Información sobre REP en switches Catalyst 9000

Contenido

Introducción

Este documento describe cómo configurar y validar el Resilient Ethernet Protocol (REP) en los switches Catalyst 9000.

Prerequisites

Requirements

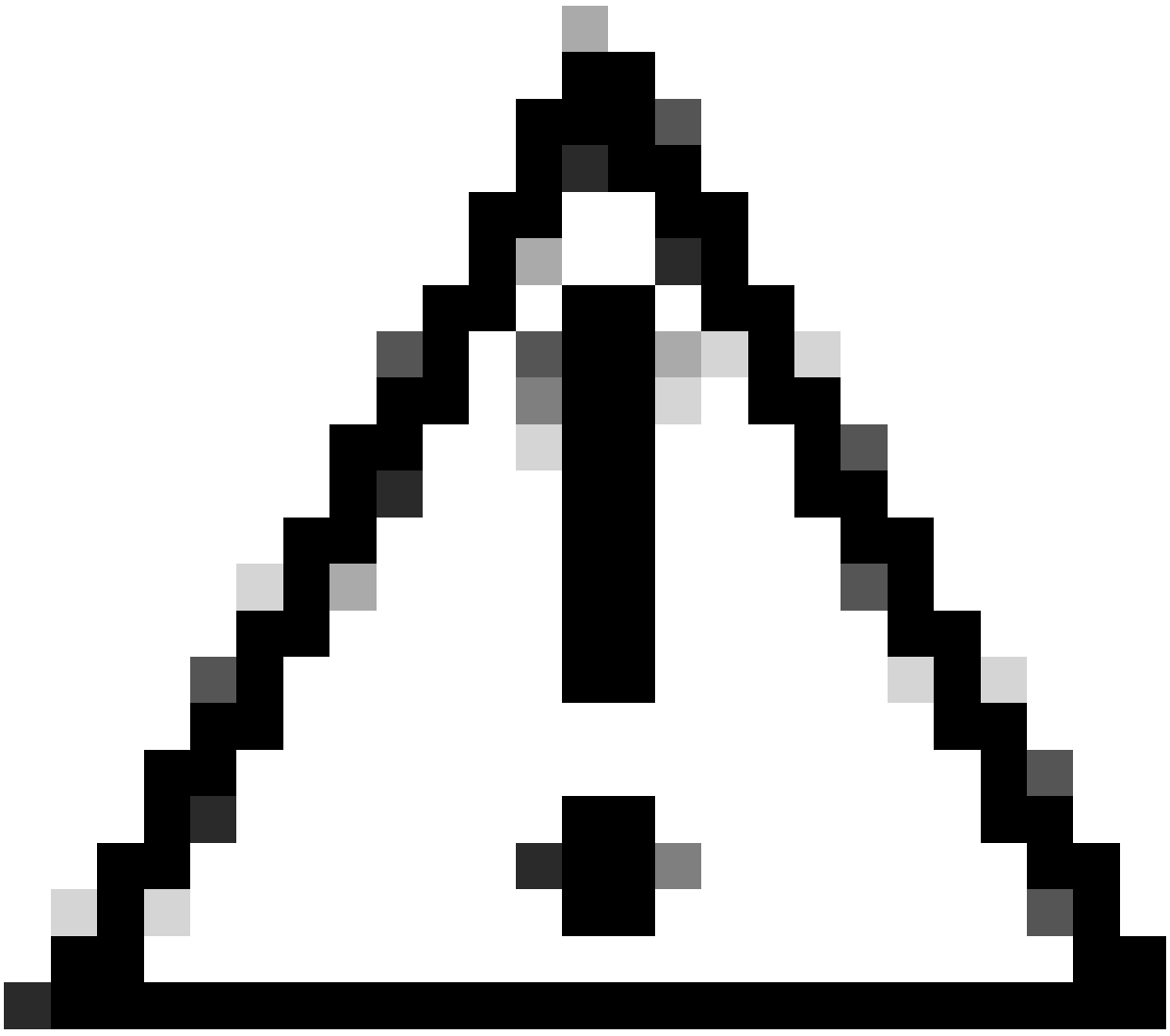
Cisco recomienda tener conocimientos de estos temas:

- Prevención de loop de Capa 2

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Catalyst 9200
- Catalyst 9300
- Catalyst 9400
- Catalyst 9500
- Catalyst 9600
- Cisco IOS XE 17.6.5 y posterior



Precaución: REP no es compatible con switches con Stackwise Virtual (SVL)

