

Configureer STP met Looptbewaking en BPDU-scheefdetectie

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Conventies](#)

[Achtergrondinformatie](#)

[Beschikbaarheid functies](#)

[STP-poortrollen](#)

[STP-looptbewaking](#)

[Beschrijving van functie](#)

[Configuratieoverwegingen](#)

[Loop Guard versus UDLD](#)

[Interoperabiliteit van Loop Guard met andere STP-functies](#)

[BPDU-scheefheid detecteren](#)

[Beschrijving van functie](#)

[Configuratieoverwegingen](#)

[Gerelateerde informatie](#)

Inleiding

Dit document beschrijft Spanning Tree Protocol-functies die bedoeld zijn om Layer 2-netwerkstabiliteit te verbeteren.

Voorwaarden

Vereisten

Dit document gaat ervan uit dat de lezer bekend is met de basisbediening van STP. Zie [Spanning Tree Protocol \(STP\) op Catalyst-Switches begrijpen en configureren](#) voor meer informatie.

Gebruikte componenten

Dit document is gebaseerd op Catalyst-switches, maar de beschikbaarheid van de beschreven functies kan afhankelijk zijn van de gebruikte softwarerelease.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Conventies

Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

Achtergrondinformatie

Spanning Tree Protocol (STP) zet fysiek redundante topologieën om in lusvrije, topologieën met een boomstructuur. Het grootste probleem met STP is dat bepaalde hardwarestoringen ertoe kunnen leiden dat STP mislukt. Bij deze fout ontstaan doorstuurlussen (STP-lussen). STP-lussen kunnen grootschalige netwerkuitval veroorzaken.

Dit document beschrijft de functie STP van de lijnbewaking die bedoeld is om de stabiliteit van Layer 2-netwerken te verbeteren. Dit document beschrijft ook de detectie van scheefheid in Bridge Protocol Data Unit (BPDU). De scheefheid van BPDU opsporing is een kenmerkende eigenschap die syslog berichten produceert wanneer BPDUs niet op tijd worden ontvangen.

Beschikbaarheid functies

CatOS

- De STP-lusbeveiliging werd geïntroduceerd in CatOS versie 6.2.1 van de Catalyst software voor Catalyst 4000 en Catalyst 5000 platforms en in versie 6.2.2 voor Catalyst 6000 platform.
- De BPDU scheefdetectiefunctie werd geïntroduceerd in CatOS versie 6.2.1 van de Catalyst software voor Catalyst 4000 en Catalyst 5000 platforms en in versie 6.2.2 voor het Catalyst 6000 platform.

Cisco IOS®

- De functie STP-lusbewaking is geïntroduceerd in Cisco IOS-software release 12.1(12c)EW voor Catalyst 4500 switches en Cisco IOS-software release 12.1(11b)EX voor Catalyst 6500.
- De optie voor scheefheid met BPDU wordt niet ondersteund in Catalyst-switches waarop Cisco IOS-systeemsoftware wordt uitgevoerd.

STP-poortrollen

Intern kent STP aan elke bridge (of switch) poort een rol toe die is gebaseerd op configuratie, topologie, relatieve positie van de poort in de topologie en andere overwegingen. De poortrol bepaalt het gedrag van de poort vanuit het STP-standpunt. Gebaseerd op de poortrol verzendt of ontvangt de poort STP BPDU's en doorstuurt of blokkeert het gegevensverkeer. Deze lijst geeft een korte samenvatting van elke STP-poortrol:

- *Aangewezen-één* aangewezen haven wordt geselecteerd per verbinding (segment). De aangewezen haven is de haven die het dichtst bij de root-brug ligt. Deze poort stuurt BPDU's op de link (segment) en voorwaarts verkeer naar de root-brug. In een STP geconvergeerd netwerk, is elke aangewezen poort in de STP-doorsturen staat.
- *De wortel*-brug kan slechts één wortelhaven hebben. De wortelhaven is de haven die tot de root-brug leidt. In een STP geconvergeerd netwerk, is de wortelpoort in de STP-doorsturen

staat.

- *Alternate*—Alternate poorten leiden naar de root-brug maar zijn geen root poorten. De alternatieve poorten behouden de STP-blokkerende status.
- *Back-up*—Dit is een speciaal geval wanneer twee of meer poorten tussen dezelfde switches onderling verbonden zijn, rechtstreeks of via gedeelde media. In dit geval wordt één haven aangewezen en worden de overige havens geblokkeerd. De rol voor deze poort is backup.

