

Rep begrijpen op Catalyst 9000 Switches

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Terminologie](#)

[REP-theorie](#)

[REP alternatieve poortselectie](#)

[Geblokkeerde poortadvertenties](#)

[Alternatieve poortselectie](#)

[End-poortadvertenties](#)

[Melding van REP-koppelingsfouten](#)

[REP voorkeurspoort en VLAN-taakverdeling](#)

[Configureren](#)

[Netwerkdigram](#)

[Configuraties](#)

[Verifiëren](#)

[Overzicht van opdrachten](#)

[Problemen oplossen](#)

[Invoerwachtrij-wig](#)

[REP-logberichten](#)

[Gerelateerde informatie](#)

Inleiding

Dit document beschrijft hoe u Resilient Ethernet Protocol (REP) op Catalyst 9000 switches kunt configureren en valideren.

Voorwaarden

Vereisten

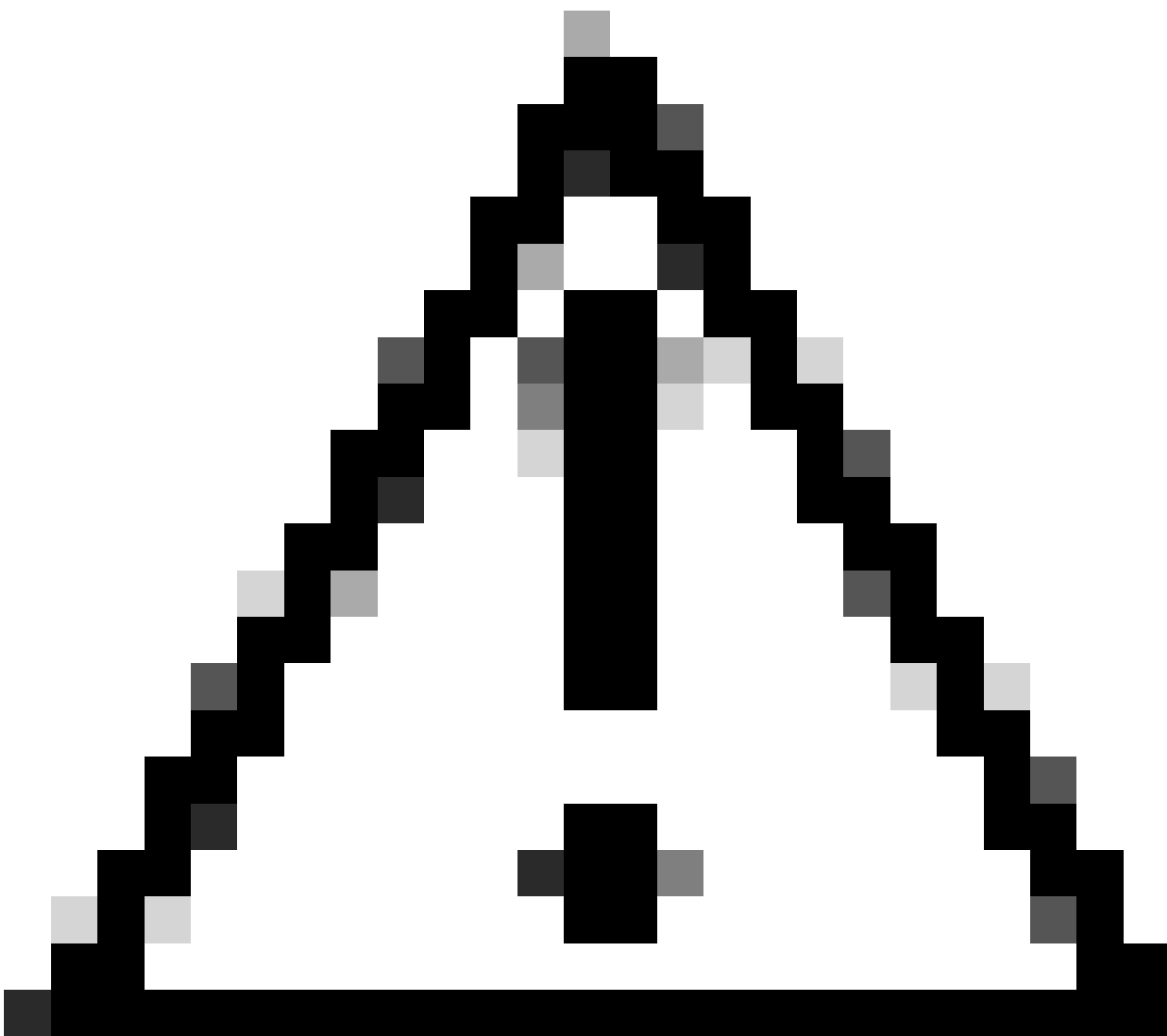
Cisco raadt u aan kennis van deze onderwerpen te hebben:

- Layer 2-luspreventie

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Catalyst 9200
 - Catalyst 9300
 - Catalyst 9400
 - Catalyst 9500
 - Catalyst 9600
 - Cisco IOS XE 17.6.5 en hoger
-



Waarschuwing: REP wordt niet ondersteund op switches met Stackwise Virtual (SVL)

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.

