ситуаций, которые могут вызвать сбой STA. Большинство этих сбоев возникает из-за больших потерь BPDU. Потери приводят к тому, что заблокированные порты переходят в режим пересылки.

Дуплексное несовпадение

Несоответствие дуплексных режимов в соединениях типа "точка-точка" является очень распространенной ошибкой настройки. При включении полнодуплексного режима с одной стороны соединения и включении режима автосогласования с другой стороны соединение будет работать в полудуплексном режиме. (Порт, для которого установлен полнодуплексный режим, более не участвует в согласовании.).)

В худшем случае у моста, посылающего BPDU, включен полудуплексный режим порта, а для порта равноправного узла на другом конце соединения включен полнодуплексный режим. В вышеуказанном примере дуплексное несоответствие на канале между мостами A и B может легко привести к замкнутой петле. Поскольку у моста B настроен полнодуплексный режим, он не выполняет контроль несущей перед доступом к соединению. Мост B начинает передачу кадров даже если мост A уже использует канал. В этой ситуации возникает ошибка для A; мост A обнаруживает коллизию и перед повторной попыткой передачи кадра запускает алгоритм задержки. При наличии достаточного трафика от B к A каждый пакет (включая BPDU) пересылаемый A, задерживается или вызывает коллизию и сбрасывается. С точки зрения протокола STP поскольку мост B больше не получает BPDU от A, мост B теряет корневой мост. Это приводит к тому, что B разблокирует свой порт, подключенный к мосту C, в результате чего возникает петля.

При любом возникновении несогласованности дуплексных параметров на консолях коммутаторов Catalyst, работающих под управлением ПО CatOS и ПО для Cisco IOS, отображаются следующие сообщения об ошибках:

CatOS

```
CDP-4-DUPLEXMISMATCH: Full/half duplex mismatch detected on port [mod]/[port]
```

ПО Cisco IOS)

```
%CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on FastEthernet5/1 (not half
duplex), with TBA05071417(Cat6K-B) 4/1 (half duplex).
```

Проверьте дуплексные параметры и при несогласованности настройте их должным образом.

Для получения дополнительной информации о том, как устранить неполадки несогласованности дуплексных параметров, обратитесь к Настройке документа и Ethernet Устранения проблем 10/100/1000Mb Половину/Полный дуплекс Автосогласования.

Однонаправленный канал

Однонаправленные каналы часто приводят к мостовой петле. В оптоволоконных каналах необнаруженные ошибки часто приводят к образованию однонаправленных каналов. Другой причиной являются неисправности в приемопередатчике. Все, что может привести к поддержанию однонаправленного соединения, очень опасно по отношению к STP. Это объясняется на примере:

Предположим, соединение между A и B является однонаправленным. В соединении сбрасывается трафик от A к B и в то же время передается трафик от B к A. Предположим, что до того, как соединение стало однонаправленным, мост B был заблокирован. Однако порт можно заблокировать только если он получает BPDU от моста с более высоким приоритетом. Поскольку в данном случае все BPDU, исходящие от A, теряются, мост B переключает порт, направленный на A, в состояние пересылки и пересылает трафик. Это приводит к образованию петли. Если этот сбой происходит при запуске, STP не может правильно провести объединение. В случае несогласованности дуплексных параметров перезагрузка ненадолго решает проблему; а в данном случае перезагрузка мостов не оказывает абсолютно никакого эффекта.

Для обнаружения однонаправленных соединений до образования петли пересылки компания Cisco разработала и внедрила протокол обнаружения однонаправленных соединений (UDLD). Данная функция позволяет обнаруживать неправильную разводку кабелей или однонаправленные соединения на уровне 2 и автоматически разрывать возникающие петли, отключая некоторые порты. Запускайте UDLD в среде с мостами при любой возможности.

Дополнительную информацию по использованию UDLD см. в документе Общие сведения и настройка протокола обнаружения однонаправленных соединений.