STP-loopbewaking

Beschrijving van functie

Loop Guard, de functie voor bescherming tegen STP-lussen, biedt extra bescherming tegen Layer 2-doorstuurlussen (STP-lussen). Er wordt een STP-lus gemaakt wanneer een STP blokkerende poort in een redundante topologie abusievelijk de doorstuurtoestand krijgt. Dit gebeurt doorgaans omdat een van de poorten van een fysiek redundante topologie (niet noodzakelijkerwijs de STP blokkerende poort) geen STP-BPDU's meer ontvangt. Voor de werking is STP afhankelijk van de voortdurende ontvangst of verzending van BPDU's op basis van de poortrol. De aangewezen poort verzendt BPDU's, de niet-aangewezen poort ontvangt BPDU's.

Wanneer een van de poorten in een fysiek redundante topologie geen BPDU's meer ontvangt, gaat STP ervan uit dat de topologie geen lussen bevat. Uiteindelijk wordt de blokkerende poort van de alternatieve of back-uppoort aangewezen en krijgt deze een doorstuurtoestand. Deze situatie leidt tot een lus.

Loop Guard voert extra controles uit. Als BPDU's niet op een niet-aangewezen poort worden ontvangen en Loop Guard wordt ingeschakeld, krijgt die poort de voor STP-lussen inconsistente blokkeertoestand in plaats van de luister-, leer- of doorstuurtoestand. Zonder de functie Loop Guard neemt de poort de rol van aangewezen poort aan. De poort krijgt de STP-doorstuurtoestand en maakt een lus.

Wanneer de lusbescherming een inconsistente poort blokkeert, wordt dit bericht vastgelegd:

- **CatOS**

```
%SPANNTREE-2-LOOPGUARDBLOCK: No BPDUs were received on port 3/2 in vlan 3. Moved to loop-inconsistent state.
```

- **Cisco IOS**

```
%SPANNTREE-2-LOOPGUARD_BLOCK: Loop guard blocking port FastEthernet0/24 on VLAN0050.
```

Zodra BPDU op een poort in een loop-inconsistente STP-status is ontvangen, verandert de poort in een andere STP-status. Voor de ontvangen BPDU betekent dit dat het herstel automatisch verloopt en dat interventie niet nodig is. Na herstel wordt dit bericht vastgelegd:

- **CatOS**

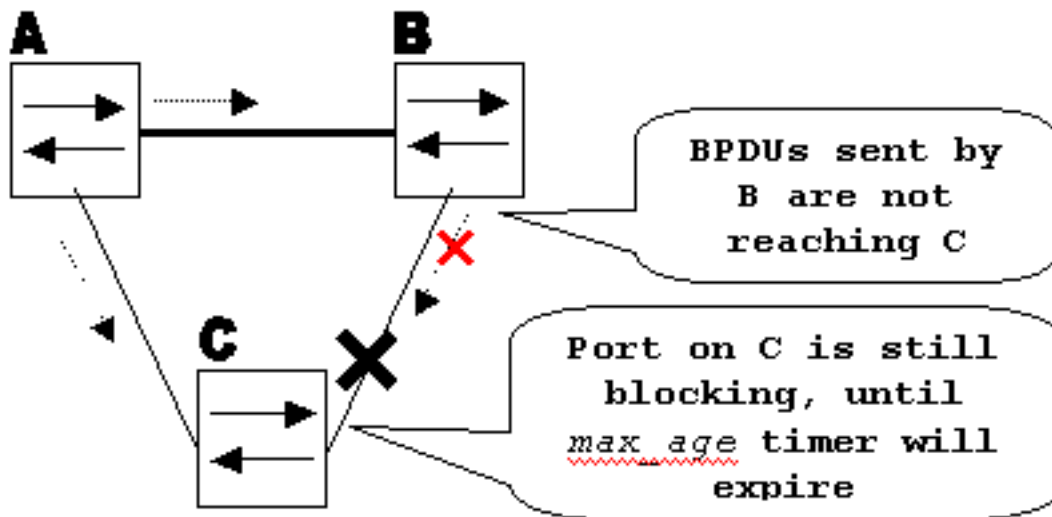
```
%SPANNTREE-2-LOOPGUARDUNBLOCK: port 3/2 restored in vlan 3.
```