Achtergrondinformatie

REP is een bedrijfseigen protocol van Cisco dat is ontworpen om netwerkluss te voorkomen en

snelle convergentie van koppelingsfouten in Layer 2 Ethernet-netwerken te bieden. Het is een alternatief voor Spanning Tree Protocol en wordt vaak gebruikt in specifieke Layer 2-topologieën die grote Layer 2-uitbreidingen vereisen, zoals IoT-netwerken, industriële netwerken of productienetwerken. REP "segmenten" worden gevormd door poorten tussen switches aan elkaar te koppelen die zijn geconfigureerd met dezelfde segmentid. Met functies zoals REP-taakverdeling en de mogelijkheid om samen met STP te bestaan, kan REP worden gebruikt om complexe maar voorspelbare Layer 2-topologieën te construeren.

Terminologie

Begrip	Definitie
Segment	Keten van onderling verbonden havens die hetzelfde segment-ID delen
Segment-ID	Aantal dat wordt gebruikt om het segment weer te geven en ligt tussen 1 en 1024
REP-poort	Poort die ingesteld is op REP. STP is uitgeschakeld op REP-poorten.
Edge-poort	Poort die één rand van het REP-segment beëindigt.
Alternatieve poort	Poort die VLAN's in het segment blokkeert om lusvorming te voorkomen. Er zijn 2 alternatieve poorten in het segment als taakverdeling is geconfigureerd
Open poort	Poorten in het segment dat alle VLAN's doorstuurt
Gesloten segment	REP Segment waar beide randpoorten op dezelfde switch staan en verbinding met elkaar hebben. Wordt ook wel een 'Ring Segment' genoemd.
Segment openen	REP Segment waar de randhavens geen connectiviteit aan elkaar hebben. De randpoorten bevinden zich op verschillende switches en hebben daartussen een blokkerende poort.
Link Status Layer (LSL)	3-weg handshake protocol verantwoordelijk voor buurnabijheid oprichting en het handhaven van link status. LSL frames worden elke 1 seconde verzonden op REP poorten.
Hardware Flood Layer (HFL)	Layer 2 die verantwoordelijk is voor het faciliteren van snelle convergentie na koppelingsfouten door REP PDU's via multicast te overspoelen

BPA (Blocked Port Advertisement)	Bericht dat door een poort wordt verzonden om de lijst met VLAN's te adverteren die worden geblokkeerd. BPA's kunnen ook topologiewijzigingen dragen, waardoor de ontvangende poorten hun MAC-tabel kunnen doorspoelen
End-poortadvertenties (EPA)	Verstrekt globale informatie over het REP segment en wordt verzonden door Edge-poorten
REP-beheer VLAN	VLAN gebruikt voor overstromingen REP snelle meldingen voor convergentie na koppelingsfout. De HFL werkt hier als hij geconfigureerd is. Als dit niet het geval is, is REP Admin VLAN 1.

REP-theorie

Met REP kunt u switching loops voorkomen door VLAN's te blokkeren op één poort in het segment dat bekend staat als de alternatieve poort. Wanneer alle poorten in het REP-segment zich in een UP-staat bevinden, blokkeert de alternatieve poort om de lus te voorkomen. Wanneer een link in het REP-segment mislukt, of als een switch een probleem heeft dat resulteert in het verlies van REP-protocolpakketten, dan worden de alternatieve poortwezens doorgestuurd voor de VLAN's die het voorheen blokkeerde. Het is belangrijk om op te merken dat vanwege dit, REP-segmenten slechts één mislukte poort binnen het segment kunnen verwerken. Meer dan 1 koppelingsfout op het REP-segment kan verkeersverlies tot gevolg hebben.

Wanneer REP is ingeschakeld op een interface blokkeert het onmiddellijk alle VLAN's. De REP LSL neemt het over en begint met het verzenden van LSL PDU's om een nabijheid duidelijk te maken. De nabijheid wordt gemaakt met behulp van een 3-weg handdruk met volgende LSL hello pakketten die met 1 seconde intervallen worden verzonden om REP burenen te handhaven.

Tijdens de detectie van de REP-buur wisselen de apparaten hun REP-segment-ID en hun poort-ID uit.

- Segment-ID is een nummer tussen 1 en 1024 en is op de interface geconfigureerd wanneer REP wordt ingeschakeld. Dit is een unieke identificatie van het REP-segment.
- Port-id is een 60-bits woord dat automatisch wordt gegenereerd vanaf het MAC-adres van het systeem en het poortnummer op de switch.
- De LSL PDU wordt verzonden naar het adres van bestemming MAC is 0180.c200.0000

```
<#root>
```

```
9200-STACK-1#
```

```
show interface port-channel1 rep detail | i PortID
```

```
PortID: 08E9
```

```
78BC1A4FDD80
```

```
<--- Port ID with system MAC in bold
```

9200-STACK-1#

```
show version | i MAC
```

Base Ethernet MAC Address :

78:bc:1a:4f:dd:80

<-- Switch system MAC

Een REP poort gaat naar een Failure-status nadat deze is uitgeschakeld of de LSL hello-time-out verloopt na 5 seconden.

