# Konfiguration von STP mit Loop Guard und BPDU Skew Detection

## Inhalt



## Einleitung

In diesem Dokument werden Spanning Tree Protocol-Funktionen beschrieben, die die Stabilität des Layer-2-Netzwerks verbessern sollen.

## Voraussetzungen

### Anforderungen

In diesem Dokument wird davon ausgegangen, dass der Leser mit der grundlegenden Funktionsweise von STP vertraut ist. Weitere Informationen finden Sie unter Understanding and Configure Spanning Tree Protocol (STP) on Catalyst Switches.

### Verwendete Komponenten

Dieses Dokument basiert auf Catalyst Switches. Die Verfügbarkeit der beschriebenen Funktionen kann jedoch von der verwendeten Softwareversion abhängen.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher,

dass Sie die möglichen Auswirkungen aller Befehle verstehen.

### Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps von Cisco zu Konventionen).

## Hintergrundinformationen

Spanning Tree Protocol (STP) löst physisch redundante Topologien in schleifenfreie, strukturähnliche Topologien auf. Das größte Problem bei STP besteht darin, dass einige Hardware-Fehler zu einem Fehler führen können, der Weiterleitungsschleifen (oder STP-Schleifen) verursacht. Diese STP-Schleifen können wiederum zu schwerwiegenden Netzwerkausfällen führen.

In diesem Dokument wird die STP-Funktion für den Loop Guard beschrieben, die die Stabilität von Layer-2-Netzwerken verbessern soll. In diesem Dokument wird auch die BPDU-Skew-Erkennung (Bridge Protocol Data Unit) beschrieben. Die BPDU-Skew-Erkennung ist eine Diagnosefunktion, die Syslog-Meldungen generiert, wenn BPDUs nicht rechtzeitig empfangen werden.

## Verfügbarkeit von Funktionen

### CatOS

- Die Funktion zum STP-Loop-Guard wurde in CatOS 6.2.1 der Catalyst-Software für die Plattformen Catalyst 4000 und Catalyst 5000 und in Version 6.2.2 für die Plattform Catalyst 6000 eingeführt.
- Die Funktion zur BPDU-Skew-Erkennung wurde in CatOS 6.2.1 der Catalyst-Software für Catalyst 4000- und Catalyst 5000-Plattformen und in Version 6.2.2 für die Catalyst 6000-Plattform eingeführt.

### Cisco IOS®

- Die Funktion zum STP-Loop-Guard wurde in Version 12.1(12c)EW der Cisco IOS-Software für Catalyst Switches der Serie 4500 und in Version 12.1(11b)EX der Cisco IOS-Software für Catalyst 6500 eingeführt.
- Die Funktion zur Erkennung von BPDU-Verzerrungen wird von Catalyst Switches, auf denen Cisco IOS-Systemsoftware ausgeführt wird, nicht unterstützt.

## STP-Port-Rollen

Intern weist das STP jedem Bridge- (oder Switch-) Port eine Rolle zu, die auf der Konfiguration, der Topologie, der relativen Position des Ports in der Topologie und anderen Überlegungen basiert. Die Portrolle definiert das Verhalten des Ports aus STP-Sicht. Je nach Portrolle sendet oder empfängt der Port STP-BPDUs und leitet den Datenverkehr weiter oder blockiert ihn. Diese Liste bietet eine kurze Zusammenfassung der STP-Portrollen:

- *Designated (*Festgelegt) - Pro Verbindung (Segment) wird ein Port ausgewählt. Der designierte Port ist der Port, der der Root-Bridge am nächsten liegt. Dieser Port sendet

BPDUs an den Link (das Segment) und leitet den Datenverkehr an die Root-Bridge weiter. In einem konvergenten STP-Netzwerk befindet sich jeder designierte Port im STP-Weiterleitungsstatus.
- *Root* - Die Bridge kann nur einen Root-Port haben. Der Root-Port ist der Port, der zur Root-Bridge führt. In einem konvergenten STP-Netzwerk befindet sich der Root-Port im STP-Weiterleitungsstatus.
- *Alternate (Alternativ*): Alternative Ports führen zur Root-Bridge, sind aber keine Root-Ports. Die alternativen Ports behalten den STP-Blockierungsstatus bei.
- *Backup* - Dies ist ein Sonderfall, wenn zwei oder mehr Ports zwischen denselben Switches direkt oder über gemeinsam genutzte Medien verbunden sind. In diesem Fall wird ein Port festgelegt, und die übrigen Ports werden blockiert. Die Rolle dieses Ports ist "backup".

