Revisión del protocolo Ethernet resistente

Contenido

Introducción

Este documento describe una descripción general del Resilient Ethernet Protocol (REP).

Plataformas Soportadas

- Conmutadores Metro (y) de la Unidad Comercial de Intercambio de Escritorios (), versión 12.2(40) en adelante
- Conmutador Cisco Catalyst Serie 4500, versión 12.2(44) en adelante

- Conmutador Cisco Catalyst Serie 6500 a partir del modelo Whitney2 (12.2SXI)
- Enrutador Cisco Catalyst Serie 7600 a partir del modelo Cobra (12.2SRC)

Antecedentes

¿Por Qué Debe Elegir REP?

REP es un protocolo que sustituye el Protocolo de árbol de expansión (STP) en algunos diseños de red de capa 2. La especificación más actual de es Protocolo de árbol de expansión múltiple (MST), que se define en 802.1Q-2005. Los usuarios que buscan una alternativa al MST tienen las siguientes preocupaciones:

- El STP considera un dominio de puente como un dominio único. En consecuencia, se obtiene una falla local si se cambia el estado de un enlace remoto arbitrario. La aparente impredictibilidad del STP se atenúa solamente si se divide el dominio de puente en fragmentos pequeños e independientes. Desafortunadamente, esto es complejo, si no imposible, de lograr sin la eliminación de algunas características clave del Spanning Tree (como la prevención de loops en todos los escenarios).

- La convergencia de STP puede parecer lenta para los proveedores de servicios que esperan tiempos de recuperación de 50 milisegundos (ms), que son comunes en las tecnologías de switching de circuitos. Esta lentitud no es causada por el protocolo en sí; las plataformas requieren optimización para ejecutar STP de una manera más eficiente. Por lo pronto, se necesitan nuevas soluciones que ayuden a resolver las limitaciones de plataforma.

- La configuración del balanceo de carga del MST no es flexible. Para que el MST alcance un balanceo de carga inmediato, los puentes deben pertenecer a la misma región. Las regiones se definen por la configuración del usuario y no hay manera de modificar la configuración de MST en un switch sin la introducción de alguna reconvergencia en la red. Este problema podría resolverse con una preconfiguración cuidadosa o, en cierto modo, con otros protocolos tales como el Protocolo troncal VLAN (VTP) v3.

Beneficios

A continuación se detallan algunas de las ventajas de usar un REP:

- Con REP, se obtienen los tiempos de convergencia que se expresan a continuación:
  - El modelo tiene un tiempo de convergencia de entre 20 ms y 79 ms.
  - El modelo tiene un tiempo de convergencia de entre 20 ms y 79 ms.
- Funciona en el hardware actual
- Posee puertos predecibles y cerrados.
- Es de fácil configuración.

Limitaciones

A continuación se detallan algunas de las limitaciones de usar un REP:

- No tiene funciones plug-and-play.
- No posee protección de configuración deficiente (se generan lagunas con facilidad).
- Su capacidad de redundancia es limitada (tolera solo un enlace fallido).
- No puede descubrir la topología global (solamente la topología del segmento).
- Es de propiedad exclusiva de Cisco.

Funcionamiento del Protocolo

Segmentos

REP utiliza un segmento como bloque de construcción mínimo de la red. Un segmento es una recopilación de puertos encadenados. Un segmento puede estar formado por solo dos puertos en un puente, y cada puerto del segmento puede tener como máximo un vecino externo. La definición del segmento queda determinada en su totalidad por la configuración de usuario. El segmento se define con dos puertos de borde que también son determinados por el usuario. El protocolo REP donde se ejecutan los segmentos es lo más corto posible y garantiza únicamente las propiedades que se detallan a continuación:

- Si todos los puertos en el segmento están en línea y son funcionales, uno solo puede bloquear el tráfico de cada VLAN.
- Si al menos un puerto en el segmento no es funcional por algún motivo, todos los otros puertos funcionales se redireccionan a todas las VLAN.
- En caso de que el enlace falle, los puertos funcionales restantes se abren tan rápido como sea posible. Del mismo modo, cuando el último puerto fallido vuelve a estar operativo, cuando se elige un puerto bloqueado lógicamente por VLAN, debe causar interrupciones en la red lo menos posible.

