Mejoras del protocolo de árbol de expansión usando las funciones de Loop Guard y BPDU Skew detección de desviación

Contenido

Introducción

Spanning-Tree Protocol (STP) resuelve físicamente las topologías redundantes en topologías de árbol sin loop. El mayor problema con el STP es que algunos errores de hardware pueden hacerlo fallar. Este error crea forwarding loops (o STP loops). Los loops STP causan importantes interrupciones de red.

Este documento describe la característica del Loop Guard STP que se piensa para mejorar la estabilidad de las redes de la capa 2. Este documento también describe la detección de desviación del (BPDU) de la Unidad de bridge protocol data. La detección de desviación BPDU es una función de diagnóstico que genera los mensajes de Syslog cuando los BPDU no se reciben a tiempo.

prerrequisitos

Requisitos

Este documento asume que el lector es familiar con el funcionamiento básico de STP. Refiera a

comprensión y al protocolo configuring spanning-tree (STP) en los switches de Catalyst para aprender cómo el STP trabaja.

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

Disponibilidad de funciones

CatOS

- La característica del STP Loop Guard fue introducida en la versión CatOS 6.2.1 del software Catalyst para las Plataformas del Catalyst 4000 and Catalyst 5000 y en la versión 6.2.2 para la plataforma del Catalyst 6000.
- La característica de detección oblicua BPDU fue introducida en la versión CatOS 6.2.1 del software Catalyst para las Plataformas del Catalyst 4000 and Catalyst 5000 y en la versión 6.2.2 para la plataforma del Catalyst 6000.

Cisco IOS®

- La característica del STP Loop Guard fue introducida en el Cisco IOS Software Release 12.1(12c)EW para los Catalyst 4500 Switch y el Cisco IOS Software Release 12.1(11b)EX para el Catalyst 6500.
- La característica de detección oblicua BPDU no se soporta en los switches de Catalyst que funcionan con el software del sistema del Cisco IOS.

Breve resumen de las funciones del puerto STP

Internamente, el STP asigna a cada puerto del Bridge (o Switch) un papel que se base en la configuración, la topología, la posición relativa del puerto en la topología, y las otras consideraciones. El rol del puerto define el comportamiento del puerto desde el punto de vista STP. De acuerdo con la función del puerto, el puerto envía o recibe STP BPDU y adelante o bloquea el tráfico de datos. Esta lista proporciona un Resumen breve de cada función del puerto STP:

- *Señalado* — Un puerto designado se elige por el link (segmento). El puerto designado es el puerto más cercano al Root Bridge. Este puerto envía los BPDU en el link (segmento) y adelante trafica hacia el Root Bridge. En una red con convergencia STP, cada puerto designado está en el estado del reenvío STP.
- *Raíz* — El Bridge puede tener solamente un puerto raíz. El puerto raíz es el puerto que ése lleva al Root Bridge. En una red con convergencia STP, el puerto raíz está en el estado del reenvío STP.
- *Suplente* — Los puertos alternativos llevan al Root Bridge, pero no son puertos raíz. Los

puertos alternativos mantienen el estado bloqueado del STP.
- *Respaldo* — Esto es un caso especial cuando dos o más puertos del mismo Bridge (Switch) están conectados juntos, directamente o a través de los medios compartidos. En este caso, se señala un puerto, y el bloque de los puertos remanentes. El papel de este puerto es de reserva.

Loop Guard STP

Descripción de la Función

La función de protección de loop del STP brinda protección adicional contra los loops de reenvío de Capa 2 (loops STP). Un loop de STP se crea cuando un puerto de bloqueo STP en las transiciones erróneas de una topología redundante al estado de reenvío. Esto sucede generalmente porque uno de los puertos de una topología redundante (no no necesariamente el puerto de bloqueo STP) recibe físicamente no más de BPDU de STP. En su operación, el STP está basado en la transmisión o en la recepción continua de las BPDU, según el rol del puerto. El puerto designado transmite los BPDU, y el puerto no designado recibe los BPDU.