Повреждение пакета

Повреждение пакета также может привести к таким сбоям. Если в соединении наблюдается высокий уровень физических ошибок, может произойти потеря определенного количества последовательных BPDU. Эта потеря может привести к тому, что заблокированные порты переходят в режим пересылки. Это случается достаточно редко, поскольку по умолчанию установлены умеренные параметры STP. Для перехода заблокированного порта в режим пересылки он не должен получать BPDU в течение 50 секунд. Успешная передача единственного BPDU приводит к разрыву петли. Такое обычно происходит при неосторожной настройке параметров STP. Примером такой настройки может быть уменьшение максимального времени устаревания (max-age).

Повреждение пакетов может быть вызвано несогласованностью дуплексных параметров, плохими кабелями или неверной длиной кабеля. Описание выходных данных счетчика ошибок ПО CatOS и Cisco IOS см. в документе Устранение неисправностей портов и интерфейсов коммутаторов.

Ошибка ресурсов

Даже в высокопроизводительных коммутаторах, в которых большая часть функций коммутации выполняется аппаратно при помощи специальных микросхем ASIC, используется программная реализация STP. Если по какой-либо причине на ЦП моста приходится чрезмерная нагрузка, для передачи BPDU может не хватить ресурсов. Обычно STA не очень загружает процессор и имеет приоритет перед другими процессами. В разделе Поиск ошибок ресурсов данного документа приведены некоторые данные по количеству экземпляров STP, с которым могут работать определенные платформы.

Ошибка конфигурации PortFast

PortFast является функцией, обычно разрешенной для порта или интерфейса, соединенного с хостом. Если этот порт используется для установления соединения, мост пропускает первые стадии STA и переключается непосредственно в режим пересылки.

Внимание. : Функцию PortFast нельзя использовать на портах или интерфейсах коммутаторов, подключенных к другим коммутаторам, концентраторам или маршрутизаторам. В противном случае в сети может образоваться петля.

В данном примере устройство A является мостом, порт p1 которого уже выполняет пересылку. Для порта p2 включена функция PortFast. Устройство B является концентратором. После подключения второго кабеля к A порт p2 переходит в режим пересылки и образует петлю между p1 и p2. Данная петля разрывается как только p1 или p2 получает BPDU, которое переводит один из этих двух портов в режим блокировки. Однако с таким типом временных петель существует проблема. Если трафик петли слишком интенсивный, у моста может возникнуть проблема успешной передачи BPDU, которое приведет к разрыву петли. Это может привести к значительной задержке сходимости или в крайних случаях остановить работу сети.

Для получения дополнительной информации о корректном использовании PortFast на коммутаторах, которые выполняют CatOS и программное обеспечение Cisco IOS, обратитесь к документу Использование PortFast и Других Команд Исправить Задержки Подключения при запуске рабочей станции.

. Даже при включении функции PortFast порт или интерфейс участвуют в работе STP. Если к порту или интерфейсу, на которых настроена функция PortFast, подключается коммутатор с более низким приоритетом моста, чем приоритет текущего активного корневого моста, он может быть выбран в качестве корневого моста. Эта смена корневого моста может отрицательно сказаться на активной топологии STP и привести к неоптимальной настройке сети. Для предотвращения такой ситуации большинство коммутаторов Catalyst, работающих под управлением ПО CatOS и Cisco IOS, оснащены функцией, которая называется BPDU Guard. При получении BPDU портом или интерфейсом, на которых включена функция PortFast, BPDU Guard отключает такой порт или интерфейс.

Для получения дополнительной информации об использовании функции Защиты BPDU на коммутаторах, которые выполняют CatOS и программное обеспечение Cisco IOS,

обратитесь к Усовершенствованию защиты быстрого порта BPDU Связующего дерева документа.