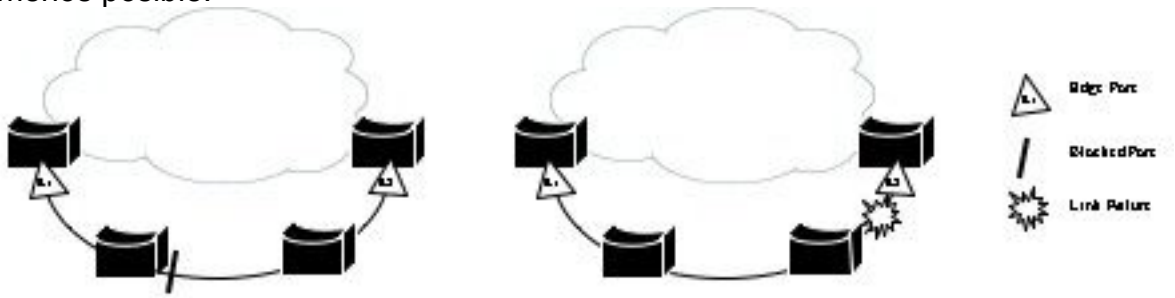

Figura 1.

Segmento como bloque de construcción simple

La Figura 1 muestra un ejemplo de un segmento que incluye seis puertos alocados en cuatro puentes. Los puertos de borde E1 y E2 se representan con un triángulo en el gráfico, y el puerto cerrado se representa con una barra. Cuando todos los puertos son funcionales, según lo representado en el gráfico de la izquierda, se cierra un solo puerto. Cuando hay un error en la red, como se muestra en el gráfico de la derecha, el puerto bloqueado se redirecciona nuevamente.

Cuando el segmento está abierto, según se indica en la Figura 1, no permite la conectividad entre sus dos puertos de borde. Se supone que la conectividad entre los conmutadores de borde REP existe por fuera del segmento (en protocolos STP). Con la configuración funcional, se genera una notificación de cambio de la topología (TCN) si ocurre un error en el segmento REP para acelerar la convergencia.

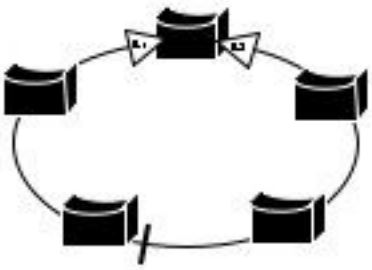

Figura 2 Conversión de segmento en anillo.

Cuando los dos puertos de borde están situados en el mismo conmutador, tal y como se muestra en la Figura 2, el segmento se convierte en un anillo. En este caso, hay conectividad en todo el segmento entre los puertos de borde. De hecho, esta configuración permite que crear una conexión redundante entre dos conmutadores cualesquiera dentro del segmento.

Si se utilizan combinaciones de segmentos abiertos y cerrados, según lo representado en la Figura 1 y la Figura 2, se puede alcanzar una variedad de diseños de red.

Capa de Estado de Enlace

Responsabilidades

- Establezca la conectividad con un vecino único.
- Controle periódicamente la integridad de la conexión con el vecino.
- Envíe y reciba mensajes para las máquinas de estado de la capa superior.
- Reconozca los datos recibidos del vecino.
- Limite los índices de las Unidades de datos de protocolo (PDU).

Estados de Puertos

Cuando se configura un puerto para REP, este experimenta los estados que se describen a continuación:

- Estado fallido (bloqueo)
- Formulación de relación con el puerto vecino:
- Puerto alternativo (bloqueado, igualmente funcional)
- Opción de Punto de acceso (AP) perdida:
- Puerto abierto (si el "AP " fue elegido por otro puerto)

Un puerto no alcanza funcionalidad en las siguientes circunstancias:

- No se ha detectado un puerto vecino
- Se ha detectado más de un puerto vecino
- El vecino no reconoce (ACK) los mensajes

Detalle del Paquete

El envía paquetes de saludo a una dirección MAC de la Unidad de información del protocolo de puente (BPDU) en la VLAN nativa (sin etiqueta) por defecto, de modo que los dispositivos que no tienen esta función los omitan. Cada PDU de capa de estado de link (LSL) incluye un número de secuencia de la PDU que se envía y el número de secuencia remota de la última PDU recibida. Esto asegura que las transmisiones entre los puertos sean confiables. Cada vecino guarda una

copia de cada PDU enviada hasta que se reciba un mensaje ACK. Si no se recibe ningún mensaje ACK, se vuelve a enviar la PDU una vez transcurrido el período de expiración.