# STP-Schleifenschutz

## Beschreibung

Die STP Loop Guard-Funktion bietet zusätzlichen Schutz vor Layer-2-Weiterleitungsschleifen (STP-Schleifen). Eine STP-Schleife (Loop) wird erstellt, wenn in einer redundanten Topologie ein blockierender STP-Port irrtümlicherweise in den Weiterleitungszustand übergeht. Dies tritt in der Regel ein, weil einer der Ports in einer physisch redundanten Topologie (nicht zwangsläufig der blockierende STP-Port) keine STP-BPDUs mehr empfängt. Bei seinem Betrieb stützt sich STP auf kontinuierlichen Empfang oder die Übertragung von BPDUs basierend auf der Port-Rolle. Der designierte Port überträgt BPDUs und der nicht designierte Port empfängt BPDUs.

Wenn einer der Ports in einer physisch redundanten Topologie keine BPDUs mehr empfängt, stellt der STP fest, dass die Topologie schleifenfrei ist. Anschließend wird der blockierende Port des alternativen oder Backup-Ports festgelegt und wechselt in den Weiterleitungsstatus. Diese Situation erzeugt eine Schleife.

Die Loop Guard-Funktion führt zusätzliche Prüfungen durch. Wenn BPDUs auf einem nicht designierten Port nicht empfangen werden und Loop Guard aktiviert ist, wird dieser Port in den inkonsistenten STP Loop-Blockierstatus statt in den Überwachungs-, Ermittlungs- oder Weiterleitungsstatus versetzt. Ohne die Loop Guard-Funktion übernimmt der Port die angegebene Port-Rolle. Der Port wechselt in den STP-Weiterleitungsstatus und erstellt eine Schleife.

Wenn der Loop Guard einen inkonsistenten Port blockiert, wird diese Meldung protokolliert:

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

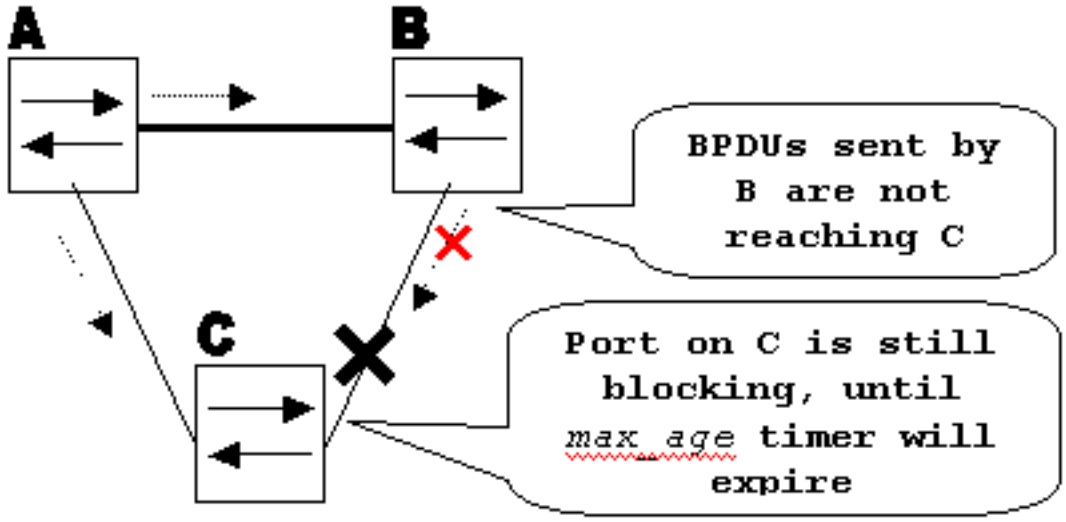
Sobald die BPDU an einem Port in einem schleifeninkonsistenten STP-Zustand empfangen wird, wechselt der Port in einen anderen STP-Zustand. Für die empfangene BPDU bedeutet dies, dass die Wiederherstellung automatisch erfolgt und kein Eingriff erforderlich ist. Nach der Wiederherstellung wird diese Meldung protokolliert:

- CatOS
```
%SPANTREE-2-LOOPGUARDUNBLOCK: port 3/2 restored in vlan 3.
```
- Cisco IOS

```
%SPANTREE-2-LOOPGUARD_UNBLOCK: Loop guard unblocking port FastEthernet0/24 on
VLAN0050.
```

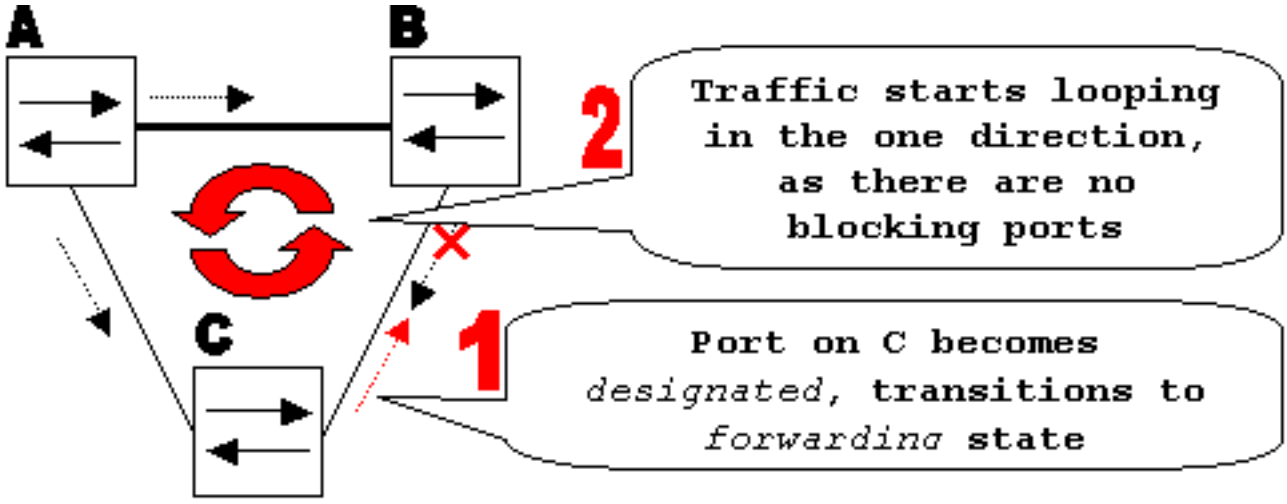
Betrachten Sie dieses Beispiel, um dieses Verhalten zu veranschaulichen:

Switch A ist der Root-Switch. Switch C empfängt keine BPDUs von Switch B aufgrund eines Fehlers der unidirektionalen Verbindung auf der Verbindung zwischen Switch B und Switch C.