REP alternatieve poortselectie

De REP Alternate poort is de poort in het segment dat VLAN's blokkeert.

- De verkiezing van de Alternate haven gebeurt onmiddellijk nadat REP-buren zijn opgericht met behulp van een voorstel en een overeenkomst mechanisme om te bepalen welke enkele haven in het segment nog steeds blokkeert.
- Elke haven in het segment adverteert met zijn havensleutel en havenprioriteit en wacht op de overeenkomst.
- De haven met de hoogste prioriteit wordt gekozen als de Alternate haven.
- Het verkiezingsproces verloopt via REP BPA-berichten.

Geblokkeerde poortadvertenties

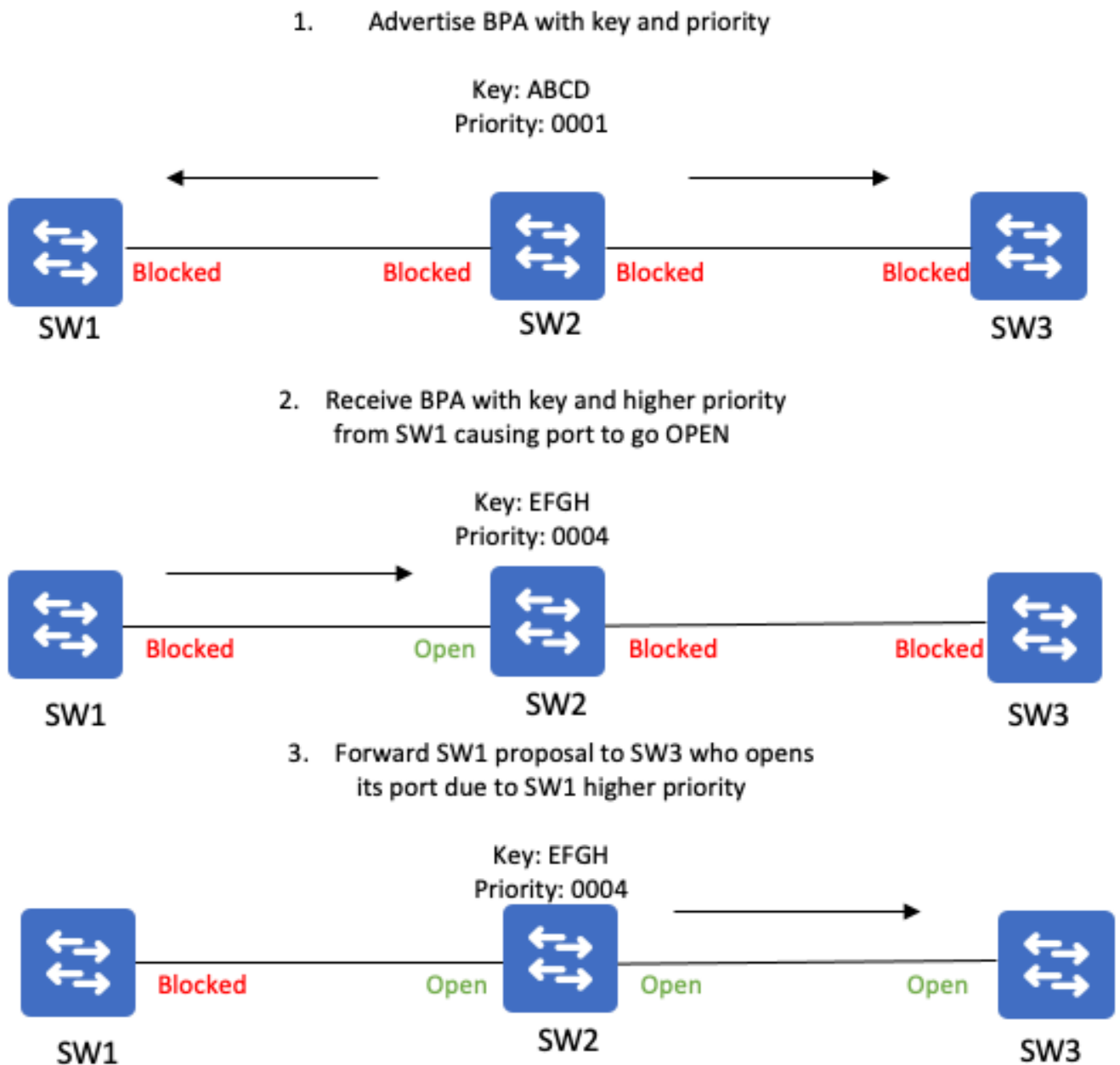
Een BPA-bericht bestaat uit een poortsleutel en poortprioriteit.