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

REP es un protocolo propiedad de Cisco diseñado para evitar bucles de red y proporcionar convergencia rápida en caso de fallo de enlace en redes Ethernet de capa 2. Se trata de una alternativa al protocolo de árbol de extensión y se utiliza a menudo en topologías de capa 2 específicas que requieren extensiones de capa 2 de gran tamaño, como redes de IoT, redes industriales o redes de fabricación. Los "segmentos" de REP se forman encadenando puertos entre switches que se configuran con el mismo ID de segmento. Con funciones como el equilibrio de carga de REP y su capacidad para coexistir con STP, REP se puede utilizar para construir topologías de capa 2 complejas pero predecibles.

Terminology

Término	Definición
Segmento	Cadena de puertos conectados entre sí que comparten el mismo ID de segmento
ID de segmento	Número utilizado para representar el segmento y que se encuentra entre 1 y 1024
Puerto REP	Puerto configurado para ejecutar REP. STP está inhabilitado en los puertos REP.
Puerto de borde	Puerto que termina un borde del segmento REP.
Puerto alternativo	Puerto que bloquea las VLAN en el segmento para evitar loops. Hay 2 puertos alternativos en el segmento si se configura el balanceo de carga
Puerto abierto	Puerto en el segmento que reenvía todas las VLAN
Segmento cerrado	Segmento REP donde ambos puertos de borde están en el mismo switch y tienen conectividad entre sí. También se denomina 'Segmento de timbre'.
Abrir segmento	Segmento REP donde los puertos de borde no tienen conectividad entre sí. Los puertos de borde están en diferentes switches y tienen un puerto de bloqueo entre ellos.
Capa de	Protocolo de enlace de 3 vías responsable del establecimiento de adyacencia de

estado de enlace (LSL)	vecinos y del mantenimiento del estado del link. Las tramas LSL se envían cada 1 segundo en los puertos REP.
Capa de Inundación del Hardware (HFL)	Capa responsable de facilitar la convergencia rápida después de un fallo de enlace inundando las PDU de REP a través de la multidifusión
Anuncio de puerto bloqueado (BPA)	Mensaje enviado por un puerto para anunciar la lista de VLAN que bloquea. Los BPA también pueden transportar cambios de topología, haciendo que los puertos de recepción vacíen su tabla MAC
Anuncio de puerto final (EPA)	Transporta información global sobre el segmento REP y la envían los puertos periféricos
REP Admin VLAN	VLAN utilizada para la inundación de notificaciones rápidas de REP para la convergencia después de la falla del link. El HFL funciona aquí si está configurado. Si no es así, la VLAN de REP Admin es 1.

Teoría del REP

REP puede prevenir loops de switching mediante el bloqueo de VLAN en un solo puerto en el segmento conocido como puerto alternativo. Cuando todos los puertos en el segmento REP están en estado UP, el puerto alternativo se bloquea para evitar el loop. Cuando un link en el segmento REP falla, o si un switch tiene un problema que resulta en la pérdida de link de los paquetes del protocolo REP, el puerto alternativo comienza a reenviar para las VLAN que estaba bloqueando anteriormente. Es importante tener en cuenta que debido a esto, los segmentos REP sólo pueden manejar un único puerto fallido dentro del segmento. Más de 1 fallo de enlace en el segmento REP puede provocar la pérdida de tráfico.

Cuando REP está habilitado en una interfaz, bloquea inmediatamente todas las VLAN. El REP LSL toma el control y comienza a enviar PDU LSL para establecer una adyacencia. La adyacencia se crea usando un protocolo de enlace de 3 vías con los subsiguientes paquetes hello LSL que se envían en intervalos de 1 segundo para mantener los vecinos REP.

Durante la detección de vecinos REP, los dispositivos intercambian su ID de segmento REP y su ID de puerto.

