Verbetering in Spanning Tree Port Fast BPDU Guard

Inhoud

Inleiding

In dit document wordt de functie voor het verbeteren van de bewaking van PortFast Bridge Protocol Data Unit (BPDU) van Spanning Tree Protocol (STP) beschreven.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

Deze softwareversies introduceerden de STP PortFast BPDU guard:

- Catalyst OS (CatOS) softwareversie 5.4.1 voor de Catalyst 4500/4000 (Supervisor Engine II), 5500/5000, 6500/6000, 2926, 2926G, 2948G en 2980G platforms

- Cisco IOS®-softwarerelease 12.0(7)XE voor Catalyst 6500/6000-platforms
- Cisco IOS-softwarerelease 12.1(8a)EW voor Catalyst 4500/4000 Supervisor Engine III
- Cisco IOS-softwarerelease 12.1(12c)EW voor Catalyst 4500/4000 Supervisor Engine IV
- Cisco IOS-softwarerelease 12.0(5)WC5 voor de Catalyst 2900XL- en 3500XL-reeks
- Cisco IOS-softwarerelease 12.1(11)AX voor Catalyst 3750 Series switches
- Cisco IOS-softwarerelease 12.1(14)AX voor Catalyst 3750 Metro switches
- Cisco IOS-softwarerelease 12.1(19)EA1 voor Catalyst 3560 Series switches
- Cisco IOS-softwarerelease 12.1(4)EA1 voor Catalyst 3550 Series switches
- Cisco IOS-softwarerelease 12.1(11)AX voor Catalyst 2970 Series switches
- Cisco IOS-softwarerelease 12.1(12c)EA1 voor Catalyst 2955 Series switches
- Cisco IOS-softwarerelease 12.1(6)EA2 voor Catalyst 2950 Series switches
- Cisco IOS-softwarerelease 12.1(11)EA1 voor Catalyst 2950 Long Reach Ethernet (LRE) switches
- Cisco IOS-softwarerelease 12.1(13)AY voor Catalyst 2940 Series switches

---

Opmerking: STP PortFast BPDU-beveiliging is niet beschikbaar voor de switches Catalyst 8500, 2948G-L3 of 4908G-L3.

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

In dit document wordt de functie PortFast Bridge Protocol Data Unit (BPDU) Guard beschreven. Deze functie is een van de verbeteringen van het Spanning Tree Protocol (STP) die Cisco heeft ontwikkeld. Hiermee worden de betrouwbaarheid, beheerbaarheid en security van het switchnetwerk verbeterd.

Beschrijving van functie

STP configureert een ingeschakelde topologie in een lusvrije, boomachtige topologie. Wanneer de verbinding op een brughaven omhoog gaat, komt de berekening STP op die haven voor. Het resultaat van de berekening is de overgang van de haven in het door:sturen of het blokkeren staat. Het resultaat hangt af van de positie van de poort in het netwerk en van de STP-parameters. Deze berekening en overgangsperiode duurt gewoonlijk ongeveer 30 tot 50 seconden. Op dat moment gaan er geen gebruikersgegevens via de poort over. Sommige gebruikerstoepassingen kunnen een time-out tijdens de periode uitvoeren.

Schakel de functie STP PortFast in om een onmiddellijke overgang van de poort naar de doorstuurstatus mogelijk te maken. PortFast schakelt de poort onmiddellijk over naar STP-doorstuurmodus bij verbinding. De haven neemt nog steeds deel aan STP. Dus als de poort onderdeel van de lus moet zijn, gaat de poort uiteindelijk over in STP-blokkeringsmodus.