Cuando uno de los puertos en una topología físicamente redundante deja de recibir BPDU, el STP considera a la topología como un loop libre. Finalmente, se designa el puerto de bloqueo del puerto de respaldo o alternativo y pasa al estado de reenvío. Esta situación crea un loop.

La función de protección de loop hace verificaciones adicionales. Si ya no se reciben las BPDU en un puerto no designado y el protector de loop está habilitado, ese puerto será desplazado a un estado de bloqueo incoherente con el loop en lugar de desplazarse a un estado de escuchar/aprender/reenviar. Sin la función de protección de loop, el puerto asumiría el rol de puerto designado. El puerto se desplaza al estado de reenvío de STP y crea un loop.

Cuando la protección contra loops bloquea un puerto inconsistente, se registra este mensaje:

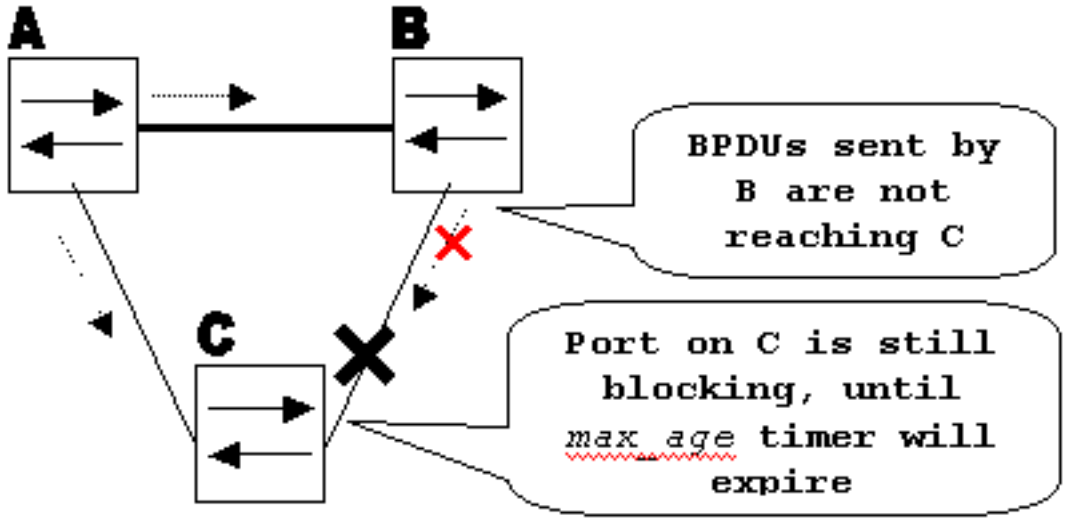
- CatOS`%SPANTREE-2-LOOPGUARDBLOCK: No BPDUs were received on port 3/2 in vlan 3. Moved to loop-inconsistent state.`
- IOS de Cisco`%SPANTREE-2-LOOPGUARD_BLOCK: Loop guard blocking port FastEthernet0/24 on VLAN0050.`

Una vez que el BPDU se recibe en un puerto en un estado sin consistencia en loop STP, las transiciones de puerto en otro estado STP. Según el BPDU recibido, esto significa que la recuperación es automática y la intervención no es necesaria. Después de la recuperación, se registra este mensaje:

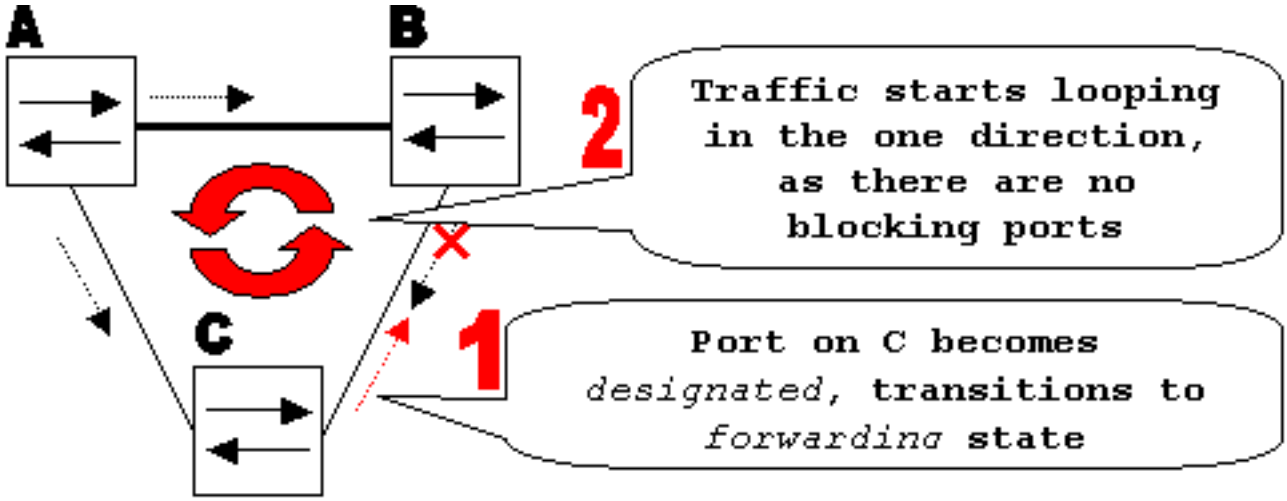
- CatOS`%SPANTREE-2-LOOPGUARDUNBLOCK: port 3/2 restored in vlan 3.`
- IOS de Cisco`%SPANTREE-2-LOOPGUARD_UNBLOCK: Loop guard unblocking port FastEthernet0/24 on VLAN0050.`

Considere este ejemplo para ilustrar este comportamiento:

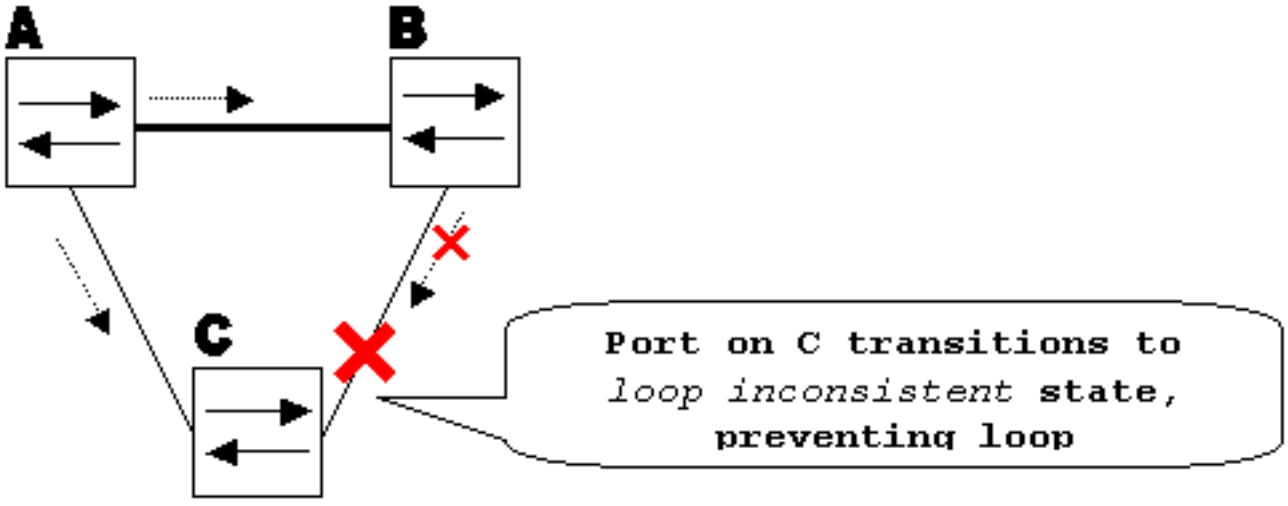
El switch A es el switch raíz. El C del Switch no recibe los BPDU del switch B debido al Error de link unidireccional en el link entre el switch B y el C del Switch.