- El ID de segmento es un número entre 1 y 1024 y se configura en la interfaz al habilitar REP. Identifica de forma exclusiva el segmento de REP.
- El ID de puerto es una palabra de 60 bits que se genera automáticamente a partir de la

dirección MAC del sistema y el número de puerto del switch.
- La PDU de LSL se envía a la dirección MAC de destino es 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
```

Un puerto REP pasa a un estado Fallado después de que se apague o el tiempo de espera hello de LSL caduca después de 5 segundos.

REP elección de puerto alternativo

El puerto REP alternativo es el puerto en el segmento que está bloqueando las VLAN.

- La elección del puerto alternativo ocurre inmediatamente después de que se establezcan los vecinos REP mediante un mecanismo de propuesta y acuerdo para determinar qué puerto único del segmento permanece bloqueado.
- Cada puerto del segmento anuncia su clave de puerto y prioridad de puerto y espera el acuerdo.
- El puerto que tiene la prioridad más alta se elige como puerto alternativo.
- El proceso de elección se realiza a través de mensajes REP BPA.

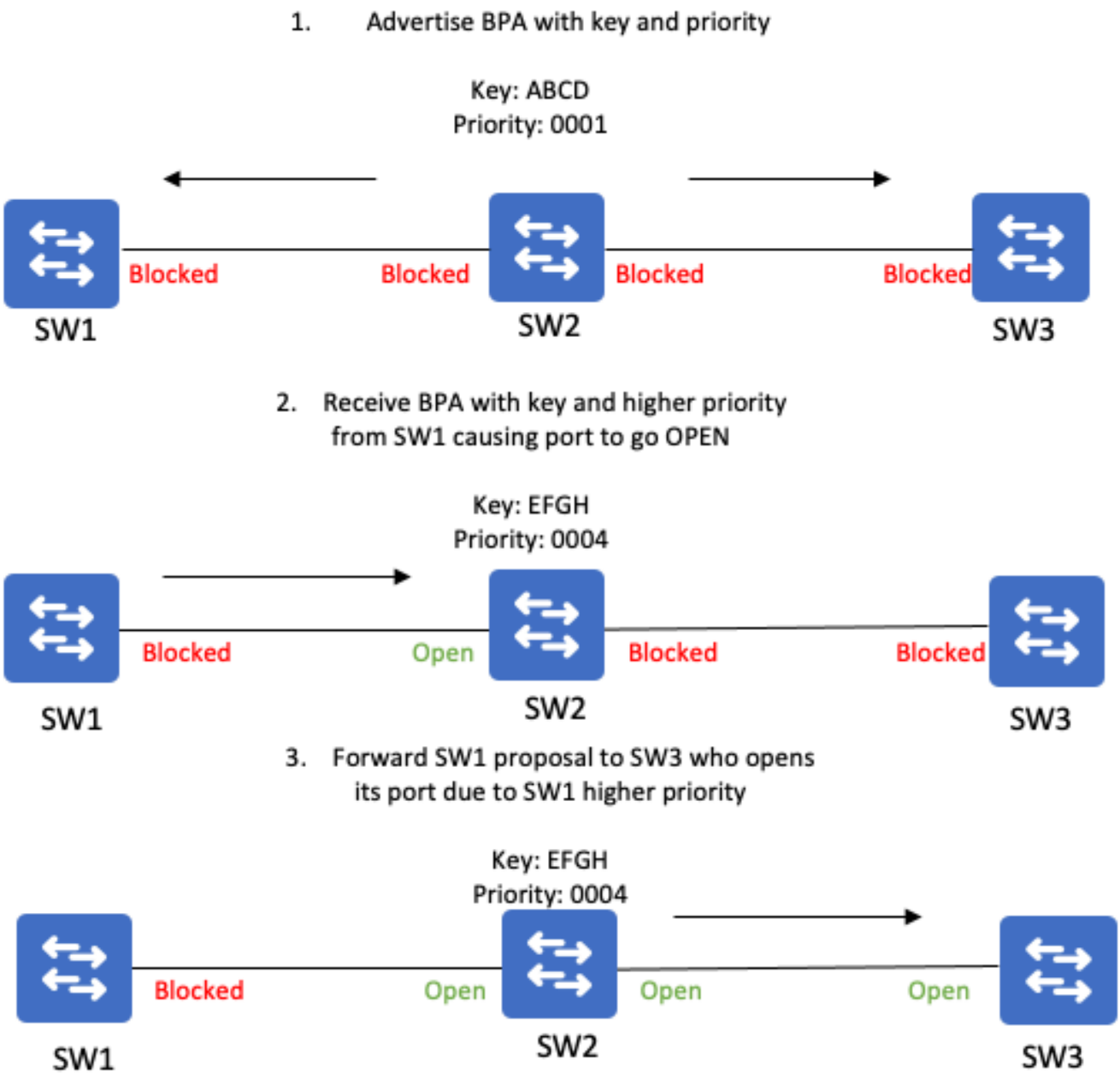
Anuncios de puertos bloqueados

Un mensaje BPA consta de una clave de puerto y una prioridad de puerto.

- La clave de puerto REP es un identificador de 9 bytes que se genera cada vez que el puerto entra en un estado de bloqueo (que está inmediatamente en link activo para los puertos REP habilitados).
- Es una combinación del ID de puerto y un número generado aleatoriamente.
- La prioridad de puerto también es un identificador de 9 bytes.

Elección de puerto alternativo