Проблемы неудачных настроек параметров и диаметра STP

Экстремальные значения параметра времени существования и задержки пересылки могут привести к образованию очень нестабильной топологии STP. В таких случаях потеря нескольких BPDU может привести к образованию петли. Другая не очень известная проблема связана с диаметром сети с мостовыми подключениями. Умеренные устанавливаемые по умолчанию значения таймеров STP задают максимальный диаметр сети, равный семи. Данный максимальный диаметр сети ограничивает удаленность мостов друг от друга. Это означает, что между двумя различными мостами в сети не должно быть больше семи переходов. Это ограничение частично зависит от поля срока давности BPDU.

Когда BPDU распространяется от корневого моста к листьям дерева, поле времени устаревания увеличивается при каждом прохождении BPDU через мост. Когда значение в поле времени существования превышает максимальное время существования, мост отбрасывает BPDU. Данная проблема может возникать когда корневой узел расположен слишком далеко от некоторых мостов сети. Данная проблема влияет на сходимость связующего дерева.

При изменении устанавливаемых по умолчанию значений таймеров STP следует проявлять особую осторожность. При попытке добиться более скорой сходимости существует определенная опасность. Изменение значения таймера STP может оказать влияние на диаметр сети и стабильность STP. Для выбора корневого моста можно изменять приоритеты мостов, а для управления резервированием и распределением нагрузки можно изменять параметры стоимости или приоритета порта.

ПО Cisco Catalyst снабжено макрокомандами, которые помогают выполнять точную настройку наиболее важных параметров STP:

- Макрокоманда set spantree root [secondary] уменьшает приоритет моста так, что он становится корневым (или дополнительным корневым). У данной команды есть дополнительный параметр, который позволяет настраивать таймеры STP посредством указания диаметра сети. Даже при правильной настройке таймер незначительно улучшает время сходимости, но при этом увеличивает риск возникновения нестабильности в сети. Кроме того, настройку данного параметра необходимо выполнять всякий раз при добавлении устройства в сеть. Следует задавать умеренные значения, которые устанавливаются по умолчанию и знакомы проектировщикам сетей.
- Команда set spantree uplinkfast для ПО CatOS или команда spanning-tree uplinkfast для ПО Cisco IOS увеличивает приоритет коммутатора так, чтобы он не мог стать корневым. Команда увеличивает время схождения STP в случае неисправностей каскадного подключения. Данную команду следует использовать на распределительных коммутаторах с двойным подключением к нескольким основным коммутаторам. См. Понимание документа и Настройку Характеристика UplinkFast Cisco.
- Команда set spantree backbonefast enable для ПО CatOS или команда spanning-tree backbonefast для ПО Cisco IOS может увеличить время схождения STP коммутатора в случае нарушения обходного канала. BackboneFast - это специальное средство Cisco. См. Понимание документа и Backbone Fast Настройки на Коммутаторах Catalyst.

Для получения дополнительной информации о таймерах STP и правилах настроить их при

необходимости, обратитесь к документу Понимающие и Настраивающиеся Таймеры Протокола STP.

Ошибки программного обеспечения

Как было указано в разделе Общие сведения, STP - одна из первых функций, реализованных в продуктах Cisco. Это средство очень стабильно. Причинами сбоев STP в некоторых редких случаях, упоминаемых здесь, было только взаимодействие с новыми функциями, такими как EtherChannel. Некоторое количество различных факторов может привести к программной ошибке и вызвать различные последствия. Невозможно надлежаще описать проблемы, которые могут быть вызваны ошибкой. Самой опасной ситуацией, возникающей в результате программных ошибок, является игнорирование нескольких BPDU или, другими словами, переход заблокированного порта в режим пересылки.

Устранение сбоя

Систематической процедуры для устранения проблем с STP пока, к сожалению, не существует. Однако в данном разделе приведены некоторые возможные варианты действий. Большинство шагов, приведенных здесь, в основном применимо к устранению неисправностей, заключающихся в образовании мостовых петель. Для выявления других неисправностей STP, приводящих к потерям соединения можно использовать более привычный подход. Например, можно исследовать путь, по которому трафик, проходит с нарушениями.

Примечание: Большинство этих шагов по устранению неисправностей предполагает подключение к различным устройствам сети с мостовыми соединениями. Другими словами, необходим доступ к консоли. Во время замкнутой петли, например, не всегда удается создать соединение Telnet.