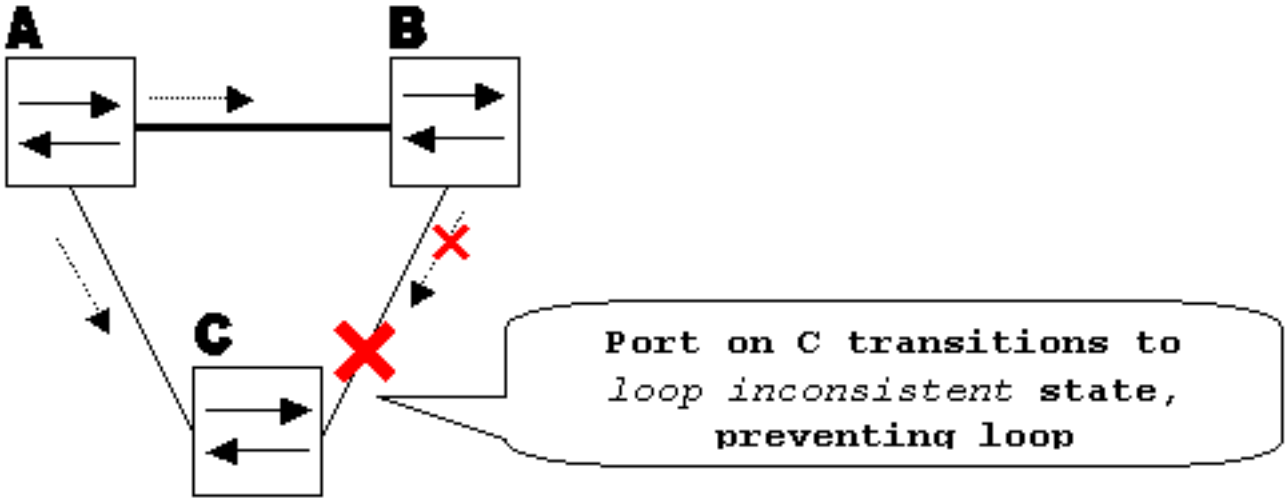

*Unidirektionaler Verbindungsausfall*

Ohne Loop Guard wechselt der STP-Blockierungsport an Switch C in den STP-Überwachungsstatus, wenn der Timer max_age abläuft, und wechselt dann in den Weiterleitungsstatus, der dem Zweifachen der Forward_Delay-Zeit entspricht. Diese Situation erzeugt eine Schleife.




*Schleife wird erstellt*

Bei aktiviertem Loop Guard wechselt der blockierende Port an Switch C nach Ablauf des Timers max_age in den Status "STP loop-inconsistent" (STP, Loop-inkonsistent). Ein Port im Status "STP loop-inconsistent" (STP-Loop inkonsistent) leitet keinen Benutzerdatenverkehr weiter, sodass keine Loop erstellt wird. (Der schleifeninkonsistente Status entspricht im Grunde dem Blockierungsstatus.)