- De REP Port Key is een 9-byte identifier die wordt gegenereerd elke keer dat de poort een blokkerende status bereikt (die onmiddellijk wordt ingeschakeld voor de link naar REP-poorten).
- Het is een combinatie van de poort-ID en een willekeurig gegenereerd nummer.
- De Port Priority is ook een identificatie van 9 bytes.

Alternatieve poortselectie

1. Op verbinding en terwijl de REP-poort in een blokkerende staat is, adverteert het zijn poortsleutel en prioriteit aan zijn REP-buur
2. De ontvangende haven vergelijkt de ontvangen BPA-poortprioriteit met zijn eigen poortprioriteit
3. De ontvangende poort reageert met een ACK-bericht met de sleutel die in de BPA van de buurpoort werd ontvangen. Wanneer de buur zijn eigen sleutel in de BPA ontvangt weet hij dat de BPA een ACK-bericht is van zijn buur
4. Als ACK een poortprioriteit bevat die hoger is dan de lokale poortprioriteit, wordt de lokale poort naar een OPEN status verplaatst. Het reageert niet op de buur met de hogere prioriteit, maar het doet het voorstel zijn andere REP-rapport aan zijn andere REP-buur toekomen

5. De andere REP-buur vergelijkt de ontvangen poortprioriteit met zijn eigen prioriteit. Als de ontvangen prioriteit hoger is dan de lokale prioriteit, reageert het ook niet en stuurt het voorstel langs. Als de lokale prioriteit hoger is, reageert het op het oorspronkelijke voorstel met een eigen prioriteit



Dit proces herhaalt zich tot de poort met de hoogste prioriteit in de blokkeringsmodus blijft staan. Dit wordt de alternatieve poort van het segment. De Alternate poort blijft BPA-berichten met de poortsleutel naar het REP-segment verzenden. Alle REP-poorten in het segmentcachegeheugen vormen de sleutel van de Alternate poort.

In een stabiel REP-segment zijn alle havens het eens over de Alternate-poort door allen die dezelfde kopie van de alternatieve poortsleutel hebben. Elke switch die de poort-sleutel-ID van de Alternate-poort bewaart, wordt van belang tijdens koppelingsstoringsscenario's.

End-poortadvertenties

EPA-berichten worden elke 4 seconden gegenereerd door edge ports. Deze berichten worden door elke REP-interface in het segment doorgestuurd en elke poort voegt zijn eigen topologieinformatie toe aan het bericht.

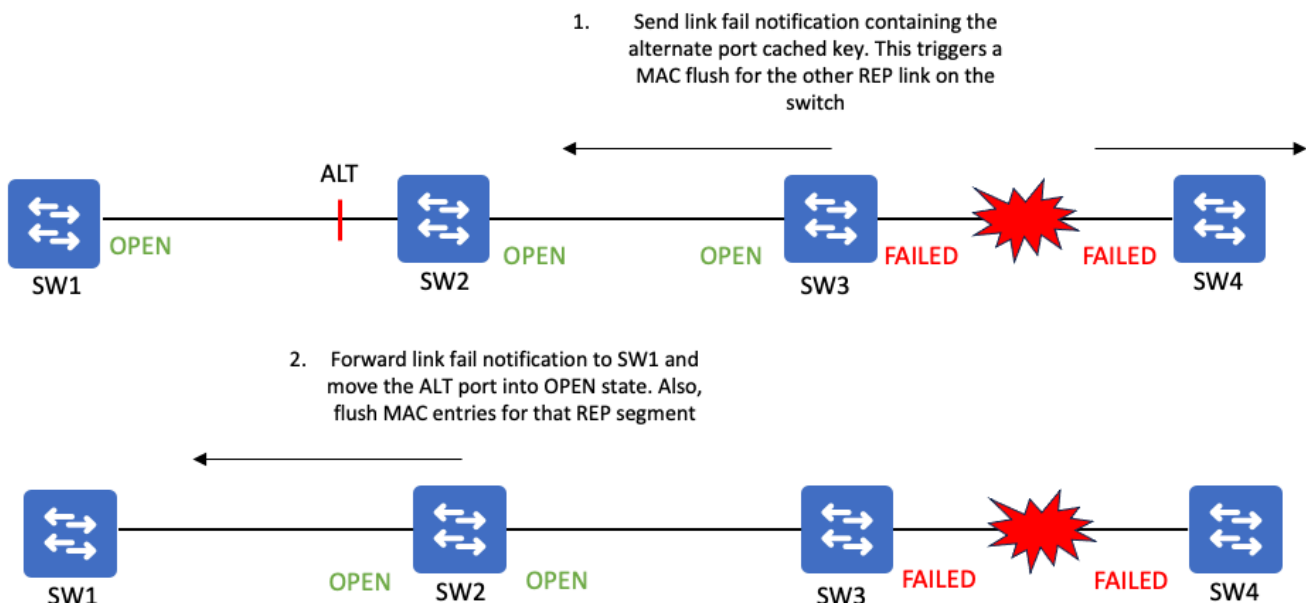
Zodra de randpoort een EPA ontvangt die door de andere randpoort in het segment wordt gegenereerd, heeft het een volledige topologie van het gehele segment.