Una PDU de LSL real contiene:

- Versióndeprotocolo (actualmente 0)
- IDdesegmento
- IDdepuertoremoto
- IDdepuertolocal
- Númerodeseclocal
- Númerodesecremoto
- TLV de capa superior

Los paquetes LSL se envían en cada intervalo de saludo, o cuando un protocolo de capa más alta lo pide. Cuando se construye la PDU de LSL, primero se propagan los campos propios, como la IDdesegmento y la IDdepuertolocal. Después, se analizan las colas del protocolo de capa más alta, como Anuncios de bloqueo de puertos () o Anuncios de puertos finales (), para comprobar si es necesario poner en cola información adicional.

Capa de Inundación del Hardware (HFL)

La HFL es el módulo de REP que facilita la convergencia rápida cuando los enlaces fallan. No envía PDU a la dirección MAC de BPDU como LSL, sino que envía PDU de multidifusión a una dirección MAC especial (0100.0ccc.ccce) en la VLAN administrativa de REP. Entonces, se inundan desde el hardware todos los conmutadores del segmento.

El formato de los paquetes HFL es simple:

- Versión del protocolo (aún 0)
- IDdesegmento
- Valores de tipo de longitud de capa superior (TLV)

Ahora, los únicos TLV enviados desde la HFL son BPA.

BPA

Los comandos BPA se envían mediante los AP para anunciar las VLAN que se bloquean y su prioridad de puerto. Esto ayuda a notificar al segmento de las fallas de link y garantiza que haya un solo AP por segmento y por VLAN. Esto no es fácil de lograr.

Consideraciones

En una topología estable, las elecciones AP son simples. Un puerto que entra en línea comienza como un AP para todas las VLAN (bloqueo). Cuando recibe un comando BPA de otro puerto con una prioridad más alta, sabe que puede desbloquearse con seguridad. Cuando un puerto en el segmento falla, este mismo proceso se utiliza para desbloquear los otros puertos. Todos los puertos fallidos generan una prioridad de puerto más alta (con un **bit fallido** en la prioridad) que los AP actuales, lo que hace que el AP actual se desbloquee.

Sin embargo, cuando el enlace re restablece puede traer problemas. Cuando esto sucede, el bit fallado en la prioridad se borra, y la prioridad se restablece. Aunque este puerto conoce su nueva prioridad, otras partes del segmento pueden tener información de BPA obsoleta de este puerto.

Este diagrama ilustra este escenario:

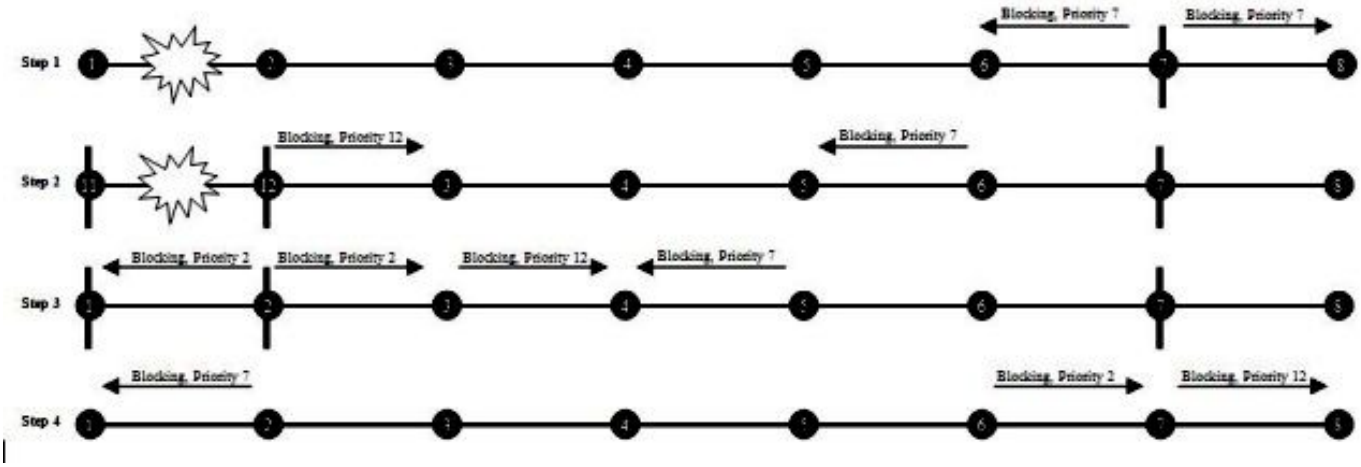

Figura 3. Información obsoleta que abre el segmento

Al principio de este escenario, el puerto 7 está bloqueando y anuncia su prioridad como 7. A continuación, el enlace entre 11 y 12 se rompe, lo que hace que 12 envíe un comando que indique que está bloqueado y que la prioridad es 12. Antes de que estos puertos de bloqueo reciban el BPA del otro puerto, el puerto 12 vuelve a activarse y está operativo. Entonces, el puerto 12 recibe el comando BPA del puerto 7 con prioridad 7, así que se desbloquea. El puerto 7 recibe entonces la información desactualizada del puerto 12 con prioridad 12, así que desbloquea. Esto hace que se genere una laguna. Debido a esta situación de carrera, los comando BPA usan claves.

Comportamiento del BPA

Cada puerto calcula una prioridad de puerto con esta información:

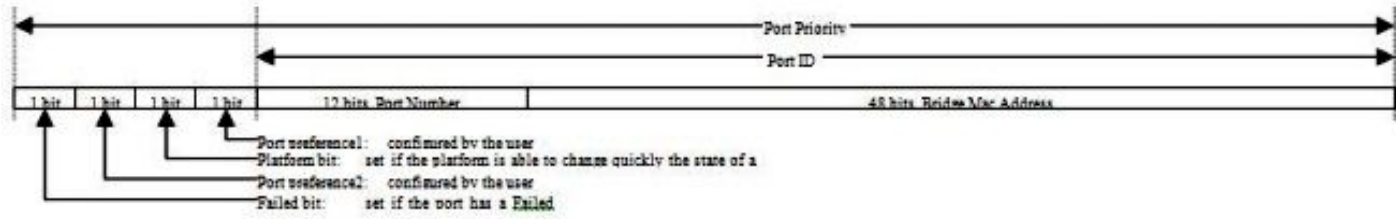

Figura 4 prioridad de puerto

Es evidente ahora por qué los puertos fallidos siempre se eligen como AP en el segmento. Cuando un puerto cambia su estado de Fallido a Alternativo, genera una clave única basada en su ID de puerto y un número aleatorio, y envía esta información junto con su ID de puerto. Un AP se desbloquea únicamente si recibe un mensaje de un puerto bloqueado que incluya su clave local. Este mecanismo ayuda a prevenir la situación de carrera descrita en la sección anterior. Aquí están los diagramas que muestran qué sucede cuando los puertos se conectan y desconectan:

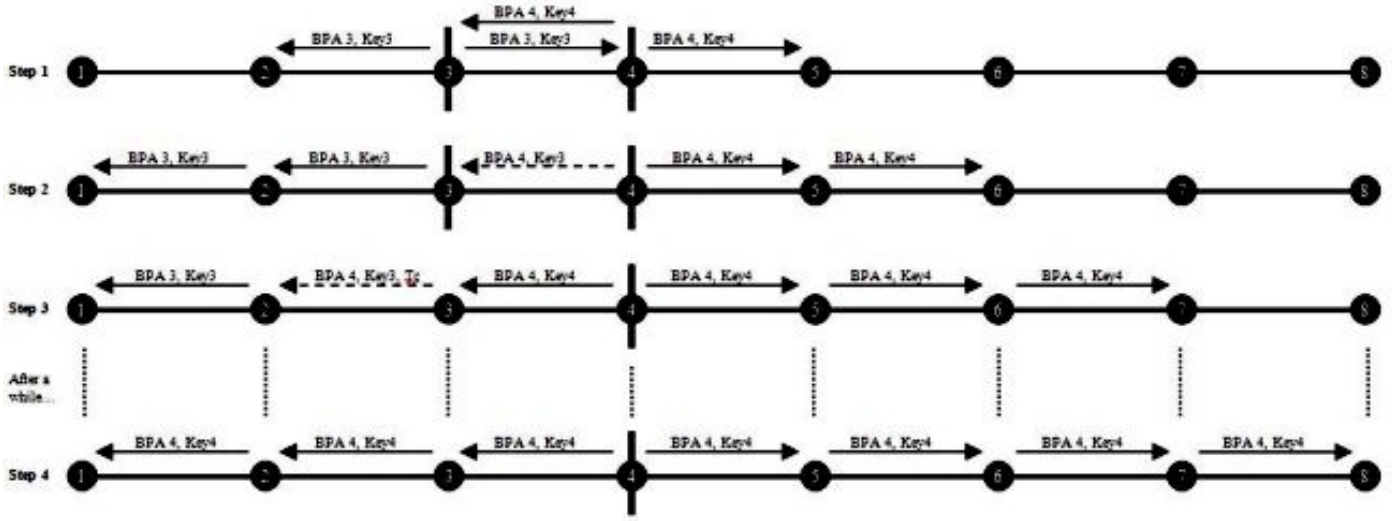

Figura 5. Funcionamiento del durante el enlace.

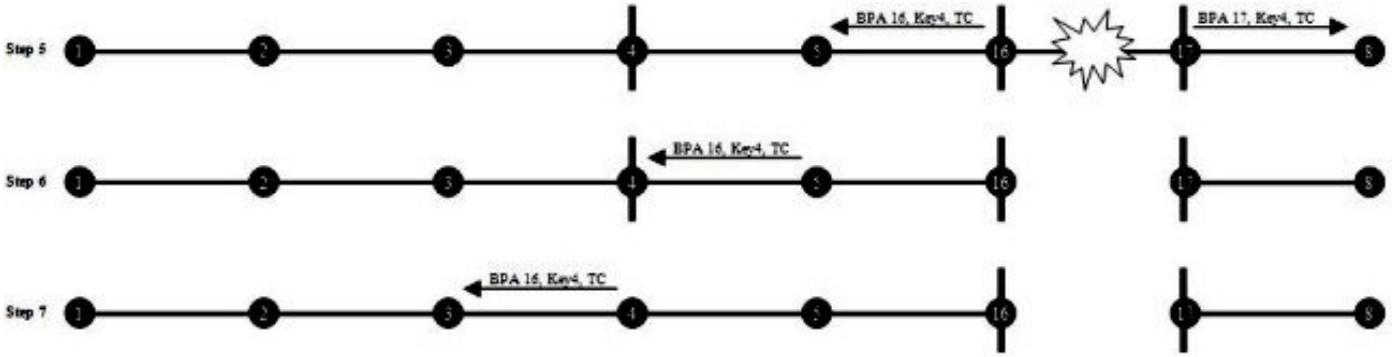

Figura 6. Funcionamiento del BPA después de la falla de enlace.

Asistencia de Hardware

Cuando un enlace falla en un segmento, se envía un comando BPA a los otros puertos del segmento mediante una HFL. Para que esto sea completamente eficaz, la VLAN administrativa se debe llevar a todos los puertos del segmento, y debe ser llevada entre los puertos de borde fuera del segmento. BPA también envía esta información a través de LSL, ya que HFL no puede garantizar un transporte fiable. Si la entrega mediante HFL presenta inconvenientes, el LSL asegura la reconvergencia.

EPA

Un puerto final es un puerto de borde o un puerto fallido. Cuando un segmento está determinado en los ambos lados por un puerto de borde, se considera completo y posibilita el equilibrio de carga VLAN. Cuando un segmento está determinado por un puerto fallado, no se posibilita el equilibrio de carga porque todos los puertos están abiertos.