- **Cisco IOS**

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

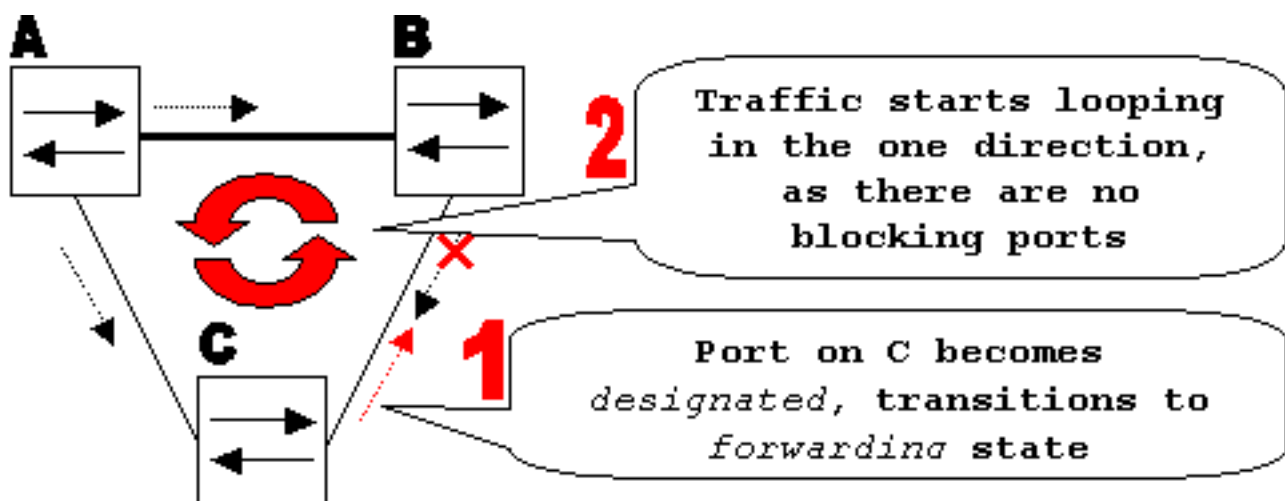
Neem dit voorbeeld om dit gedrag te illustreren:

Switch A is de wortel switch. Switch C ontvangt geen BPDU's van switch B als gevolg van een unidirectionele koppelingsfout op het verband tussen switch B en switch C.



Unidirectionele linkfout

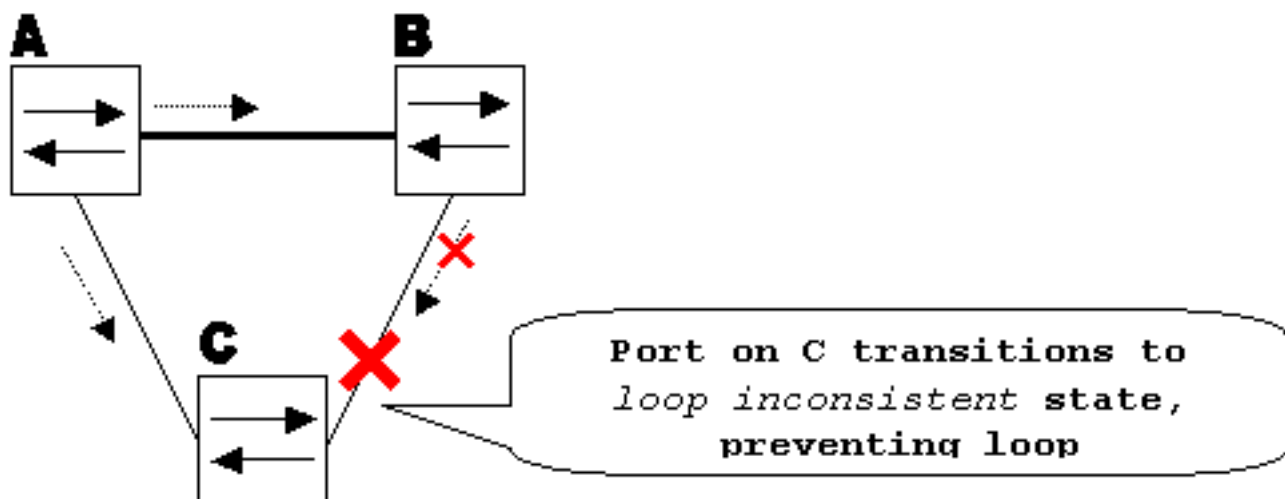
Zonder lusbeveiliging, de STP blokkerende poort op switch C overgaan naar de STP luisterstatus wanneer de `max_age` timer verval, en dan overgaat het naar de doorsturen staat in twee keer de `forward_delay` tijd. Deze situatie leidt tot een lus.