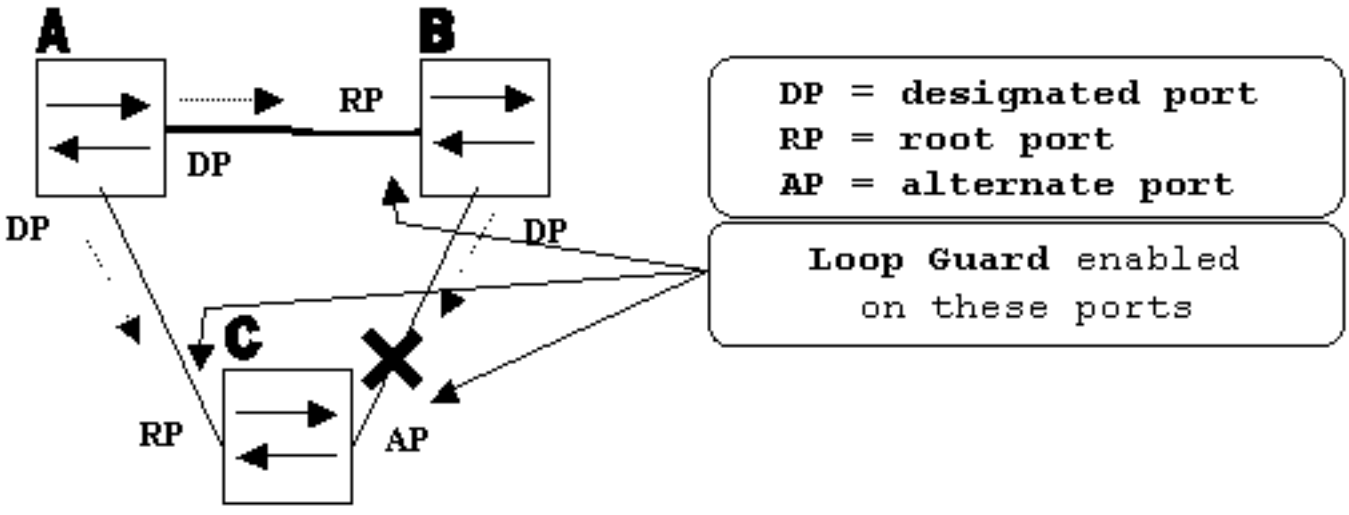

*Loop Guard aktiviert verhindert Schleife*

## Überlegungen zur Konfiguration

Die Funktion "Loop Guard" wird für jeden Port aktiviert. Solange jedoch der Port auf STP-Ebene blockiert wird, blockiert Loop Guard inkonsistente Ports auf VLAN-Basis (aufgrund von VLAN-basiertem STP). Das heißt, wenn BPDUs auf dem Trunk-Port nur für ein bestimmtes VLAN nicht empfangen werden, wird nur dieses VLAN blockiert (in den Status eines schleifeninkonsistenten STP verschoben). Aus demselben Grund wird bei Aktivierung auf einer EtherChannel-Schnittstelle der gesamte Kanal für ein bestimmtes VLAN blockiert, nicht nur für eine Verbindung (da EtherChannel aus STP-Sicht als ein logischer Port betrachtet wird).

An welchen Ports ist der Loop Guard aktiviert? Die naheliegendste Antwort ist die Blockierung von Ports. Das ist jedoch nicht ganz richtig. Loop Guard muss für alle möglichen Kombinationen aktiver Topologien auf den nicht designierten Ports (genauer gesagt auf Root- und alternativen Ports) aktiviert werden. Solange der Loop Guard keine VLAN-basierte Funktion ist, kann derselbe (Trunk-) Port für ein VLAN und ein anderer als für das andere VLAN festgelegt werden. Auch die möglichen Failover-Szenarien müssen berücksichtigt werden.

### Beispiel




*Ports mit aktiviertem Loop Guard*

Standardmäßig ist "loop guard" deaktiviert. Dieser Befehl wird verwendet, um "loop guard" zu aktivieren:

- CatOS

```
set spantree guard loop
```

```
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
```

Mit Version 7.1(1) der Catalyst-Software (CatOS) kann Loop Guard global auf allen Ports aktiviert werden. Auf allen Punkt-zu-Punkt-Verbindungen ist Loop Guard aktiviert. Die Point-to-Point-Verbindung wird durch den Duplexstatus der Verbindung erkannt. Wenn die Duplexeinheit voll ist, gilt die Verbindung als Point-to-Point. Es ist weiterhin möglich, globale Einstellungen pro Port zu konfigurieren oder zu überschreiben.

Führen Sie diesen Befehl aus, um Loop Guard global zu aktivieren:

- CatOS

```
Console> (enable)  set spantree global-default loopguard enable
```

- Cisco IOS

```
Router(config)# spanning-tree loopguard default
```

Führen Sie diesen Befehl aus, um den Loop Guard zu deaktivieren:

- CatOS

```
Console> (enable) set spantree guard none
```

- Cisco IOS

```
Router(config-if)#no spanning-tree guard loop
```

Führen Sie diesen Befehl aus, um den Loop Guard global zu deaktivieren:

- CatOS

```
Console> (enable) set spantree global-default loopguard disable
```

- Cisco IOS

```
Router(config)#no spanning-tree loopguard default
```

Führen Sie diesen Befehl aus, um den Status des Loop Guard zu überprüfen:

- CatOS

**show spantree guard**

```
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
```

## Loop Guard und UDLD

Loop Guard- und UDLD-Funktionen (Unidirectional Link Detection) überschneiden sich, teilweise in dem Sinne, dass beide vor STP-Ausfällen durch unidirektionale Verbindungen schützen. Diese beiden Funktionen unterscheiden sich jedoch hinsichtlich der Funktionalität und der Art und Weise, wie sie das Problem angehen. In dieser Tabelle werden die Loop Guard- und UDLD-Funktionen beschrieben:

| Funktionalität | Loop Guard | UDLD |
|---|---|---|
| Konfiguration | Pro Port | Pro Port |
| Detaillierte Aktionen | Pro VLAN | Pro Port |
| Automatische Wiederherstellung | Ja | Ja, mit Timeout-Funktion zum Deaktivieren |
| Schutz vor STP-Ausfällen durch unidirektionale Links | Ja, wenn in redundanter Topologie an allen Root- und alternativen Ports aktiviert | Ja, wenn auf allen Verbindungen in redundar Topologie aktiviert |
| Schutz vor STP-Ausfällen, die durch Softwareprobleme verursacht werden (designierter Switch sendet kein BPDU) | Ja | Nein |
| Schutz gegen falsche Verkabelung. | Nein | Ja |

Basierend auf den verschiedenen Designüberlegungen können Sie entweder UDLD oder die Loop Guard-Funktion auswählen. In Bezug auf STP besteht der auffälligste Unterschied zwischen den beiden Funktionen darin, dass UDLD nicht vor STP-Ausfällen aufgrund von Softwareproblemen geschützt ist. Daher sendet der designierte Switch keine BPDUs. Diese Art von Störungen ist jedoch (um ein Vielfaches) seltener als Störungen, die durch unidirektionale Verbindungen verursacht werden. Im Gegenzug kann UDLD bei unidirektionalen Verbindungen auf dem EtherChannel flexibler sein. In diesem Fall deaktiviert UDLD nur fehlerhafte Verbindungen, und der Kanal kann mit den verbleibenden Verbindungen funktionsfähig bleiben. Bei einem solchen Ausfall versetzt ihn der Loop Guard in einen Loop-Inkonsistent-Zustand, um den gesamten Kanal zu blockieren.

Darüber hinaus funktioniert Loop Guard nicht auf gemeinsam genutzten Verbindungen oder in Situationen, in denen die Verbindung seit dem Verbindungsaufbau unidirektional war. Im letzten Fall empfängt der Port niemals BPDU und wird entsprechend konfiguriert. Da dieses Verhalten normal sein kann, wird dieser spezielle Fall nicht von Loop Guard abgedeckt. UDLD bietet Schutz vor einem solchen Szenario.

Wie beschrieben, wird die höchste Schutzstufe bereitgestellt, wenn Sie UDLD und Loop Guard aktivieren.

## Interoperabilität von Loop Guard mit anderen STP-Funktionen

### Root Guard

Der Fußschutz schließt sich mit dem Schlaufenschutz gegenseitig aus. Der Root Guard wird auf designierten Ports verwendet und verhindert, dass der Port nicht designiert wird. Der Loop Guard funktioniert an nicht designierten Ports und lässt nicht zu, dass der Port bis zum Ablauf von max_age designiert wird. Der Root Guard kann nicht auf demselben Port wie der Loop Guard aktiviert werden. Wenn der Loop Guard auf dem Port konfiguriert ist, wird der auf demselben Port konfigurierte Root Guard deaktiviert.

### Uplink Fast und Backbone Fast

Sowohl Uplink Fast als auch Backbone Fast sind für den Loop Guard transparent. Wenn max_age vom Backbone zum Zeitpunkt der Rekonvergenz schnell übersprungen wird, löst dies den Loop Guard nicht aus. Weitere Informationen zu Uplink Fast und Backbone Fast finden Sie in den folgenden Dokumenten:

- Die Cisco Uplink Fast-Funktion verstehen und konfigurieren
- Schnelles Verständnis und Konfiguration des Backbone auf Catalyst-Switches

### PortFast, BPDU Guard und Dynamic VLAN

Loop Guard kann nicht für Ports aktiviert werden, auf denen "portfast" aktiviert ist. Da BPDU Guard auf portfast-fähigen Ports arbeitet, gelten für BPDU Guard einige Einschränkungen. Loop Guard kann für dynamische VLAN-Ports nicht aktiviert werden, da für diese Ports "portfast" aktiviert ist.