1. En el link activo y mientras el puerto REP está en estado de bloqueo, anuncia su clave de puerto y prioridad a su vecino REP
2. El puerto receptor compara la prioridad de puerto BPA recibida con su propia prioridad de puerto
3. El puerto receptor responde con un mensaje ACK que contiene la clave que se recibió en el BPA del puerto vecino. Cuando el vecino recibe su propia clave en el BPA sabe que el BPA es un mensaje ACK de su vecino
4. Si el ACK contiene una prioridad de puerto superior a la prioridad de puerto local, el puerto local pasa a un estado OPEN. No responde al vecino con la prioridad más alta, pero reenvía la propuesta fuera de su otro puerto REP a su otro vecino REP
5. El otro vecino REP compara la prioridad del puerto recibido con la suya propia. Si la prioridad recibida es superior a la prioridad local, tampoco responde y envía la propuesta. Si la prioridad local es mayor, responde a la propuesta original con su propia prioridad



Este proceso se repite hasta que el puerto de mayor prioridad permanece en modo de bloqueo. Esto se convierte en el puerto alternativo del segmento. El puerto alternativo continúa enviando mensajes BPA que contienen su clave de puerto al segmento REP. Todos los puertos REP de la caché de segmentos muestran la clave del puerto alternativo.

En un segmento REP estable, todos los puertos están de acuerdo en el puerto alternativo al tener la misma copia de la clave de puerto alternativa. Cada switch que mantiene el ID de clave de puerto del puerto alternativo se vuelve relevante durante los escenarios de falla de link.

Anuncios de puerto final

Los puertos de borde generan mensajes EPA cada 4 segundos. Cada interfaz REP del segmento reenvía estos mensajes y cada puerto agrega su propia información de topología al mensaje.