De EPA's zorgen ervoor dat elke randpoort elkaar kan zien en vergemakkelijken de keuze van de primaire randpoort. De randpoort met de hoogste prioriteit wordt de primaire randpoort.

Melding van REP-koppelingsfouten

Wanneer een link in een REP-segment mislukt, wordt deze verplaatst naar 'Mislukte' status en wezens die meldingen van link-falen verzenden die de gecacheerde sleutel van de Alternatieve poort bevatten. De verzendende switch spoelt ook MAC-adressen voor de REP-link die nog steeds omhoog is.

De REP-switch ontvangt het bericht van koppelingsstoring en stuurt het door naar elke REP-buren in het segment, evenals doorspoelt MAC-adresgegevens voor poorten in het REP-segment. Als de switch die het bericht van koppelingsstoring ontvangt de alternatieve poort op het segment bevat, verplaatst deze de poort naar een OPEN status.



Meldingen van linkfouten worden op twee manieren verspreid:

1. Snelle REP-meldingen via het verzenden van BPA-berichten naar het Cisco-multicastadres van 100.0ccc.ccce
2. REP Betrouwbare meldingen via het verzenden van BPA-berichten in REP BPDU-frames

(vergelijkbaar met REP LSL-frames).

Feature	Snelle melding	Betrouwbare melding
Doorsturen van hardware	Ja	Nee
betrouwbaar	Nee	Ja via volgnummer en heruitzendingen
Gaat door een alternatieve/blokkerende poort	Nee	Ja
Doorgestuurd buiten het REP-segment	Ja	Nee
Verstuurd via REP Admin VLAN	Ja	Nee (gebruikt native VLAN)

REP Link Mislukte Kennisgevingen handelen vergelijkbaar met STP TCN's in die zin dat ze gepunteerd worden naar de CPU en MAC-flushing op REP-poorten veroorzaken. Met extra configuratie op REP-poorten tegenover STP-segmenten, kan een melding van REP-koppelingfout worden geconverteerd naar een STP-TCP om het STP-domein te informeren over het doorspoelen van MAC's vanwege de REP-koppelingfout.

REP voorkeurspoort en VLAN-taakverdeling

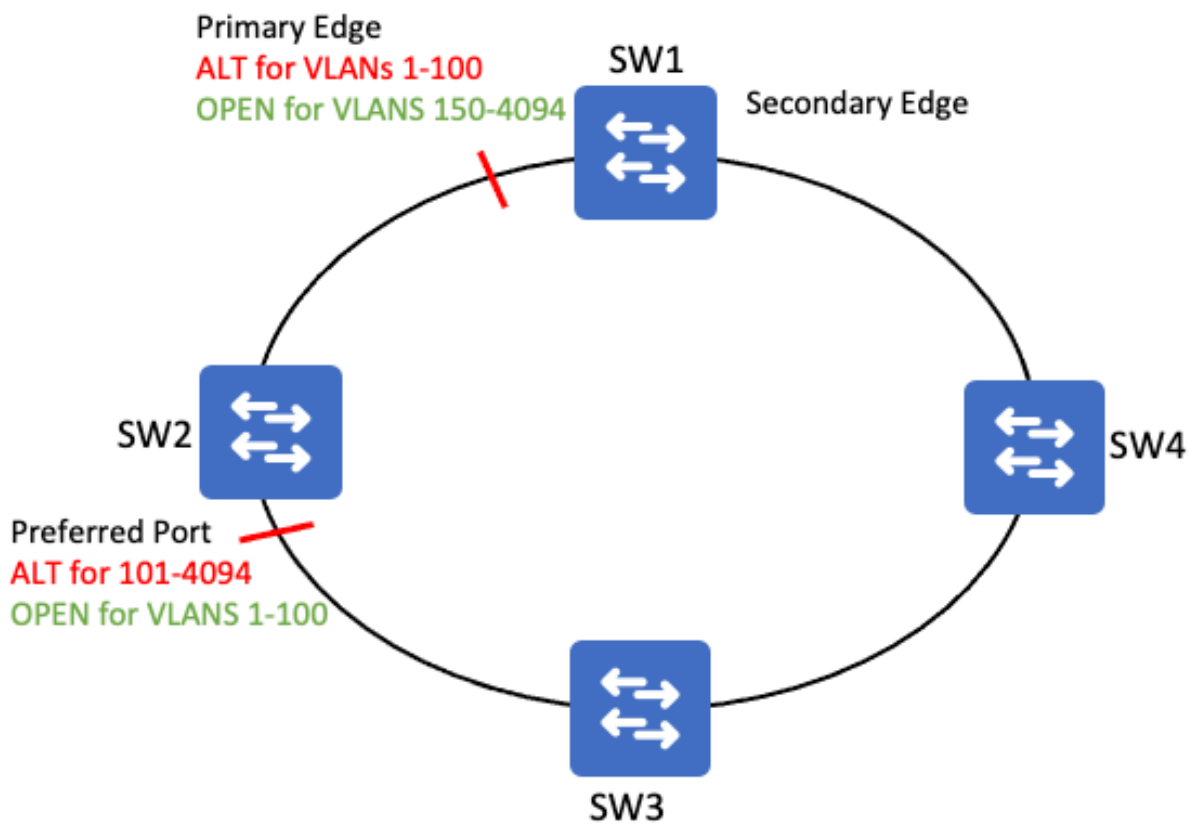
Wanneer VLAN-taakverdeling is geconfigureerd, is de REP Primaire Edge-poort de poort die taakverdeling kan initiëren. De REP Preferred-poort is de poort die de voorkeur heeft om de alternatieve poort te worden.