Sin el Loop Guard, el puerto de bloqueo STP en las transiciones del C del Switch al estado de escucha STP cuando expira el temporizador del max_age, y entonces él transiciones al estado de reenvío en dos veces el tiempo del forward_delay. Esta situación crea un loop.



Con el Loop Guard habilitado, el puerto de bloqueo en las transiciones del C del Switch en el estado de STP Loop-Inconsistent cuando expira el temporizador del max_age. Un puerto en el estado de STP Loop-Inconsistent no pasa el tráfico de usuarios, así que un loop no se crea. (El estado de Loop-Inconsistent es con eficacia igual al estado de bloqueo.)

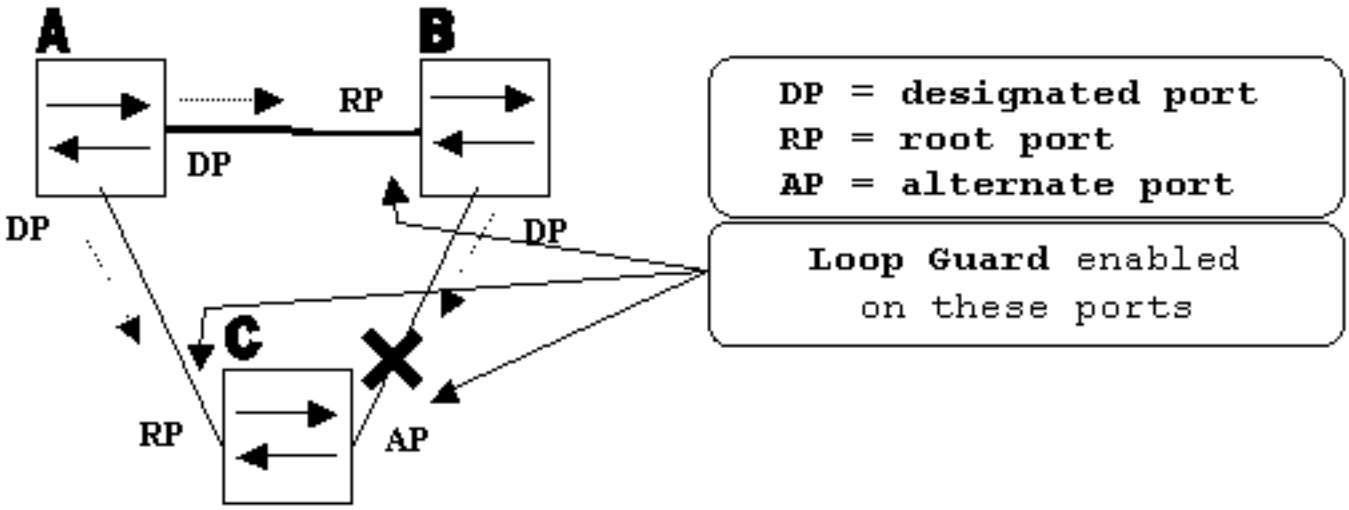


Consideraciones de Configuración

La característica del Loop Guard se habilita en una basada en cada puerto. Sin embargo, mientras bloquee el puerto en el nivel STP, el Loop Guard bloquea los puertos contrarios sobre una base del por el VLAN (debido al por el VLAN STP). Es decir, si los BPDU no se reciben en el puerto troncal para solamente un VLAN determinado, sólo se bloquea ese VLA N (movido al estado sin consistencia en loop STP). Por la misma razón, si está habilitado en una interfaz del EtherChannel, el canal entero se bloquea para un VLAN determinado, no apenas un link (porque el EtherChannel se mira como un puerto lógico desde el punto de vista STP).

¿En qué puertos debe el Loop Guard ser habilitado? La respuesta más obvia está en los puertos de bloqueo. Sin embargo, esto no está totalmente correcto. El Loop Guard se debe habilitar en los puertos no designados (más exacto, en la raíz y los puertos alternativos) para todas las combinaciones posible. de topologías activas. Siempre que la protección contra loop no sea una función por VLAN, el mismo puerto (tronco) podría ser designado para una VLAN y no designado para otra. Los escenarios de falla posibles deben también ser tenidos en cuenta.