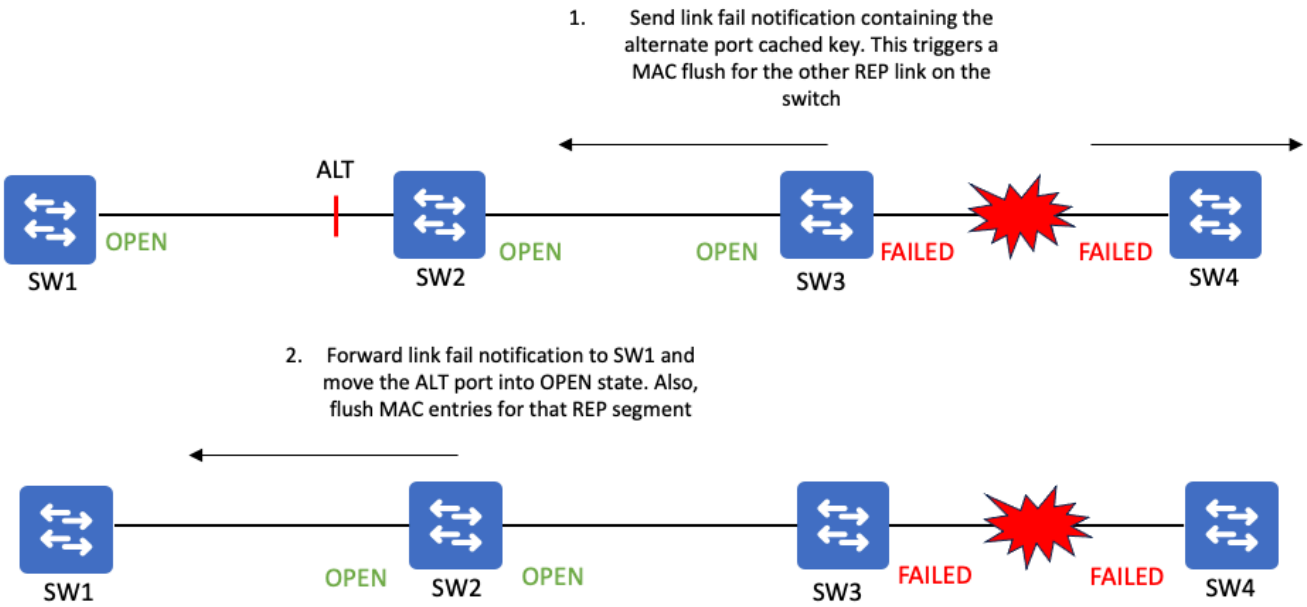
Una vez que el puerto de borde recibe una EPA generada por el otro puerto de borde en el segmento, tiene una topología completa del segmento completo.

Los EPA permiten que cada puerto de borde se vea entre sí y facilita la elección del puerto de borde primario. El puerto de borde con la prioridad más alta se convierte en el puerto de borde primario.

Notificación de fallo de enlace REP

Cuando un link falla en un segmento REP, pasa al estado 'Failed' y comienza a enviar notificaciones de fallas de link que contienen la clave almacenada en caché del puerto alternativo. El switch de envío también vacía las direcciones MAC para su link REP que aún está activo.

El switch vecino REP recibe la notificación de falla de link y la reenvía a cualquier vecino REP en el segmento, así como vacía las entradas de dirección MAC para los puertos en el segmento REP. Si el switch que recibe la notificación de falla de link contiene el puerto alternativo en el segmento, mueve el puerto a un estado OPEN.



Las notificaciones de fallos de enlace se distribuyen de dos maneras:

1. Rep Fast Notifications mediante el envío de mensajes BPA a la dirección de multidifusión de Cisco 0100.0ccc.ccce
2. Notificaciones fiables de REP mediante el envío de mensajes BPA en tramas REP BPDU (similares a tramas REP LSL).

Función	Notificación rápida	Notificación fiable
Hardware reenviado	Yes	No
Fiable	No	Sí, mediante numeración de secuencias y retransmisiones
Pasa a través de un puerto alternativo/de bloqueo	No	Yes
Reenviado fuera del segmento de REP	Yes	No