При наличии выходных данных команды show-tech support от устройства Cisco для отображения потенциальных проблем и исправлений можно использовать Output Interpreter (только для зарегистрированных клиентов).

Используйте схему сети

Перед тем, как приступить к устранению неисправности, вызванной образованием мостовой петли, необходимо, как минимум, знать следующее:

- Топологию сети с мостовыми подключениями
- Местоположение корневого моста
- Расположение заблокированных портов и резервных каналов

Данная информация имеет существенное значение по двум причинам:

- Чтобы знать, что отлаживать в сети, необходимо знать, как все должно выглядеть при нормальной работе.
- **Большинство действий по устранению неполадок просто использует команды show для определения условий возникновения ошибок.** Знание сетей помогает сфокусироваться на критических портах ключевых устройств.

Идентифицируйте замкнутую петлю

Раньше лавина широковещательных пакетов могла привести к плачевным последствиям для сети. На сегодняшний день благодаря высокоскоростным каналам и устройствам, обеспечивающим коммутацию на аппаратном уровне, трудно представить, чтобы один сервер смог, например, вывести сеть из строя при помощи широковещательных пакетов. Наилучший способ установить наличие мостовой петли – захватить трафик на насыщенном канале и проверить наличие множества сходных пакетов. Однако если у всех пользователей домена моста одновременно возникают проблемы с подключением, логично предположить образование мостовой петли.

Проверьте уровень загрузки портов устройств на предмет наличия непредусмотренных значений. См. раздел "Проверка уровня загрузки портов" данного документа.

В коммутаторах Catalyst, работающих под управлением CatOS, можно легко проверить уровень общей загрузки объединительной платы при помощи команды show system. Команда выдает текущее использование объединительной платы коммутатора и отображает пиковую загрузку и дату пиковой загрузки. Необычная пиковая загрузка указывает на возникновение мостовых петель на данном устройстве.

Быстрое восстановление подключения и готовность к следующему

Отключение портов для устранения петли

Мостовые петли приводят к очень серьезным последствиям в сетях с мостовыми соединениями. Обычно у администраторов нет времени на поиск причин образования петель, они предпочитают восстанавливать работоспособность сети как можно скорее. Самым простым выходом в данной ситуации является отключение вручную каждого отдельного порта, обеспечивающего избыточность в сети. В том случае, если удалось определить наиболее пострадавшую часть сети, начните отключать порты в этой области. По возможности рекомендуется сначала отключить порты, которые должны быть заблокированы. При каждом отключении порта следует проверять, восстановилась ли связь в сети. При определении отключенного порта, позволившего устранить петлю, также определяется избыточный путь, на котором расположен данный порт. Если этот порт должен был быть заблокирован, скорее всего, обнаружился канал, на котором произошел сбой.

Регистрируйте события STP на устройствах, на которых размещены заблокированные порты

Если невозможно точно определить источник неисправностей, или если проблема возникает временно, включите регистрацию событий STP в мостах и коммутаторах сети, в которых возникают неисправности. Если требуется ограничить число настраиваемых устройства, включите эту регистрацию событий хотя бы на устройствах, содержащих заблокированные порты, поскольку именно изменение состояния заблокированного порта и приводит к образования петли.

- Cisco IOS Softwareâ Проблема debug spanning-tree events команды exec для включения отладочной информации STP. Чтобы сохранять эту отладочную информацию в буферах устройства, введите команду общей настройки logging buffered.
- CatOSГ ___команда set logging level spantree 7 по умолчанию увеличивает уровень по

умолчанию событий, которые касаются STP к уровню отладки. **При помощи команды set logging buffer 500 обеспечьте регистрацию максимального количества сообщений в буферах коммутатора.**

Также можно отправить выходные данные отладки на устройство системных журналов. К сожалению, при возникновении мостовых петель редко удается сохранить подключение к серверу с системными журналами.