De primaire randpoort is relevant in het scenario voor taakverdeling omdat taakverdeling wordt gestart vanaf de primaire randpoort via extra configuratie.

Taakverdeling wordt bereikt door te configureren welke VLAN's door de voorkeurspoort moeten worden geblokkeerd.

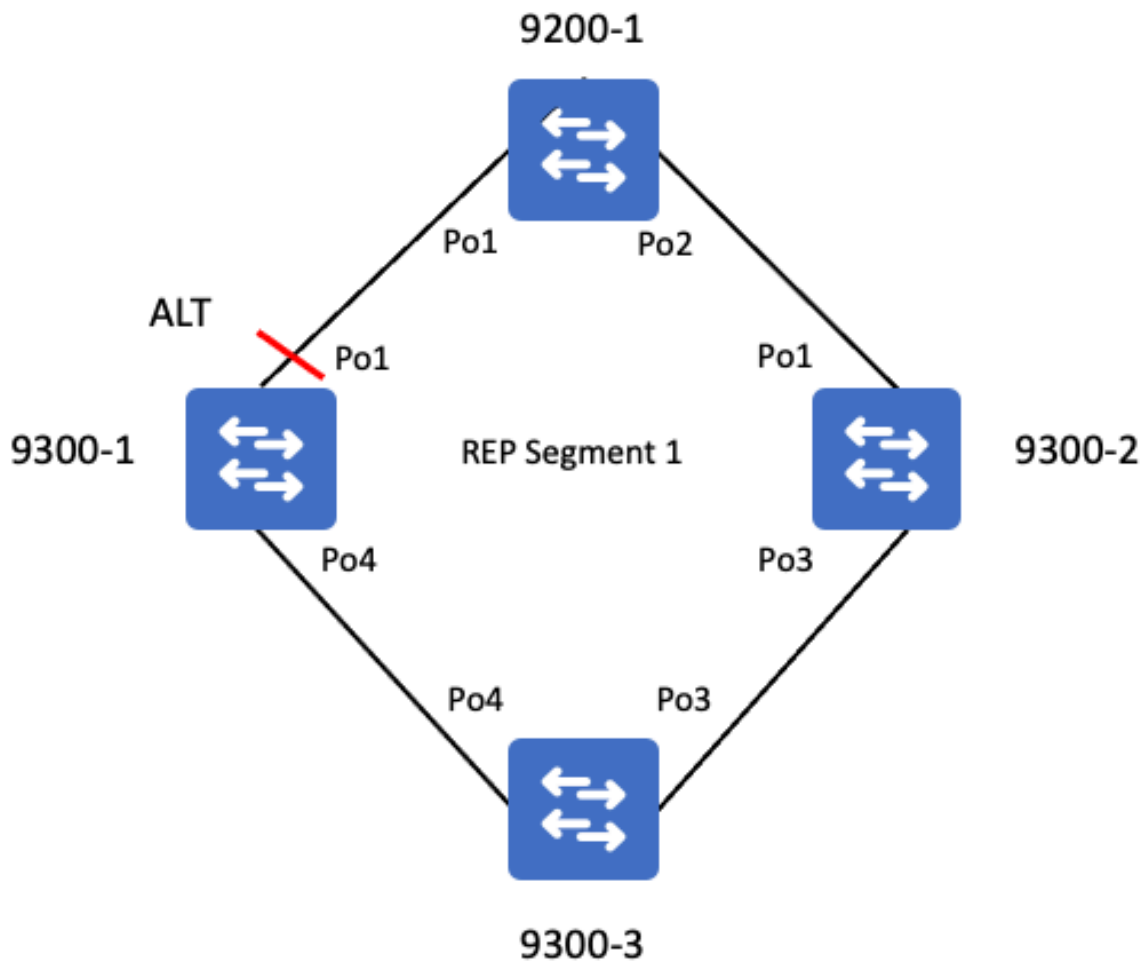
- De resterende VLAN's worden geblokkeerd op de primaire Edge-poort.
- Er zijn 2 alternatieve poorten wanneer VLAN-taakverdeling is geconfigureerd en actief is.