Enviado a la VLAN de administración de REP	Yes	No (utiliza VLAN nativa)

Las notificaciones de falla de link REP actúan de manera similar a las TCN STP en el sentido de que son impulsadas a la CPU y activan el vaciado de MAC en los puertos REP. Con la configuración adicional en los puertos REP que enfrentan los segmentos STP, una notificación de falla de link REP se puede convertir en una TCN STP para informar al dominio STP que purgue las MAC debido a la falla de link REP.

Equilibrio de carga de VLAN y puerto preferido de REP

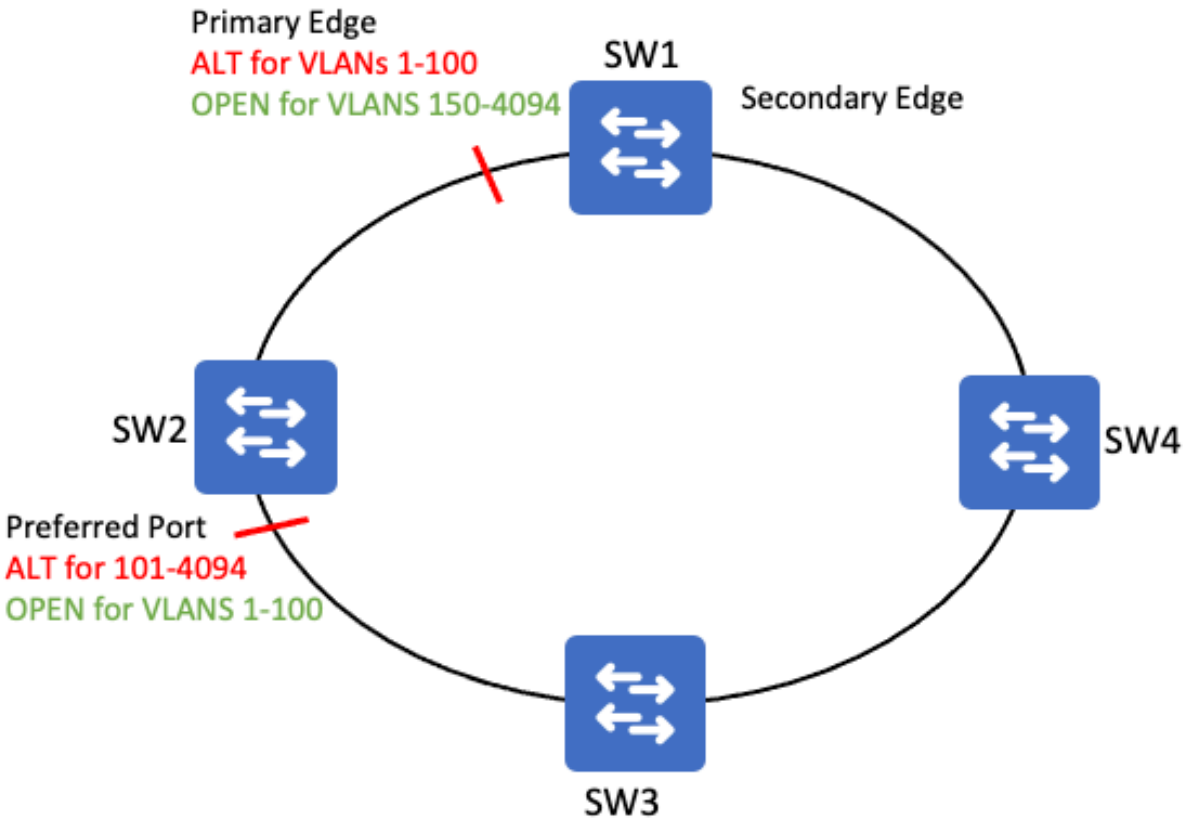
Cuando se configura el balanceo de carga de VLAN, el puerto de borde principal de REP es el puerto que puede iniciar el balanceo de carga. El puerto REP preferido es el puerto que se prefiere para convertirse en el puerto alternativo.

El puerto de borde primario es relevante en el escenario de balanceo de carga porque el balanceo de carga se inicia desde el puerto de borde primario a través de la configuración adicional.

El balanceo de carga se logra al configurar qué VLAN debe bloquear el puerto preferido.

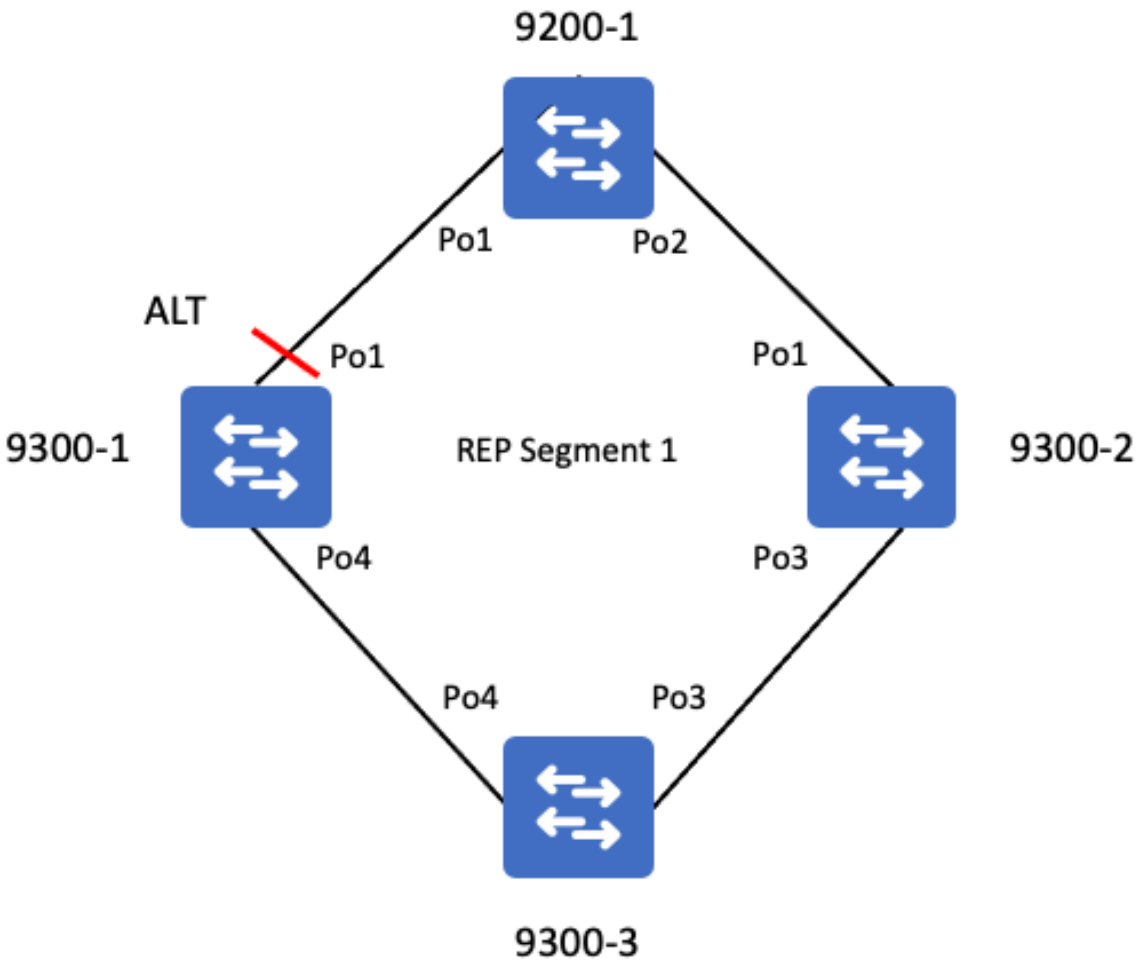
- Las VLAN restantes se bloquean en el puerto de borde primario.
- Hay 2 puertos alternativos cuando el balanceo de carga de VLAN está configurado y activo.

Una vez configurado el balanceo de carga, no tiene efecto hasta que se activa una falla de link o una preferencia manual desde el puerto de borde primario.



Configurar

Diagrama de la red



Configuraciones

Todos los puertos deben configurarse como puertos troncales con un ID de segmento REP coincidente. El switch de borde requiere el parámetro de borde.

<#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
```

