Verbetert Spanning Tree Protocol met Root Guard

Inhoud

Inleiding

Dit document beschrijft de verbeterde eigenschappen van de STP wortelwacht die geschakelde netwerkbetrouwbaarheid, beheersbaarheid, en veiligheid verbeteren.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

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.

Beschrijving van functie

De standaard STP biedt geen mogelijkheden voor de netwerkbeheerder om de topologie van het switched Layer 2 (L2) netwerk veilig af te dwingen. Een middel om topologie af te dwingen kan vooral in netwerken met gedeelde administratieve controle belangrijk zijn, waar de verschillende administratieve entiteiten of de bedrijven één geschakeld netwerk controleren.

De het door:sturen topologie van het geschakelde netwerk wordt berekend. De berekening is onder meer gebaseerd op de positie van de root-brug. Elke switch kan de root-brug in een netwerk zijn. Maar een meer optimale het door:sturen topologie plaatst de root-brug bij een specifieke vooraf bepaalde plaats. Met de standaard STP neemt elke brug in het netwerk met een lagere brug-ID de rol van de root-brug. De beheerder kan de positie van de root-brug niet afdwingen.

> Opmerking: de beheerder kan de root-brug-prioriteit op 0 instellen in een poging om de positie van de root-brug te beveiligen. Maar er is geen garantie tegen een brug met een prioriteit van 0 en een lager MAC-adres.

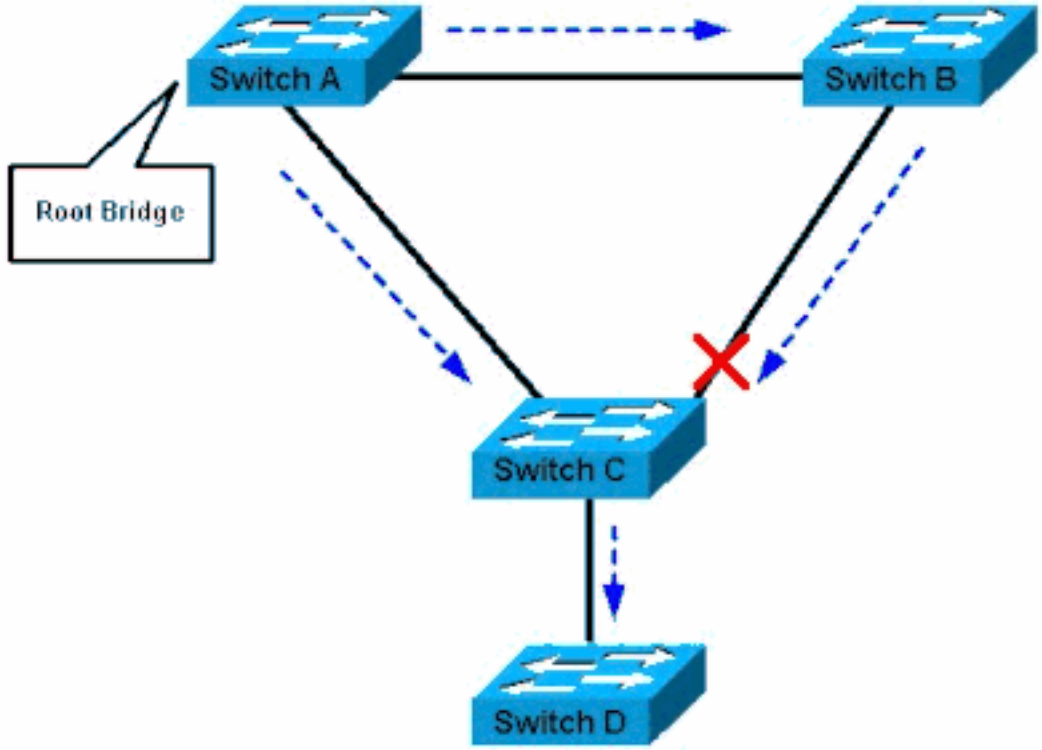
De root guard functie biedt een manier om de root-brug plaatsing in het netwerk af te dwingen.

De root guard zorgt ervoor dat de poort waarop de root guard is ingeschakeld de aangewezen poort is. Normaliter zijn root-brug poorten alle aangewezen poorten, tenzij twee of meer poorten van de root-brug onderling verbonden zijn. Als de brug superieure STP Bridge Protocol Data Units (BPDU's) ontvangt op een poort die met root guard is ingeschakeld, verplaatst root guard deze poort naar een root-inconsistente STP-staat. Deze wortel-inconsistente staat is effectief gelijk aan een luisterstaat. Geen verkeer wordt door:sturen over deze haven. Op deze manier wordt de positie van de root-brug afgedwongen door de wortelbeschermer.

Het voorbeeld in deze sectie toont aan hoe een schurkenroot-brug problemen op het netwerk kan veroorzaken en hoe de wortelwacht kan helpen.