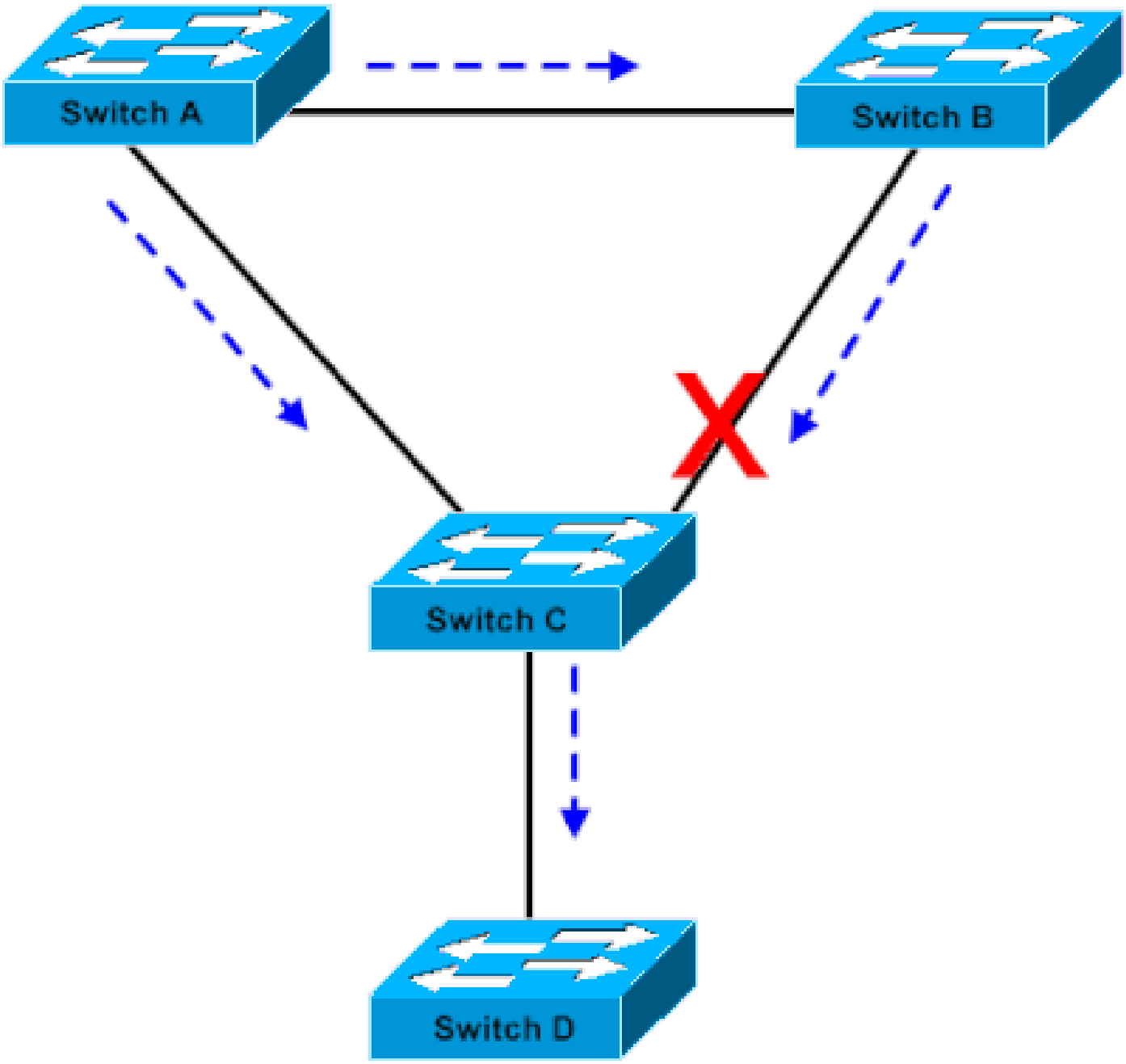
Zolang de poort deelneemt aan STP kan enig toestel de root-brug functie aannemen en de actieve STP topologie beïnvloeden. Om de root-brug functie over te nemen, zou het toestel worden aangesloten op de poort en zou STP draaien met een lagere brugprioriteit dan die van de huidige root-brug. Als een ander toestel op deze manier de root-brug functie overneemt, maakt het het netwerk suboptimaal. Dit is een eenvoudige vorm van een Denial of Service (DoS)-aanval op het netwerk. De tijdelijke introductie en de daaropvolgende verwijdering van STP-apparaten met een lage (0) brugprioriteit veroorzaken een permanente herberekening van STP.

De verbetering van de STP PortFast BPDU-beveiliging stelt netwerkontwerpers in staat om de STP-domeingrenzen af te dwingen en de actieve topologie voorspelbaar te houden. De apparaten achter de poorten die STP PortFast ingeschakeld hebben, kunnen de STP-topologie niet beïnvloeden. Bij de ontvangst van BPDU's schakelt de BPDU-bewaker de poort uit die PortFast heeft geconfigureerd. De BPDU bewaker zet de poort over naar de erreless status en er verschijnt een bericht op de console. Dit bericht is een voorbeeld:

```
2000 May 12 15:13:32 %SPANTREE-2-RX_PORTFAST:Received BPDU on PortFast enable port.
Disabling 2/1
2000 May 12 15:13:32 %PAGP-5-PORTFROMSTP:Port 2/1 left bridge port 2/1
```