Los puertos REP que no son puertos de borde no requieren la palabra clave edge.

<#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
```

Verificación

Una vez que se hayan configurado todos los puertos de segmento, el segmento estará completo y no habrá ningún puerto fallido.

Confirme la topología REP.

<#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
```

Confirmar el estado de REP en una interfaz.

<#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
```

La salida de detalle ofrece una perspectiva más detallada del estado de REP del puerto

<#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
```

Resumen de Comandos

```
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
```

Troubleshoot

Cuña de cola de entrada

En ciertas versiones de código, el paquete REP HSL puede acuñar la cola de entrada de una interfaz.

- Esto puede afectar la convergencia REP si los paquetes HSL llenan la cola de entrada y los paquetes de convergencia LSL no se pueden procesar
- Esto es causado por el ID de bug de Cisco CSCwc52868
- La cola de entrada gestiona el procesamiento de TODOS los protocolos. Una vez que la cola se "llena", elimina el tráfico de control de red legítimo y no se puede vaciar manualmente.

Síntomas de la cuña de cola

- Protocolos como CDP, IGMP, etc. dejan de funcionar (puede perder un vecino en CDP, problemas de programación multidifusión IGMP, etc.).
- Los síntomas varían dependiendo de las características y protocolos que llegan a la interfaz y que necesitan ser procesados.
- La cola de entrada de la interfaz se utiliza para los paquetes que llegan a una interfaz que se ponen en cola y se envían a la CPU para su procesamiento
- Una cola de entrada se atasca cuando un paquete determinado no se puede quitar de la cola y, finalmente, se alcanza el límite de la cola de entrada
- Una vez que se alcanza el límite de la cola de entrada de la interfaz, no se pueden almacenar otros paquetes y se descartan.

Verificar una cuña de cola

El hardware REP inundó los paquetes de capa sobre la VLAN administrativa REP hace que la cola de entrada en un puerto L2 se atasque.

<#root>

```
C9300#

show interface gi1/0/48


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...>
```

Verifique esta CLI para confirmar si una interfaz está conteniendo búferes con tramas REP HFL