Tenga en cuenta este ejemplo:



Por abandono, se inhabilita el Loop Guard. Se utiliza este comando de habilitar el Loop Guard:

- 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.
```

- IOS de Cisco

```
spanning-tree guard loop

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

Con la versión 7.1(1) del software Catalyst (CatOS), el Loop Guard se puede habilitar global en todos los puertos. Con eficacia, el Loop Guard se habilita en todos los enlaces punto a punto. Al estado dúplex del link detecta al enlace punto a punto. Si el modo es dúplex completo, el link se considera de punto a punto. Es todavía posible configurar, o invalidación, las configuraciones globales en una basada en cada puerto.

Publique este comando para habilitar el Loop Guard global:

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

Publique este comando para inhabilitar el Loop Guard:

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

Publique este comando para global inhabilitar el Loop Guard:

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

Publique este comando para verificar el estatus del Loop Guard:

- 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)
```

- IOS de Cisco

```
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
```

Loop Guard contra el UDLD

La coincidencia de las funciones del Loop Guard y del UniDirectional Link Detection (UDLD), en el sentido que ambas protegen contra las fallas del STP causó en parte por los links unidireccionales. Sin embargo, estas dos características diferencian en las funciones y cómo abordan el problema. Esta tabla describe el Loop Guard y la funcionalidad de UDLD:

Funcionalidad	Protección de loop	UDLD
Configuración	Por puerto	Por puerto
Granularity de la acción	Por el VLAN	Por puerto
Autorecover	Sí	Sí, con la

		función de tiempo de espera del err-disable
Protección contra las fallas del STP causadas por los links unidireccionales	Sí, cuando está habilitado en toda la raíz y puertos alternativos en topología redundante	Sí, cuando está habilitado en todos los links en topología redundante
Protección contra las fallas del STP causadas por los problemas en el software (el switch designado no envía el BPDU)	Sí	No
Protección contra miswiring.	No	Sí

De acuerdo con los diversos aspectos del diseño, usted puede elegir el UDLD o la característica del Loop Guard. Con respecto al STP, la mayoría de la diferencia notoria entre las dos características es la ausencia de protección en el UDLD contra las fallas del STP causadas por los problemas en el software. Como consecuencia, el switch designado no envía los BPDU. Sin embargo, este tipo de error es (por un orden de magnitud) más raro que los errores causados por los links unidireccionales. En cambio, la UDLD podría ser más flexible en el caso de links unidireccionales en EtherChannel. En este caso, el UDLD inhabilita solamente los links fallidos, y el canal debe seguir siendo funcional con los links que sigue habiendo. En tal error, el Loop Guard lo pone en el estado de Loop-Inconsistent para bloquear el canal entero.

Además, la protección contra loop no funciona en links compartidos o en aquellas situaciones en las que el link ha sido unidireccional desde la activación del link. En el caso más reciente, el puerto nunca recibe el BPDU y se señala. Porque este comportamiento podría ser normal, este caso particular no es cubierto por el Loop Guard. El UDLD proporciona la protección contra tal escenario.

Según lo descrito, el del más alto nivel de la protección se proporciona cuando usted habilita el UDLD y el Loop Guard.

Interoperabilidad de Loop Guard con otras características de STP

Protección de raíz

La protección raíz es mutuamente - exclusiva con el Loop Guard. Utilizan a la protección raíz en los puertos señalados, y no permite que el puerto llegue a ser no señalado. El Loop Guard trabaja en los puertos no designados y no permite que el puerto se señaló con la expiración del max_age. El protector de raíz no puede estar habilitado en el mismo puerto que el protector de loop. Cuando el Loop Guard se configura en el puerto, inhabilita a la protección raíz configurada en el mismo puerto.