Проверьте порты

Критические порты, которые должны исследоваться в первую очередь, - это блокирующие порты. Здесь имеется список для проверки разных портов с кратким описанием команд для коммутаторов, использующих программное обеспечение CatOS и Cisco IOS.

Проверьте, чтобы блокирующие порты получали BPDU

Периодическая проверка получения BPDU особенно касается заблокированных портов и корневых портов. Порт может не получать пакеты или BPDU по нескольким причинам.

- Cisco IOS Softwareâ В программном обеспечении Cisco IOS версии 12.0 или позже, выходные данные *bridge-group* **show spanning-tree #** команда имеют поле `BPDU`. В поле указано количество BPDU, полученных каждым из интерфейсов. Если выполнить команду дополнительно один раз или дважды, можно узнать, получает ли устройство BPDU. `show spanning-tree BPDU, BPDU, STP debug spanning-tree.`
- CatOSГ команда *модуля/порта* **show mac** говорит вам количество пакетов групповой адресации, что определенный порт получает. *Однако самой простой для использования является команда show spantree statistics module#/port# vlan#.* Эта команда отображает точное число BPDU конфигурации, полученных для указанного порта в указанной виртуальной локальной сети. При транкинге порт может принадлежать нескольким виртуальным локальным сетям. См. раздел Дополнительная команда CatOS в данном документе.

Проверка несоответствия дуплексных параметров

Для проверки несоответствия дуплексных параметров необходимо проверить обе стороны соединения типа "точка-точка".

- Cisco IOS Softwareâ Проблема **show interfaces [***интерфейсный interface-number***]** команда **статуса** для проверки статуса скорости и дуплексного режима определенного порта.
- CatOSГ самые первые линии выходных данных **show port** *module#/port#* команда дает вам скорость и дуплексный режим согласно конфигурации порта.

Проверьте уровень загрузки портов

Перегруженный трафиком интерфейс может не передать необходимые BPDU. Перегрузка соединения также указывает на возможность образования мостовой петли.

- Cisco IOS Softwareâ Использование **команда show interfaces** для определения использования на интерфейсе. `Several fields help you with this determination, such as`

`load and packets input/output.` Refer to the document Troubleshooting Switch Port and Interface Problems for an explanation of the show interfaces command output.

- CatOSГ **show mac** *module#/port#* статистика показов команды о пакетах, которые порт получает и передает. **Команда show top автоматически вычисляет загрузку порта в течение 30 секунд и отображает результат.** Команда группирует результаты по значению процента использования полосы пропускания. Есть также другие параметры группировки результатов. **Кроме того, команда show system отображает использование объединительной платы даже несмотря на то, что команда не относится к какому-либо конкретному порту.**

Проверьте целостность пакета

- Cisco IOS Softwareâ Ищет ошибочные инкременты в счетчике `input errors` **команды show interfaces**. `runts, giants, no buffer, CRC, frame, overrun ignored counts.` Описание выходных данных команды show interfaces см. в документе Устранение неисправностей портов и интерфейсов коммутаторов.
- CatOSГ **команда show port** *module#/port#* дает вам некоторые подробные данные с полями `Align-Err, FCS-Err, Xmit-Err, Rcv-Err,` и `Undersize.` *Команда show counters module#/port# выдает даже еще более подробную статистику.*

Дополнительная команда CatOS

Команда show spantree statistics module#/port# vlan# выводит очень точную информацию по заданному порту. Выполните эту команду для подозреваемых портов и обратите особое внимание на следующие поля:

- `Forward trans count` â Этот счетчик помнит сколько раз переходы порта от обучения до передачи. В стабильной топологии данный счетчик всегда содержит значение 1. При выключении и включении порта счетчик сбрасывается в значение 0. Поэтому, если значение больше 1, это означает, что изменения состояния этого порта – результат пересчета STP. Изменение состояния не является результатом нарушения прямого соединения.
- `Max age expiry count` â Этот счетчик отслеживает число раз, что максимальный возраст истек на этой ссылке. В основном порт, ожидающий BPDU, до того, как посчитать выделенный мост потерянным, выжидает максимальное время устаревания. По умолчанию максимальное время устаревания равно 20 секундам. При каждом возникновении этого события значение счетчика увеличивается. Если значение не равно 0, то вы знаете, что по какой-то причине выделенный мост для данной LAN нестабилен или испытывает проблемы с передачей своих BPDU.