- El MAC de destino para las tramas HFL es 0100.0ccc.ccce

<#root>

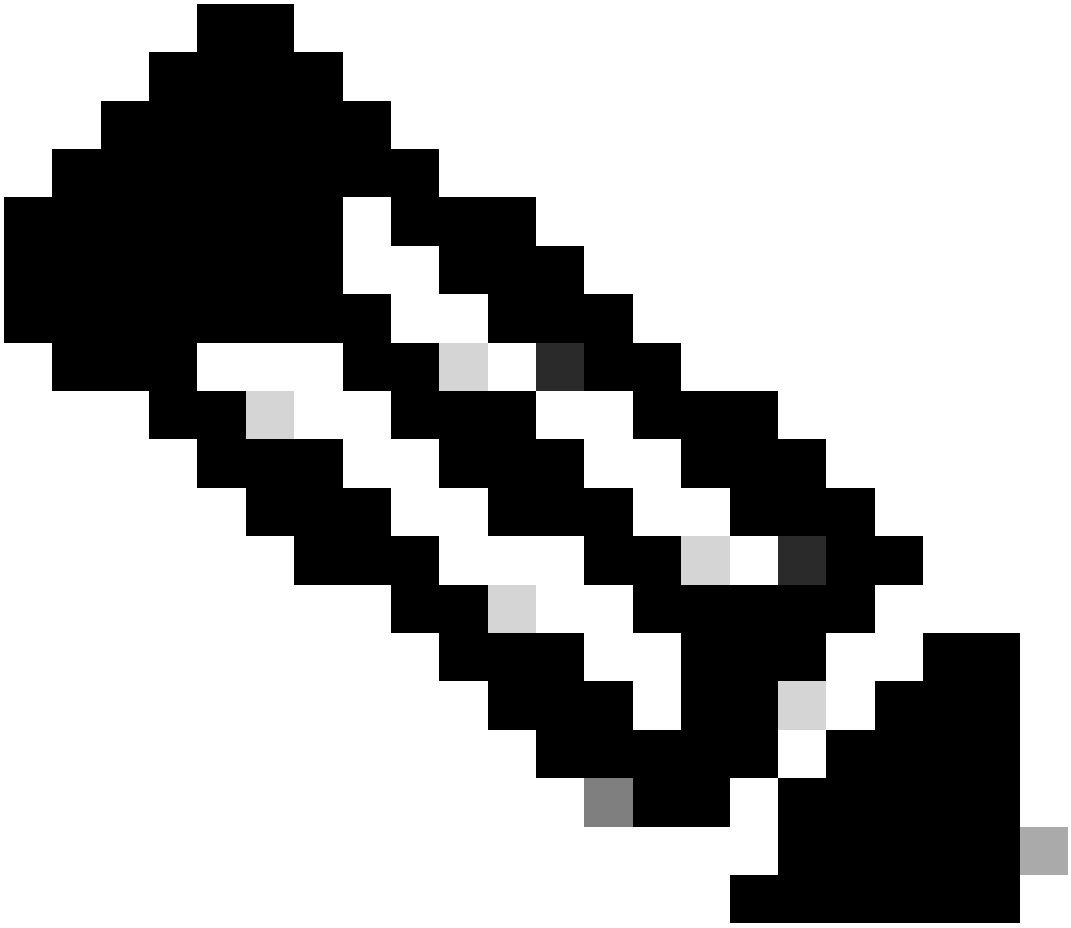
```
C9300#

show

 buffers input-interface gi1/0/48 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, rxtype 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
```

Remediar cuña de cola

- Reinicie el dispositivo (no se puede borrar una cola de entrada sin una recarga). El cierre/no el cierre de la interfaz no borra estas memorias intermedias)
- Actualizar a una versión de código que no se vea afectada por este problema
- Ajustar el tamaño de la cola de entrada (En los casos en los que esté seguro de que no van a llegar más tramas HSL, puede intentar aumentar el tamaño de la cola de entrada. Tenga en cuenta que es probable que el problema se vuelva a manifestar la próxima vez que se produzca una inundación de HSL).

En este estado se producen algunos syslogs de REP. Estos registros se indican en la siguiente sección



Nota: Tenga en cuenta que este es un registro genérico que indica una pérdida de LSL entre vecinos, lo que puede suceder por otras razones. Por lo tanto, es útil identificar este problema específico, pero no se limita a este problema

Mensajes de registro de REP

Mensaje de registro	Definición	Acciones de recuperación
%REP-4-LINKSTATUS: TenGigabitEthernet1/1/1 (segmento 1) no está operativo debido a que el vecino no responde	Indica una pérdida de LSL entre vecinos	• Las interfaces de confirmación no tienen una cola de entrada acuñada • Verificar que los links estén libres de CRCs y otros errores crecientes • Verifique que no haya CoPP o

		caídas en la trayectoria de punt de la CPU
%REP-5-EDGEMISCONFIG: topología no válida. Más de dos puertos de borde configurados para segmento	se muestra cuando el anuncio de puerto de borde recibido no es igual al anuncio de puerto de borde enviado	• El comportamiento esperado cuando varios puertos en una topología se están recuperando del estado fallido permite ver este mensaje, pero no después de que la topología se haya establecido • cada puerto fallido en la topología rep actúa como un puerto de borde y envía un anuncio

Información Relacionada

- Guía de configuración de capa 2, Cisco IOS XE Bengaluru 17.6.x (switches Catalyst 9500)
- ID de bug de Cisco CSCwc52868

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).