Neem dit voorbeeld:

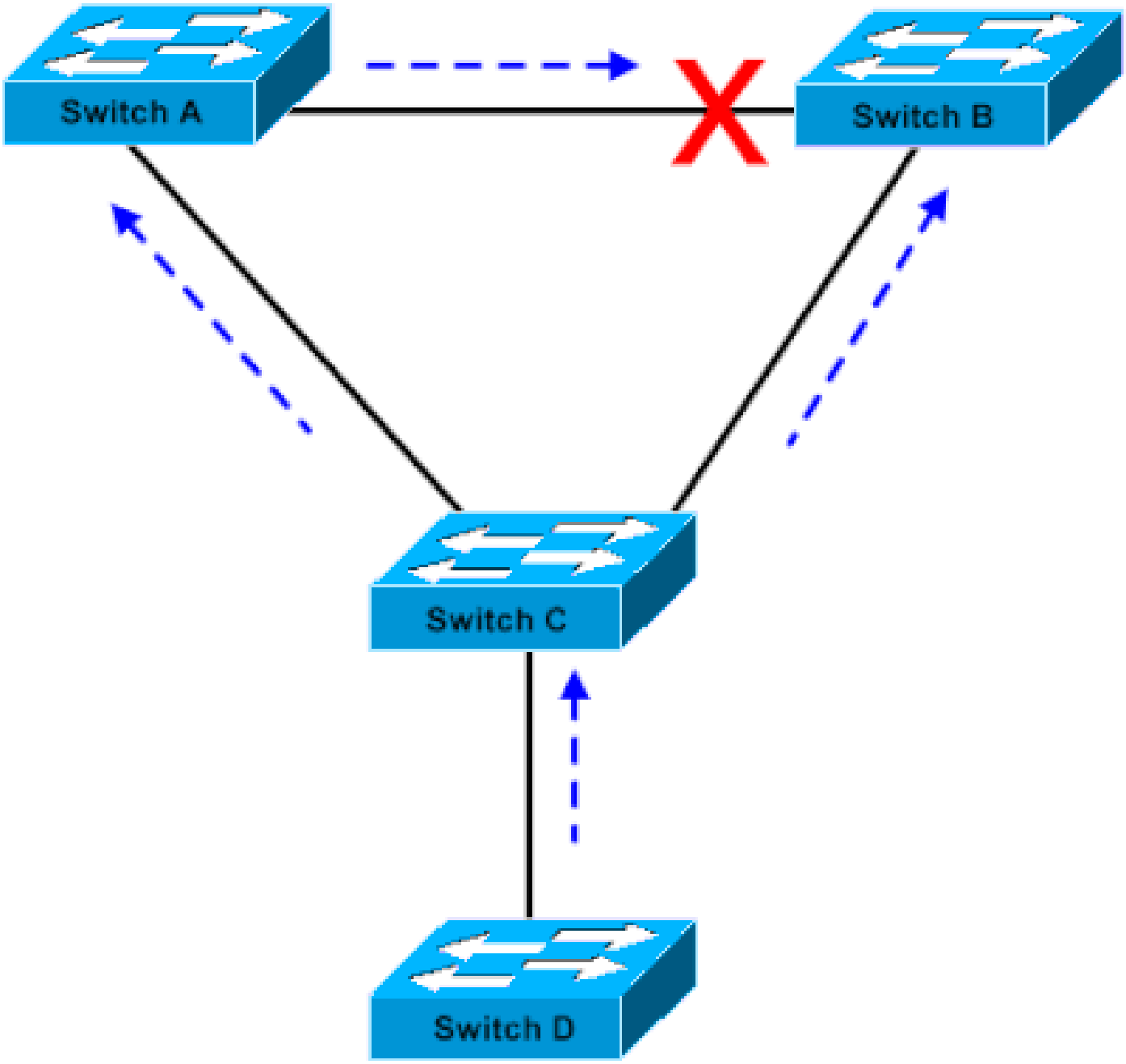
Afbeelding 1



Brugverbinding

Bridge A heeft prioriteit 8192 en is de basis voor het VLAN. Bridge B heeft 16384 en is de back-up-root-brug voor hetzelfde VLAN. De bruggen A en B, die een Gigabit Ethernet-verbinding vormen, vormen een kern van het netwerk. Bridge C is een access switch en heeft PortFast geconfigureerd op de poort die verbinding maakt met apparaat D. Als de andere STP parameters standaard zijn, is de brug C poort die verbinding maakt met brug B in STP blokkerende staat. Apparaat D (PC) neemt niet deel aan STP. De stippelpijlen geven de stroom van STP BPDU's aan.