Ищите ошибки ресурсов

Высокий коэффициент загрузки CPU может быть опасным для системы, в которой работает STA. Данный способ следует использовать для проверки соответствия ресурсов ЦП устройству:

- Cisco IOS Softwareâ Проблема **команда show processes cpu**. Убедитесь, что CPU не слишком загружен. Для коммутаторов Catalyst серий 4500/4000, работающих под

управлением ПО CatOS или Cisco IOS, см. документ Использование ЦП в коммутаторах Catalyst 4500/4000, 2948G, 2980G и 4912G .

- Проблема CatOSГ **команда show proc cpu** для отображения информации об использовании ЦП. Убедитесь, что CPU не слишком загружен.

Существует ограничение количества различных экземпляров STP, которые может обработать Supervisor Engine. Убедитесь в том, что общее число логических портов по всем примерам STP для различных VLAN не превышает максимального числа, поддерживаемого для каждого типа Supervisor Engine и конфигурации памяти.

Для коммутаторов, работающих под управлением ПО CatOS, введите команду show spantree summary, а для коммутаторов, работающих под управлением ПО Cisco IOS, введите команду show spanning-tree summary totals. `STP Active` . Общее количество отображается внизу этого столбца. Общее число логических портов отображает общее число по всем экземплярам STP для различных виртуальных локальных. Убедитесь в том, что это количество не превышает максимального числа, поддерживаемого для каждого типа Supervisor Engine.

Примечание: Формула вычисления суммы логических портов коммутатора выглядит следующим образом:

```
(number of non-ATM trunks * number of active Vlans on that trunk)
+ 2*(number of ATM trunks * number of active Vlans on that trunk)
+ number of non-trunking ports
```

Обзор ограничений для STP, применяющихся в коммутаторах Catalyst, см. следующие документы:

Платформа	Ограничения STP в CatOS	Ограничения STP в ПО Cisco IOS
Catalyst 6500/6000 Supervisor Engine I и II	Устранение неисправностей, связанных с протоколом STP	Устранение неполадок протокола связующего дерева
Catalyst 6500/6000 Supervisor Engine 720	Устранение неисправностей, связанных с протоколом STP	Устранение неполадок протокола связующего дерева
Catalyst 5500/5000	Связующее дерево	â
Catalyst 4500/4000	Связующее дерево	Устранение неисправностей связующего дерева
Catalyst 3750	â	Настройка STP
Catalyst 3550	â	Настройка STP
Catalyst 2970	â	Настройка STP
Catalyst 2950/2955	â	Настройка STP
Catalyst 2940	â	Настройка STP

Catalyst 2900/3500 XL	â	Настройка STP

Отключите ненужные функции

Устранение неисправностей направлено на определение элементов, неработающих в сети в данный момент. Отключите по возможности максимальное количество функций. Отключение помогает упростить схему сети и упрощает определение проблемы. EtherChanneling, например, является функцией, которая требует от STP логического объединения несколько различных каналов в один; отключение этой функции при устранении неисправностей имеет смысл. Как правило, создание как можно более простой конфигурации облегчает поиск неисправностей.

Полезные команды

Команды ПО Cisco IOS

- show interfaces
- show spanning-tree
- show bridge
- show processes cpu
- debug spanning-tree
- logging buffered

Команды CatOS

- show port
- show mac
- show spantree
- show spantree statistics
- show spantree blockedports
- show spantree summary
- show top
- show proc cpu
- show system
- show counters
- set spantree root [secondary]
- set spantree uplinkfast
- set logging level
- set logging buffered

Предусмотрительное проектирование STP

Знать, где находится корень

Очень часто во время устранения неисправностей информация о местоположении корневого моста является недоступной. Не позволяйте STP выбирать, какой мост сделать

корневым. Обычно для всех виртуальных локальных сетей можно определить, какой коммутатор лучше подойдет на роль корневого. Это зависит от конфигурации сети. Как правило, целесообразно выбирать мост с большой пропускной способностью в центре сети. Постановка корневого моста в центр сети, напрямую соединенного с серверами и маршрутизаторами, обычно сокращает среднее расстояние от клиентов до серверов и маршрутизаторов.