link ascendente rápido y Estructura básica rápida

Tanto el link ascendente rápido como la estructura básica rápida son transparentes para el protector de loop. Cuando el max_age es saltado por el Backbone Fast a la hora del reconvergence, no acciona el Loop Guard. Para más información sobre el Uplink Fast y el Backbone Fast, refiera a estos documentos:

- Comprensión y Configuración de la Función UplinkFast de Cisco
- Comprensión y configuración de Backbone Fast en switches Catalyst

PortFast y Protección BPDU y VLAN dinámica

El Loop Guard no se puede habilitar para los puertos en los cuales se habilita el portfast. Puesto que la protección BPDU funciona en los puertos activados por Portfast, algunas restricciones se aplican a la protección BPDU. El Loop Guard no se puede habilitar en los puertos VLAN dinámicos puesto que estos puertos tienen portfast habilitado.

links compartidos

El Loop Guard no se debe habilitar en los links compartidos. Si usted habilita el Loop Guard en los links compartidos, el tráfico de los host conectados con los segmentos compartidos pudo ser bloqueado.

Árbol de expansión múltiple (MST)

El Loop Guard funciona correctamente en el entorno MST.

BPDU detección de desviación

El Loop Guard debe actuar correctamente con la detección de desviación BPDU.

BPDU detección de desviación

Descripción de la Función

El funcionamiento de STP depende en gran medida de que reciba a tiempo los BPDU. En cada mensaje del hello_time (2 segundos por abandono), el Root Bridge envía los BPDU. Los puentes que son raíz no vuelven a generar BPDU para cada mensaje hello_time, pero reciben BPDU retrasados del puente raíz. Por lo tanto, cada Non-Root Bridge debe recibir los BPDU en cada VLA N para cada mensaje del hello_time. En algunos casos, se pierden los BPDU, o el Bridge CPU está demasiado ocupado retransmitir el BPDU a tiempo. Estos problemas, así como otros problemas, pueden hacer los BPDU llegar tarde (si llegan en absoluto). Este problema potencialmente compromete la estabilidad de la topología del árbol de expansión.

La detección de desviación BPDU permite que el Switch no pierda de vista los BPDU que llegan tarde y notifique al administrador con los mensajes de Syslog. Para cada puerto en el cual un BPDU ha llegado nunca tarde (o ha sesgado), la detección de desviación señala el oblicuo más reciente y la duración de la posición oblicua (tiempo de espera). También notifica el retraso más largo de BPDU en este puerto particular.

Para proteger el Bridge CPU contra la sobrecarga, un mensaje de Syslog no se genera cada vez que ocurre el sesgar BPDU. Los mensajes están limitados por tiempo a un mensaje cada 60 segundos. Sin embargo, el retardo del BPDU excede el max_age dividido por 2 (que iguala 10 segundos por abandono), el mensaje se imprime inmediatamente.

Nota: La detección de desviación BPDU es una función de diagnóstico. Al detectar el BPDU que sesga, envía un mensaje de Syslog. La detección de desviación BPDU no toma ninguna otra acción correctiva.

Éste es un ejemplo de un mensaje de Syslog generado por la detección de desviación 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
```

Consideraciones de Configuración

La detección de desviación BPDU se configura en a por switch. La configuración predeterminada está desactivada. Publique este comando para habilitar la detección de desviación BPDU:

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

Para ver información acerca de la derivación BPDU, utilice el **<vlan> BPDU-que sesga del spantree de la demostración|**comando del **<mod/port>** como se demuestra en este ejemplo:

```
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
```

Información Relacionada

- Mejora a la protección de raíz del protocolo de árbol de expansión
- Mejora de la protección BPDU del árbol de expansión Portfast
- Introducción y configuración de la función del protocolo de detección de link unidireccional
- Utilización de Portfast y Otros Comandos para Solucionar Demoras al Iniciar la Conectividad de la Estación de Trabajo
- Soporte de Producto de LAN
- Soporte de Tecnología de LAN Switching
- Soporte Técnico y Documentación - Cisco Systems