Lus

wordt gemaakt

Als loop guard is ingeschakeld, gaat de blokkerende poort op switch C over in STP-loop-inconsistente status als de `max_age` timer verloopt. Een poort in een STP-lus-inconsistente status geeft geen gebruikersverkeer door, zodat er geen lus wordt gemaakt. (De lus-inconsistente status is effectief gelijk aan blokkerende status.)



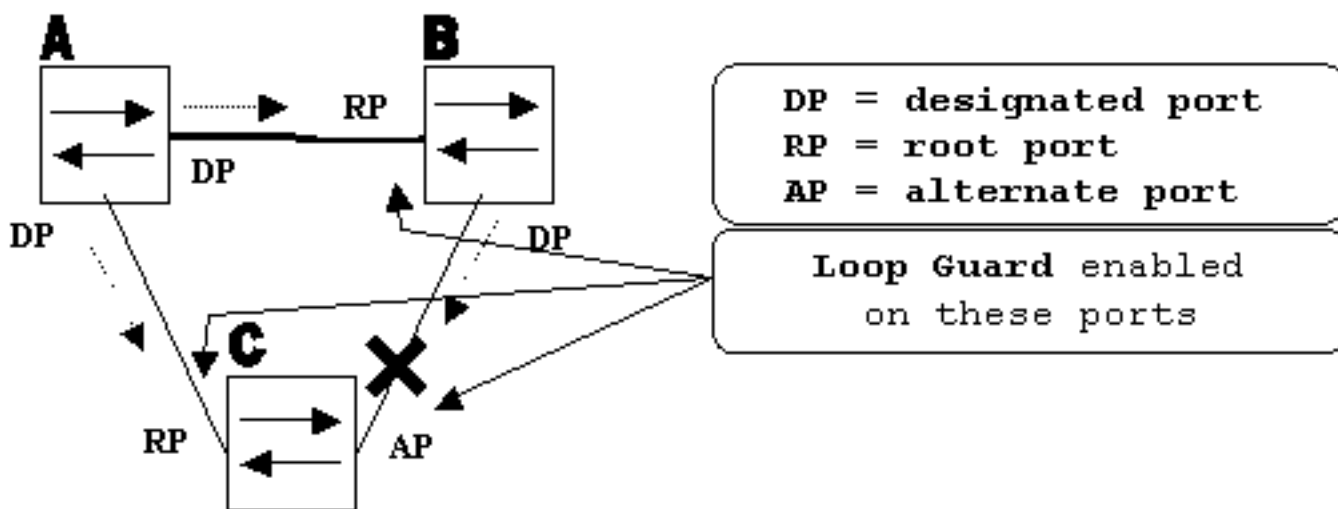
Loop

Configuratieoverwegingen

De functie loop guard is per poort ingeschakeld. Zolang echter de poort op STP-niveau wordt geblokkeerd, blokkeert loop guard inconsistente poorten per VLAN-basis (vanwege STP per VLAN). Dat wil zeggen, als BPDU's niet worden ontvangen op de trunkpoort voor slechts één bepaald VLAN, dan wordt VLAN alleen geblokkeerd (verplaatst naar loop-inconsistente STP-status). Om dezelfde reden wordt het gehele kanaal geblokkeerd voor een bepaald VLAN, niet alleen voor één link (omdat EtherChannel wordt beschouwd als één logische poort vanuit het STP-standpunt), als het op een EtherChannel-interface is ingeschakeld.

Op welke poorten is de loop guard ingeschakeld? Het meest voor de hand liggende antwoord ligt op de blokkerende havens. Dat is echter niet helemaal juist. Loop guard moet worden ingeschakeld op de niet-aangewezen poorten (meer bepaald op root en alternatieve poorten) voor alle mogelijke combinaties van actieve topologieën. Zolang de loopwacht geen per-VLAN-functie is, kan de zelfde (trunk) poort worden aangewezen voor het ene VLAN en niet voor het andere. Er moet ook rekening worden gehouden met mogelijke failoverscenario's.