Zodra load balancing is geconfigureerd, heeft dit geen invloed tot er een link uitval of handmatige voorrang wordt geactiveerd vanaf de primaire edge poort.



Configurieren

Netzwerkdiagramm



Configuraties

Alle poorten moeten worden geconfigureerd als trunkpoorten met een overeenkomende REP-segment-id. De edge switch vereist de edge parameter.

```
<#root>
```

```
9200-STACK-1#
```

```
show running-config interface port-channel 1
```

```
Building configuration...
```

```
Current configuration : 100 bytes
```

```
!
```

```
interface Port-channel1
```

```
switchport mode trunk          <-- Must be a trunk
```

```
load-interval 30
```

```
rep segment 1 edge            <-- configure edge port in REP segment 1
```

```
end
```

REP-poorten die geen edge-poorten zijn, vereisen het edge-sleutelwoord niet.

```
<#root>
9300-STACK-2#
show running-config interface port-channel 1
Building configuration...
Current configuration : 69 bytes
!
interface Port-channel1
  switchport mode trunk

rep segment 1                <-- non-edge REP port configuration
end
```

Verifiëren

Zodra alle segmentpoorten zijn geconfigureerd is het segment volledig en zijn er geen mislukte poorten aanwezig.

Bevestig de REP-topologie.

```
<#root>
9200-STACK-1#
show rep topology

REP Segment 1
BridgeName          PortName  Edge Role
-----
9200-STACK-1       Po1
Pri  Open          <-- primary edge port
9300-STACK-1       Po1
Alt

<-- alternate port that is blocking VLANs
9300-STACK-1       Po4          Open
9300-STACK-3       Po4          Open
9300-STACK-3       Po3

Open          <-- port is OPEN and forwarding all VLANs
9300-STACK-2       Po3          Open
9300-STACK-2       Po1          Open
9200-STACK-1       Po2
```

Sec Open <-- secondary edge port

Bevestig REP status op een interface.

<#root>

9200-STACK-1#

show interface port-channel 1 rep <-- check REP status for the port

Interface	Seg-id	Type	LinkOp	Role
Port-channel1	1	Primary Edge	TWO_WAY	

Open <-- Edge port is not blocking any VLANs

Detailuitvoer geeft meer inzicht in de REP-status van de poort

<#root>

9200-STACK-1#

show interfaces port-channel1 rep detail

Port-channel1 REP enabled
Segment-id: 1 (Primary Edge)
PortID:

08E978BC1A4FDD80 <-- port ID made from system MAC + random number

Preferred flag: No
Operational Link Status: TWO_WAY
Current Key:

0BE934ED1B4798003405 <-- cached key of the segment Alternate port

Port Role: Open
Blocked VLAN:

Admin-vlan: 1 <-- REP admin vlan

Preempt Delay Timer: disabled

LSL Ageout Timer: 5000 ms

<-- default link status adjacency hold down timer

LSL Ageout Retries: 5
Configured Load-balancing Block Port:

none <-- no load balancing configured on the port

Configured Load-balancing Block VLAN: none

STCN Propagate to: none <-- sending TCNs into STP domain is disabled

LSL PDU rx: 924743, tx: 612406
HFL PDU rx: 1, tx: 1
BPA TLV rx: 611945, tx: 2
BPA (STCN, LSL) TLV rx: 0, tx: 0
BPA (STCN, HFL) TLV rx: 0, tx: 0
EPA-ELECTION TLV rx: 13, tx: 11
EPA-COMMAND TLV rx: 0, tx: 0
EPA-INFO TLV rx: 152998, tx: 152999

Overzicht van opdrachten

```
show rep topology
show rep topology detail
show rep topology segment <Id>
show rep topology segment <Id> detail
show rep topology archive
show rep topology archive detail
show interfaces gig<X/X> rep
show interfaces gig<X/X> rep detail
```

Problemen oplossen

Invoerwachtrij-wig

Op bepaalde versies van code kan het REP HSL-pakket de invoerwachtrij van een interface vastzetten.

- Dit kan gevolgen hebben voor REP convergentie als HSL-pakketten de invoerwachtrij vullen en LSL-convergentiepakketten niet kunnen worden verwerkt
- Dit wordt veroorzaakt door Cisco bug-id [CSCwc52868](#)
- De invoerwachtrij behandelt de verwerking van ALLE protocollen. Zodra de wachtrij "vol" wordt, verbergt het legitieme netwerkcontroleverkeer en kan het niet handmatig worden geleegd.