На схеме показано:

- Если корневым является мост B, соединение A с C блокируется на мосте A или мосте C. В этом случае хосты, подключенные к коммутатору B, могут получить доступ к серверу и маршрутизатору за два перехода. Хосты, подключенные к мосту C, могут получить доступ к серверу и маршрутизатору за три перехода. Среднее расстояние составляет два с половиной перехода.
- Если корневым является мост A, маршрутизатор и сервер доступны за два перехода для обоих хостов, подключенных к B и C. В данном случае среднее расстояние составляет два перехода.

Логика, стоящая за этим простым примером, позволяет переходить к более сложным топологиям.

ВАЖНОЕ ПРИМЕЧАНИЕ: Для всех виртуальных локальных сетей жестко задайте корневой мост и вспомогательный корневой мост, уменьшая значения параметров приоритета STP. Для этого также можно использовать макрокоманду set spantree root.

Выявление избыточных ресурсов

Спланируйте организацию избыточных соединений. Здесь снова забудьте о функции самонастройки STP. Настройте параметр стоимости STP, помогающий определить блокируемые порты. Необходимость в такой настройке отпадает при наличии иерархической схемы и при расположении корневого моста в хорошем месте.

ВАЖНОЕ ПРИМЕЧАНИЕ: Для всех виртуальных локальных сетей необходимо знать, какие из портов будут заблокированы при стабильной работе сети. Следует иметь схему сети, на которой четко изображены все физические петли и блокированные порты, которые их разрывают.

Знание расположения избыточных соединений поможет определить случайно возникшую мостовую петлю и причину ее возникновения. Кроме того, знание расположения заблокированных портов позволяет определить местонахождение ошибки.

Минимизируйте число заблокированных портов

Единственное критическое действие, предпринимаемое STP - это блокирование портов. Один блокирующий порт, по ошибке переходящий в режим порта пересылки, может вывести из строя значительную часть сети. Хорошим способом ограничения риска, кроющегося в использовании STP, является максимальное уменьшение количества заблокированных портов.

Отсечение неиспользуемых виртуальных локальных сетей

В сети с мостовыми подключениями между двумя узлами нет необходимости в более чем двух избыточных каналах. Однако общепринятой является данная конфигурация:

Коммутатор распределения - это коммутатор с двойным подключением к двум основным коммутаторам. Пользователи, подключенные к распределительным коммутаторам, находятся только в подмножестве виртуальных локальных сетей, доступных в сети. В данном примере все пользователи, подключенные к Dist 2, находятся в сети VLAN 2; Dist 3 соединяет только пользователей в сети VLAN 3. По умолчанию к магистрали подключены все виртуальные локальные сети, определенные в домене протокола VLAN Trunk Protocol (VTP). Только Dist 2 получает ненужный широковещательный и многоадресный трафик для VLAN 3, однако он также блокирует один из своих портов для VLAN 3. В результате между Core A и Core B есть три избыточных пути. Эта избыточность приводит к наличию большего количества заблокированных портов и большей вероятности образования петли.

ВАЖНОЕ ПРИМЕЧАНИЕ: Отключите от магистралей все неиспользуемые VLAN.

Отсечение каналов в протоколе VTP может помочь это сделать, но в ядре сети не следует использовать этот вид самонастраиваемой функции.

В данном примере для связи распределительных коммутаторов с ядром используется только access VLAN:

В данной версии на каждую VLAN блокируется только один порт. Кроме того, в данной конфигурации любое избыточное соединение можно устранить в одно действие, выключая Core A или Core B.