Voorbeeld



orten met ingeschakelde loopplank

Po

Standaard is lusbeveiliging uitgeschakeld. Deze opdracht wordt gebruikt om loop guard in te schakelen:

- 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
```

Met versie 7.1(1) van de Catalyst-software (CatOS) kan lusbeveiliging globaal worden ingeschakeld op alle poorten. Effectief, wordt de lijnwacht toegelaten op alle punt-tot-punt verbindingen. De point-to-point link wordt gedetecteerd door de duplexstatus van de link. Als duplex volledig is, wordt de link beschouwd als point-to-point. Het is nog steeds mogelijk om globale instellingen per poort te configureren of deze te negeren.

Geef deze opdracht uit om loop guard wereldwijd mogelijk te maken:

- **CatOS**

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

- **Cisco IOS**

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

Geef deze opdracht uit om loop guard uit te schakelen:

- **CatOS**

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

- **Cisco IOS**

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

Geef deze opdracht uit om loop guard wereldwijd uit te schakelen:

- **CatOS**

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

- **Cisco IOS**

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

Geef dit bevel uit om de status van de lijnwacht te verifiëren:

- **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 versus UDLD

De functionaliteit van de Lijn bewaker en van de Unidirectionele Klink van de Detectie (UDLD) overlapt, gedeeltelijk in de zin dat beide tegen mislukkingen STP die door unidirectionele verbindingen worden veroorzaakt beschermen. Deze twee kenmerken verschillen echter qua functionaliteit en de manier waarop ze het probleem aanpakken. In deze tabel worden de functies van lusbescherming en UDLD beschreven:

Functionaliteit	Loop Guard	UDLD
Configuratie	Per poort	Per poort
Actiegranulariteit	Per VLAN	Per poort
Automatisch herstel	Ja	Ja, met de tijdelijke optie err-deactiveren
Bescherming tegen STP-storingen veroorzaakt door unidirectionele koppelingen	Ja, indien ingeschakeld op alle root- en alternatieve poorten in redundante topologie	Ja, indien ingeschakeld op alle koppelingen in redundante topologie
Bescherming tegen STP-storingen die worden veroorzaakt door problemen in de software (de aangewezen switch stuurt geen BPDU)	Ja	Nee
Bescherming tegen onjuiste bedrading.	Nee	Ja

Gebaseerd op de diverse ontwerpoverwegingen, kunt u of UDLD of de eigenschap van de lijnwacht kiezen. Wat STP betreft, is het meest opmerkelijke verschil tussen de twee kenmerken de afwezigheid van bescherming in UDLD tegen STP-storingen veroorzaakt door problemen in software. Dientengevolge verzendt de aangewezen switch geen BPDU's. Dit soort storingen is echter (in volgorde van grootte) zeldzamer dan storingen veroorzaakt door unidirectionele links. In ruil hiervoor kan UDLD flexibeler zijn in het geval van unidirectionele links op EtherChannel. In dit geval schakelt UDLD alleen mislukte koppelingen uit en kan het kanaal functioneel blijven met de koppelingen die overblijven. Bij een dergelijke storing zet de lusbewaker het in een loop-inconsistente toestand om het hele kanaal te blokkeren.

Daarnaast werkt lusbeveiliging niet aan gedeelde links of in situaties waar de link unidirectioneel is geweest sinds de link-up. In het laatste geval ontvangt de haven nooit BPDU en wordt deze aangewezen. Omdat dit gedrag normaal zou kunnen zijn, wordt dit specifieke geval niet gedekt

door lusbescherming. UDLD biedt bescherming tegen een dergelijk scenario.

Zoals beschreven, wordt het hoogste beschermingsniveau geboden wanneer u UDLD en lusbeveiliging inschakelt.

Interoperabiliteit van Loop Guard met andere STP-functies

Root Guard

De wortelbeschermer is wederzijds exclusief met de lusbeschermer. De root guard wordt gebruikt op aangewezen poorten, en het staat niet toe dat de poort niet aangewezen wordt. De luswachter werkt op niet-aangewezen poorten en laat de poort niet toe om aangewezen te worden door het aflopen van max_age. De root guard kan niet worden ingeschakeld op dezelfde poort als de loop guard. Wanneer de loopwacht op de poort is geconfigureerd, schakelt deze de wortelbeveiliging uit die op dezelfde poort is geconfigureerd.