### Gemeinsame Links

Loop Guard darf auf freigegebenen Links nicht aktiviert sein. Wenn Sie Loop Guard für freigegebene Verbindungen aktivieren, kann der Datenverkehr von Hosts, die mit freigegebenen Segmenten verbunden sind, blockiert werden.

### Multiple Spanning Tree (MST)

Loop Guard funktioniert in der MST-Umgebung ordnungsgemäß.

### Erkennung von BPDU-Verzerrungen

Loop Guard kann mit BPDU-Skew-Erkennung richtig funktionieren.

# Erkennung von BPDU-Verzerrungen

## Beschreibung

Der STP-Betrieb ist in hohem Maße vom rechtzeitigen Empfang von BPDUs abhängig. Bei jeder Hello_Time-Nachricht (standardmäßig 2 Sekunden) sendet die Root-Bridge BPDUs. Nicht-Root-Bridges regenerieren keine BPDUs für jede Hello_Time-Nachricht, sondern empfangen weitergeleitete BPDUs von der Root-Bridge. Daher muss jede Nicht-Root-Bridge für jede Hello_Time-Nachricht BPDUs in jedem VLAN empfangen. In einigen Fällen gehen BPDUs verloren, oder die Bridge-CPU ist zu stark ausgelastet, um BPDU rechtzeitig weiterzuleiten. Diese und andere Probleme können dazu führen, dass BPDUs zu spät eintreffen (wenn überhaupt). Dieses Problem beeinträchtigt möglicherweise die Stabilität der Spanning Tree-Topologie.

Durch die Erkennung von BPDU-Skew kann der Switch verspätete BPDUs nachverfolgen und den Administrator mit Syslog-Meldungen benachrichtigen. Für jeden Port, an dem ein BPDU jemals verspätet eingetroffen ist (oder einen Skew-Wert erreicht hat), meldet die Skew-Erkennung den letzten Skew und die Dauer des Skew (Latenz). Er meldet auch die längste BPDU-Verzögerung an diesem bestimmten Port.

Um die Bridge-CPU vor Überlastung zu schützen, wird nicht bei jedem Auftreten einer BPDU-Verzerrung eine Syslog-Meldung generiert. Die Nachrichtenrate ist auf eine Nachricht alle 60 Sekunden begrenzt. Muss die Verzögerung von BPDU jedoch max_age dividiert durch 2 überschreiten (dies entspricht standardmäßig 10 Sekunden), wird die Nachricht sofort ausgegeben.

> **Hinweis**: Die BPDU-Skew-Erkennung ist eine Diagnosefunktion. Bei Erkennung einer BPDU-Verzerrung wird eine Syslog-Meldung gesendet. Die BPDU-Skew-Erkennung ergreift keine weiteren Korrekturmaßnahmen.

> **Hinweis**: Die Funktion zur Erkennung von BPDU-Verzerrungen wird von Catalyst Switches mit Cisco IOS-Systemsoftware nicht unterstützt.

Dies ist ein Beispiel für eine Syslog-Meldung, die von der BPDU-Skew-Erkennung generiert wurde:

```
%SPANTREE-2-BPDU_SKEWING: BPDU skewed with a delay of 10 secs (max_age/2)
```

## Überlegungen zur Konfiguration

Die BPDU-Skew-Erkennung wird Switch-weise konfiguriert. Standardmäßig ist diese Option deaktiviert. Führen Sie diesen Befehl aus, um die BPDU-Skew-Erkennung zu aktivieren:

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

Verwenden Sie den Befehl **show spantree bpdu-skewing <vlan>|<mod/port>,** wie in diesem Beispiel gezeigt, um die BPDU-Neigungsinformationen anzuzeigen:

```
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
```

# Zugehörige Informationen

- Erweiterung der Spanning Tree Protocol Root Guard
- Spanning-Tree-Verbesserung des Portfast BPDU Guard
- Verstehen und Konfigurieren der Funktion des Unidirectional Link Detection Protocol
- Verwenden von PortFast und anderen Befehlen zum Beheben von Verzögerungen bei der Workstation-Startverbindung
- Technischer Support und Downloads - Cisco Systems

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.