Использование коммутации уровня 3

Коммутация уровня 3 означает маршрутизацию примерно со скоростью коммутации. Маршрутизатор выполняет две основные функции:

- Маршрутизатор строит таблицу пересылки. Построение таблицы пересылки обычно выполняется путем обмена данными с равноправными узлами по протоколам маршрутизации.
- Маршрутизатор принимает пакеты и пересылает их на соответствующий интерфейс в соответствии с адресом назначения.

Высокопроизводительные коммутаторы Cisco уровня 3 сегодня могут выполнять эту вторую функцию с той же скоростью, что и коммутацию уровня 2. При внедрении нового перехода маршрутизации и создании дополнительных сегментов сети скорость не сокращается. На данной схеме в качестве базы используется пример из раздела Отсечение неиспользуемых виртуальных локальных сетей:

Core A и Core B назначены коммутаторами 3 уровня. VLAN 2 и VLAN 3 более не соединены мостовым подключением между Core A и Core B, поэтому возможность образования петли STP исключается.

- При этом избыточность сохраняется, что обеспечивается протоколами маршрутизации уровня 3. Конфигурация обеспечивает даже более быструю повторную сходимость, чем повторная сходимость при использовании STP.
- Больше нет ни одного порта, блокируемого STP. Поэтому отсутствует потенциальная возможность образования мостовых петель.

- Снижения скорости передачи данных не происходит, так как при использовании коммутации VLAN уровня 3 обеспечивается скорость передачи не ниже скорости мостового соединения внутри сети VLAN.

У такой конфигурации есть один недостаток. Переход к такой конфигурации приводит к пересмотру схемы адресации.

Не отключайте протокол STP, даже если он не используется

Даже если в сети успешно удалены все заблокированные порты и нет физической избыточности, в целях безопасности STP лучше не отключать. Обычно STP не потребляет много ресурсов процессора; в большинстве коммутаторов Cisco для коммутации пакетов ЦП не используется. Кроме того, небольшое количество BPDU, пересылаемых по всем соединениям, несущественно уменьшают доступную полосу пропускания. С другой стороны, сеть с мостовыми подключениями без STP может выйти из строя за доли секунды, например, если оператор допустил ошибку на патч-панели. Проще говоря, отключение STP в сети с мостовыми подключениями не оправдывает риск.

Не подпускайте трафик к административной VLAN и старайтесь не охватывать одной VLAN всю сеть

Коммутаторам Cisco обычно присваиваются простые IP-адреса, связанные с VLAN (которая часто называется административной). В этой виртуальной локальной сети принцип работы коммутатора сходен с принципом работы общего IP-хоста. В частности, каждый пакет широковещательной или многоадресной рассылки пересылается на ЦП. Высокая интенсивность широковещательного или многоадресного трафика в административной сети VLAN может снизить быстродействие ЦП и его способность обрабатывать важные пакеты BPDU. Лучше всего не использовать управляющую VLAN для абонентского трафика.

До недавнего времени в реализации Cisco не было способа удалить VLAN 1 из магистрали. Обычно VLAN 1 служит в качестве административной VLAN, в которой все коммутаторы доступны в одной подсети IP-адресов. Хотя это удобно, это может быть и опасно, поскольку мостовая петля в VLAN 1 влияет на все магистрали и может отключить всю сеть. Конечно, эта проблема существует вне зависимости от используемой VLAN. Постарайтесь разделить домены с мостовыми соединениями при помощи высокоскоростных коммутаторов уровня 3.

С версии 5.4 CatOS и программного обеспечения Cisco IOS выпуска 12.1(11b)E можно удалять VLAN 1 из магистрали. VLAN 1 существует, но блокирует трафик, исключая любую возможность образования петель.

Дополнительные сведения

- Поддержка продуктов для ЛВС
- Поддержка технологии коммутации локальных сетей
- Программные средства и ресурсы - техническая поддержка и документация
- Cisco Systems – техническая поддержка и документация