Afbeelding 2



Op Linux gebaseerde Bridge Application wordt op een PC gestart

In afbeelding 2 is apparaat D begonnen deel te nemen aan STP. Bijvoorbeeld, wordt een Linux-gebaseerde bridge applicatie gelanceerd op een PC. Als de voorrang van de softwarebrug 0 of om het even welke waarde minder dan de prioriteit van de root-brug is, neemt de softwarebrug de functie van de root-brug over. De Gigabit Ethernet-link die de twee kern-switches met elkaar verbindt, maakt de overstap naar de blokkeringsmodus. De overgang veroorzaakt alle gegevens in dat VLAN om via de 100-Mbps verbinding te stromen. Als meer gegevensstroom via de kern in VLAN dan de verbinding kan aanpassen, komt de daling van kaders voor. De framedaling leidt tot een connectiviteitsonderbreking.

De STP PortFast BPDU-wachtfunctie voorkomt een dergelijke situatie. De functie schakelt de poort uit zodra bridge C de STP BPDU van apparaat D ontvangt.

Configuratie

U kunt STP PortFast BPDU-bewaker in- of uitschakelen op wereldwijde basis, wat van invloed is op alle poorten die PortFast geconfigureerd hebben. Standaard is STP BPDU-beveiliging uitgeschakeld. Geef deze opdracht uit om STP PortFast BPDU-bewaker op de switch in te schakelen:

CatOS-opdracht

<#root>

```
Console> (enable)
set spantree portfast bpdu-guard enable

Spantree portfast bpdu-guard enabled on this switch.
Console> (enable)
```

Cisco IOS®-softwarerelease

<#root>

```
CatSwitch-IOS(config)#
spanning-tree portfast bpduguard
CatSwitch-IOS(config)
```

Wanneer STP BPDU-bewaker de poort uitschakelt, blijft de poort in de uitgeschakelde toestand staan tenzij de poort handmatig is ingeschakeld. U kunt een poort configureren om zichzelf automatisch weer in te schakelen uit de erreless status. Geef deze opdrachten uit, die het erreless-timeout-interval instellen en de timeout-functie inschakelen:

CatOS-opdrachten

<#root>

```
Console> (enable)
set errdisable-timeout interval 400

Console> (enable)
set errdisable-timeout enable bpdu-guard
```

Cisco IOS-software – opdrachten

<#root>

```
CatSwitch-IOS(config)#
errdisable recovery cause bpduguard

CatSwitch-IOS(config)#
errdisable recovery interval 400
```

Opmerking: de standaard time-outinterval is 300 seconden en de time-outfunctie is standaard uitgeschakeld.

Monitor (bewaken)

Om te verifiëren of de functie is ingeschakeld of uitgeschakeld, geeft u de volgende opdracht uit.

Opdrachtoutput

CatOS-opdracht

<#root>

```
Console> (enable)
show spantree summary
Root switch for vlans: 3-4.
Portfast bpdu-guard enabled for bridge.

Uplinkfast disabled for bridge.
Backbonefast disabled for bridge.

Summary of Connected Spanning Tree Ports By VLAN:

Vlan  Blocking Listening Learning Forwarding STP Active

----- -------- --------- -------- ---------- ----------

   1         0         0        0          1          1

   3         0         0        0          1          1

   4         0         0        0          1          1

  20         0         0        0          1          1
```

```
Blocking Listening Learning Forwarding STP Active

----- -------- --------- -------- ---------- ----------

Total        0         0        0          4          4

Console> (enable)
```

Cisco IOS-softwarerelease

<#root>

```
CatSwitch-IOS#

show spanning-tree summary totals

Root bridge for: none.

PortFast BPDU Guard is enabled

UplinkFast is disabled
BackboneFast is disabled
Spanning tree default pathcost method used is short


Name                 Blocking Listening Learning Forwarding STP Active
-------------------- -------- --------- -------- ---------- ----------
  1 VLAN                  0         0         0         1          1

CatSwitch-IOS#
```

Gerelateerde informatie

- Cisco technische ondersteuning en downloads

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.