In afbeelding 1, vormen Switches A en B de kern van het netwerk en is A de root-brug voor een VLAN. Switch C is een switch op de toegangslaag. Het verband tussen B en C is aan de C kant geblokkeerd. De pijlen tonen de stroom van STP BPDU's.

Afbeelding 1

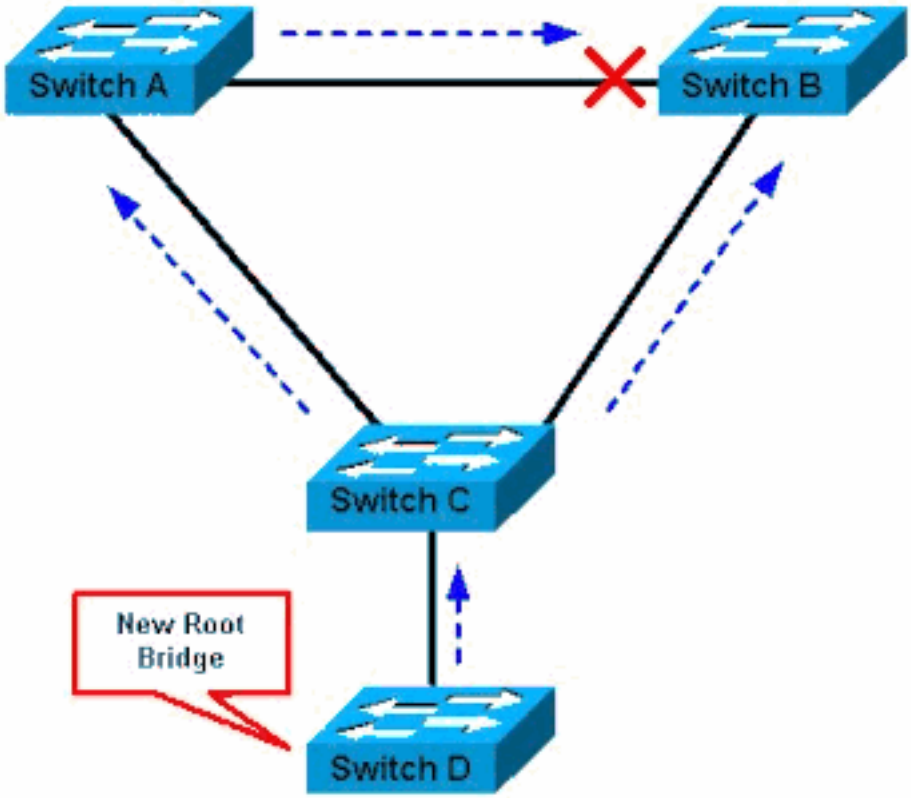


Switch A is Root-brug

In afbeelding 2 begint apparaat D deel te nemen aan STP. Software-gebaseerde bridge applicaties worden bijvoorbeeld gelanceerd op PC's of andere switches die u aansluit op een service-provider netwerk. Als de prioriteit van bridge D 0 is of een waarde die lager is dan de prioriteit van de root-brug, wordt apparaat D gekozen als een root-brug voor dit VLAN. Als de koppeling tussen apparaat A en B 1 gigabit is en de verbindingen tussen A en C evenals B en C 100 Mbps zijn, veroorzaakt de keuze van D als wortel de Gigabit Ethernet-verbinding die de twee te blokkeren kern switches verbindt.

Dit blok veroorzaakt alle gegevens in dat VLAN om via een 100-Mbps link over de toegangslaag te stromen. Als meer gegevensstromen via de kern in dat VLAN dan deze verbinding kan aanpassen, komt de daling van sommige kaders voor. De framedaling leidt tot een prestatieverlies of een connectiviteitsonderbreking.

Afbeelding 2



Switch D is een nieuwe Root-brug

De functie van de wortelwacht beschermt het netwerk tegen dergelijke kwesties.

De configuratie van root guard is per poort. Root guard laat de poort niet toe om een STP root poort te worden, dus de poort is altijd STP-aangewezen. Als een betere BPDU op deze poort aankomt, houdt de root guard geen rekening met de BPDU en kiest een nieuwe STP root. In plaats daarvan, zet de wortelwacht de haven in de wortel-inconsistente staat STP. U moet root guard inschakelen op alle poorten waar de root-brug niet mag verschijnen. Op een bepaalde manier, kunt u een perimeter rond het deel van het netwerk vormen waar de wortel STP kan worden gevestigd.

In afbeelding 2, schakelt u de hoofdbeveiliging in op de Switch C-poort die is aangesloten op Switch D.

Switch C in afbeelding 2 blokkeert de poort die wordt aangesloten op Switch D, nadat de switch een superieure BPDU heeft ontvangen. Root guard zet de poort in de root-inconsistente STP-staat. In deze toestand gaat er geen verkeer door de haven. Nadat apparaat D ophoudt superieure BPDU's te verzenden, wordt de poort opnieuw ontgrendeld. Via STP gaat de haven van de luisterstaat naar de leerstaat, en uiteindelijk overgangen naar de voorwaartse staat. Herstel is automatisch; er is geen menselijk ingrijpen nodig.