Snelle uplink en backbone

Zowel de uplink snel als de backbone snel zijn transparant voor de lusbeveiliging. Wanneer max_age op het moment van reconvergentie snel door backbone wordt overgeslagen, wordt de loop guard niet geactiveerd. Raadpleeg deze documenten voor meer informatie over snelle uplink en backbone:

- [De Cisco Uplink Fast-functie begrijpen en configureren](#)
- [Begrijp en vorm backbone snel op Catalyst Switches](#)

PortFast en BPDU Guard en Dynamisch VLAN

Loop guard kan niet worden ingeschakeld voor poorten waarop portfast is ingeschakeld. Aangezien de wacht BPDU op portfast-enabled havens werkt, zijn sommige beperkingen op de wacht BPDU van toepassing. Lijnbewaking kan niet worden ingeschakeld op dynamische VLAN-poorten omdat deze poorten portfast zijn ingeschakeld.

Gedeelde links

Loop guard moet niet worden ingeschakeld op gedeelde links. Als u loop guard op gedeelde links inschakelt, kan verkeer van hosts die verbonden zijn met gedeelde segmenten worden geblokkeerd.

Multiple Spanning Tree (MST)

Loop guard functioneert correct in de MST omgeving.

BPDU-scheefheid detecteren

Lijnbescherming kan correct werken met BPDU-scheefdetectie.

BPDU-scheefheid detecteren

Beschrijving van functie

STP-werking is sterk afhankelijk van de tijdige ontvangst van BPDU's. Bij elk hello_time bericht (2

seconden door gebrek), verzendt de root-brug BPDUs. Niet-root-bruggen regenereren BPDUs niet voor elk hello_time bericht, maar ze ontvangen doorgezonden BPDUs van de root-brug. Daarom moet elke niet-root-brug BPDUs op elk VLAN ontvangen voor elk hello_time bericht. In sommige gevallen gaan BPDUs verloren of is de bridge-CPU te druk om BPDUs tijdig af te lossen. Deze problemen, evenals andere problemen, kunnen ertoe leiden dat BPDUs laat aankomen (als ze überhaupt al aankomen). Deze kwestie kan de stabiliteit van het overspannen - boomtopologie potentieel compromitteren.

Met de detectie van scheefheid van BPDUs kan de switch BPDUs bijhouden die te laat aankomen en de beheerder met syslogberichten op de hoogte brengen. Voor elke poort waarop een BDU ooit laat is gearriveerd (of scheefgetrokken is), meldt de scheefheid de meest recente scheefheid en de duur van de scheefheid (latentie). Het meldt ook de langste BDU-vertraging op deze specifieke poort.

Om de bridge-CPU tegen overbelasting te beveiligen, wordt niet telkens een syslog-bericht gegenereerd wanneer BDU-scheefheid optreedt. Berichten worden beperkt tot één bericht elke 60 seconden. Mocht de vertraging van BDU echter de max_age overschrijden, gedeeld door 2 (wat standaard 10 seconden bedraagt), dan wordt het bericht onmiddellijk afgedrukt.

Opmerking: de detectie van scheefheid van BDU is een diagnostische functie. Op detectie van BDU scheeftrekken wordt een syslog-bericht verzonden. De scheefheid van BDU detecteert geen verdere corrigerende maatregelen.

Opmerking: de optie voor de detectie van scheefheid van BDU wordt niet ondersteund in Catalyst-switches waarop Cisco IOS-systeemsoftware wordt uitgevoerd

Dit is een voorbeeld van een syslog-bericht dat is gegenereerd door BDU-scheefdetectie:

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

Configuratieoverwegingen

De scheefheid van BDU wordt gedetecteerd per switch. De standaardinstelling is uitgeschakeld. Geef deze opdracht uit om BDU-scheefdetectie in te schakelen:

```
Cat6k> (enable) set spantree bpduskeewing enable  
Spantree bpduskeewing enabled on this switch.
```

Om BDU-scheefheid informatie te zien, gebruik de **show spantree bpduskeewing <vlan>|<mod/port>** opdracht zoals in dit voorbeeld:

```
Cat6k> (enable) show spantree bpduskeewing 1  
Bpduskeewing 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
```

Gerelateerde informatie

- [Verbetering van Spanning Tree Protocol Root Guard](#)

- [Verbetering van Spanning Tree PortFast BPDU Guard](#)
- [De functie Unidirectionele linkdetectie-protocol begrijpen en configureren](#)
- [PortFast en andere opdrachten gebruiken om connectiviteitsvertragingen bij het opstarten van werkstations op te lossen](#)
- [Technische ondersteuning en downloads - Cisco Systems](#)

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.