Symptomen van wachtrij

- Protocollen zoals CDP, IGMP, enz. werken niet meer (u kunt een buur in CDP, IGMP multicast programmeerproblemen verliezen, enzovoort).
- De symptomen variëren afhankelijk van welke eigenschappen en protocollen aan de interface arriveren die moeten worden verwerkt.
- De rij van de interfaceinput wordt gebruikt voor pakketten die bij een interface die moeten worden een rij gevormd en aan CPU voor verwerking worden gestraft aankomen
- Een invoerwachtrij wordt vastgeklemd wanneer een bepaald pakket niet kan worden dewachtrij en uiteindelijk de limiet van de invoerwachtrij wordt bereikt
- Zodra een grens van de interfaceingangrij wordt geraakt, kunnen geen andere pakketten worden opgeslagen en zij worden in plaats daarvan gelaten vallen.

Controleer een wachtrij

REP hardware overstroomde laagpakketten via het REP-beheerVLAN zorgen ervoor dat de invoerwachtrij op een L2-poort vastloopt.

```
<#root>
```

```
C9300#
```

```
show interface gil/0/48
```

```
GigabitEthernet1/0/48 is up, line protocol is up (connected)
  Hardware is Gigabit Ethernet, address is 7486.0b0c.e0b0 (bia 7486.0b0c.e0b0)
  Description: PORT
  MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 1000Mb/s, media type is 10/100/1000BaseTX
  input flow-control is on, output flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 01:14:45, output 00:00:00, output hang never
  Last clearing of "show interface" counters never
```

```
Input queue: 2438/2000
```

```
/16/0 (size/max/drops/flushes); Total output drops: 0
```

```
<-- 2438 frames in the input queue who's limit is 2000
```

```
<...snip...>
```

Controleer deze CLI om te bevestigen of een interface buffers met REP HFL frames bevat

- De bestemming MAC voor HFL frames is 0100.0ccc.ccce

```
<#root>
```

```
C9300#
```

```
show
```

```
  buffers input-interface gil/0/48 packet
```

```
Tracekey : 1#09f7811786f1de5ddfa0f5542a69f593
```

```
Buffer information for Middle buffer at 0x7F81FE8E9000
  data_area 0x7F820F78F004, refcount 1, next 0x0, flags 0x210
  linktype 189 (LINK_REP), enctype 3 (SNAP), encsize 22, rxtyp 88
  if_input 0x7F820E71DB50 (GigabitEthernet1/0/48), if_output 0x0 (None)
  inputtime 3d14h (elapsed 03:11:48.761)
  outputtime 00:00:00.000 (elapsed never), oqnumber 65535
  datagramstart 0x7F820F78F072, datagramsize 565, maximum size 804
  mac_start 0x7F820F78F072, addr_start 0x7F820F78F072, info_start 0x7F820F78F080
```

```
network_start 0x7F820F78F088, transport_start 0x0, caller_pc :55FBF3ED3000+37680AC
```

```
7F820F78F072:
```

```
01000CCC CCCE
```

```
A0F8
```

```
...LLN x          <--- HFL destination MAC is in the queue
```

Wachtrij herstellen

- Reboot het apparaat (Een inputrij kan niet zonder een herladen worden ontruimd. Sluiten / geen afsluiten van interface ontruimt deze buffers)
- Upgrade naar een versie van code waarop dit probleem geen invloed heeft
- Pas de grootte van de inputrij aan (in gevallen waar u zeker bent gaan niet meer HSL-frames aankomen u kunt proberen de grootte van de inputrij te verhogen. Onthoud dat het probleem zich waarschijnlijk opnieuw zal manifesteren de volgende keer dat er een overstroming van HSL optreedt).

In deze staat zijn er enkele REP-systemen die voorkomen. Deze logboeken worden in de volgende sectie genoemd



Opmerking: Houd in gedachten dat dit een generiek logbestand is dat wijst op een verlies van LSL tussen burens, wat kan gebeuren om andere redenen. Het is dus nuttig om dit specifieke probleem te identificeren, maar niet beperkt tot dit probleem

REP-logberichten

Logbericht	Definitie	Herstelmaatregelen
%REP-4-LINKSTATUS: TenGigabit Ethernet1/1/1 (segment 1) is niet operationeel vanwege een buur die niet reageert	Duidt op een verlies van LSL tussen burens	<ul style="list-style-type: none">• Bevestig dat interfaces geen vastgelopen invoerwachtrij hebben• Controleer of koppelingen vrij zijn van CRC's en andere incrementele fouten• Controleer of er geen CoPP of

		dalingen in het CPU puntpad zijn
%REP-5-EDGEMISCONFIG: ongeldige topologie. Meer dan twee randpoorten geconfigureerd voor segment	getoond wanneer de ontvangen advertentie van de randhaven niet het zelfde is als uitgestuurde de reclame van de randhaven	<ul style="list-style-type: none"> • Verwacht gedrag wanneer meerdere poorten in een topologie herstellen van een mislukte toestand is dit bericht te zien, maar niet nadat de topologie heeft vastgesteld • elke mislukte poort in rep topologie fungeert als een edge port en stuurt een advertentie

Gerelateerde informatie

- [Layer 2 Configuration Guide, Cisco IOS XE Bengaluru 17.6.x \(Catalyst 9500 Switches\)](#)
- Cisco fout-id [CSCwc52868](#)

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.