Dit bericht verschijnt nadat root guard een poort blokkeert:

```
%SPANTREE-2-ROOTGUARDBLOCK: Port 1/1 tried to become non-designated in VLAN 77.
Moved to root-inconsistent state
```

Beschikbaarheid

Root Guard is beschikbaar in Catalyst 6500/6000 waarin Cisco IOS®-systeemsoftware wordt uitgevoerd. Deze optie is eerst geïntroduceerd in Cisco IOS-softwarerelease 12.0(7)XE. Voor Catalyst 4500/4000 die Cisco IOS-systeemsoftware gebruikt, is deze functie beschikbaar in alle releases.

Voor de Catalyst 2900XL en 3500XL switches is root guard beschikbaar in Cisco IOS-softwarerelease 12.0(5)XU en hoger. De Catalyst 2950 Series switches ondersteunen de functie voor root guard in Cisco IOS-softwarerelease 12.0(5.2)WC(1) en hoger. De switches van Catalyst 3550 Series ondersteunen de functie voor de basisbewaking in Cisco IOS-softwarerelease 12.1(4)EA1 en hoger.

Deze optie is ook beschikbaar voor nieuwere Cisco Catalyst 650 Series Switches.

Configuratie

Cisco IOS-softwarerelease 1500/1600 en Catalyst 4500/4000

Op de switches Catalyst 6500/6000 of Catalyst 4500/4000 die Cisco IOS-systeemsoftware uitvoeren, geeft u deze set opdrachten uit om STP root guard te configureren:

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
!
Switch#(config)#interface fastethernet 3/1
Switch#(config-if)#spanning-tree guard root
!
```

> **Opmerking**: Cisco IOS-softwarerelease 12.1(3a)E3 voor Catalyst 6500/6000 waarin Cisco IOS-systeemsoftware wordt uitgevoerd, heeft deze opdracht gewijzigd van **Spanning-Tree Routing** in **Spanning-Tree Guard root** . Catalyst 4500/4000 waarop Cisco IOS-systeemsoftware wordt uitgevoerd, gebruikt de opdracht **Spanning-Tree Guard root** in alle releases.

Cisco IOS-softwareconfiguratie voor Catalyst 2900XL/3500XL, 2950 en 3550

Configureer op de Catalyst 2900XL, 3500XL, 2950 en 3550 switches met root guard in interfaceconfiguratiemodus, zoals in dit voorbeeld wordt getoond:

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# interface fastethernet 0/8
Switch(config-if)# spanning-tree rootguard
Switch(config-if)# ^Z
*Mar 15 20:15:16: %SPANTREE-2-ROOTGUARD_CONFIG_CHANGE: Rootguard enabled on
port FastEthernet0/8 VLAN 1.
Switch#
```

Wat is het verschil tussen STP BPDU Guard en STP Root Guard?

De BPDU-beveiliging en de root guard zijn vergelijkbaar, maar hun impact is anders. BPDU-

bewaker schakelt de poort uit bij ontvangst van BPDU als PortFast is ingeschakeld op de poort. De uitschakeling ontzegt apparaten achter dergelijke havens effectief aan deelname aan STP. U moet de poort die in de erreless status is gezet handmatig opnieuw inschakelen of de **errunk-time-out** configureren .

Root guard staat het apparaat toe om deel te nemen aan STP zolang het apparaat niet probeert om de root te worden. Als root guard de poort blokkeert, is het daaropvolgende herstel automatisch. Herstel vindt plaats zodra het apparaat dat van het apparaat afwijkt, geen superieure BPDU's meer verstuurt.

Zie Verbetering in Spanning Tree PortFast BPDU Guard voor meer informatie over BPDU-bewaking.

Helpt de Root Guard met het Two Roots Problem?

Er kan een unidirectionele verbindingsmislukking zijn tussen twee bruggen in een netwerk. Wegens de mislukking, ontvangt één brug niet BPDUs van de root-brug. Met zo'n mislukking ontvangt de root switch frames die andere switches verzenden, maar de andere switches ontvangen niet de BPDU's die de root switch verstuurt. Dit kan leiden tot een STP-lus. Omdat de andere switches geen BPDU's van de wortel ontvangen, geloven deze switches dat zij de wortel zijn en beginnen BPDU's te verzenden.

Wanneer de echte root-brug BPDUs begint te ontvangen, verwerpt de wortel BPDUs omdat zij niet superieur zijn. De root-brug verandert niet. Daarom helpt root guard niet om dit probleem op te lossen. De functies UniDirectional Link Detection (UDLD) en loop guard pakken dit probleem aan.

Zie Spanning Tree Protocol Problemen en Gerelateerde Design-overwegingen voor meer informatie over STP-storingsscenario's en probleemoplossing.

Gerelateerde informatie

- De UDLD-protocolfunctie begrijpen en configureren
- Herstel de uitgeschakelde poortstatus op Cisco IOS-platforms
- 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.