Los puertos finales envían periódicamente comandos EPA que se retransmiten vía el LSL. Estos mensajes:

- propagan las estadísticas del segmento;
- detectan la condición de segmento completo;
- Iniciar Balanceador de Carga VLAN

Estadísticas del Segmento

Cada puerto final envía un comando EPA periódico que contiene la información sobre sí mediante el LSL. Cada puerto intermedio agrega su propia información y transmite la EPA. Puesto que estos mensajes se mueven en ambas direcciones, cada conmutador REP participante tiene conocimiento del segmento REP entero. La información contenida en el EPA incluye:

- ID de puente
- ID del puerto y estado de ambos puertos REP participantes

Detección de Condición de Segmento Completo

Cada puerto de borde envía un mensaje especial de elección EPA con su propia prioridad de borde y una clave especial (independiente de la clave BPA). El primer puerto en recibir esta información agrega su propia prioridad de puerto al mensaje y la retransmite al conmutador siguiente. Cada switch a lo largo de la trayectoria compara su propia prioridad de puerto con la de la EPA y la reemplaza con la suya propia si la prioridad es mayor. Cuando el puerto de borde recibe un EPA, compara la prioridad de borde con la propia. Si la EPA recibida tiene una prioridad más alta, el puerto de borde envía su siguiente mensaje EPA con la clave al borde primario. Este mecanismo ayuda a:

- asegurar que el segmento esté completo;
- brindar información a ambos puertos de borde sobre el puerto intermedio con la prioridad más alta.

Iniciar Balanceador de Carga VLAN

El balanceo de carga de VLAN se logra con dos AP diferentes que bloquean VLAN diferentes. El borde primario es y es responsable del AP en al menos un subconjunto de las VLAN, y envía un mensaje EPA que indica al puerto de mayor prioridad que bloquee el resto. La información sobre el puerto intermedio con la prioridad más alta fue traída ya con el mensaje de la elección EPA. El tipo de mensaje que se genera para esto es un TLV de comando EPA que contiene un mapa de bits de las VLAN que el puerto con la prioridad más alta necesita que se bloqueen.

Formato de la PDU

Encabezado EPA:

- Tipo=EPA
- N.° de caso
- TLV opcionales

Elección TLV:

- Prioridaddeborde
- Clavedeborde
- Mejorprioridaddepuerto

Comando TLV:

- Prioridaddepuertoseleccionada
- VLANseleccionadas

Información TLV:

- ID de puente
- ID de dos puertos
- Funciones de Puerto

Troubleshoot

Investigación de Enlace Roto

El siguiente es un ejemplo de una topología correcta:

```
SwitchA#show rep topology
REP Segment 1
BridgeName PortName edge Role
---------------- ---------- ---- ----
SwitchA Fa0/2 Pri Alt
SwitchC Fa1/0/23 Open
SwitchC Fa1/0/2 Open
SwitchD Fa0/23 Open
SwitchD Fa0/2 Open
SwitchB Fa1/0/23 Sec Open
```

El siguiente es un ejemplo de topología rota:

```
SwitchA#show rep topology
REP Segment 1
Warning: REP detects a segment failure, topology may be incomplete
BridgeName PortName edge Role
---------------- ---------- ---- ----
SwitchA Fa0/2 Sec Open
SwitchC Fa1/0/23 Open
SwitchC Fa1/0/2 Fail
```

Así se veía:

```
SwitchA#show rep topology archive
REP Segment 1
BridgeName PortName edge Role
---------------- ---------- ---- ----
SwitchA Fa0/2 Pri Open
SwitchC Fa1/0/23 Open
SwitchC Fa1/0/2 Open
SwitchD Fa0/23 Open
SwitchD Fa0/2 Open
SwitchB Fa1/0/23 Sec Alt
```

Ingrese este comando para obtener más detalles sobre el enlace entre SwitchC y SwitchD que falló:

```
SwitchA#show rep topology archive detail
REP Segment 1
<snip>
SwitchC, Fa1/0/2 (Intermediate)
Open Port, all vlans forwarding
Bridge MAC: 0017.5959.c680
Port Number: 004
Port Priority: 010
```

```
Neighbor Number: 3 / [-4]
SwitchD, Fa0/23 (Intermediate)
Open Port, all vlans forwarding
Bridge MAC: 0019.e73c.6f00
Port Number: 019
Port Priority: 000
Neighbor Number: 4 / [-3]
<snip>
```

Así debe verse cuando reconecta el enlace:

```
SwitchA#show rep topology
REP Segment 1
BridgeName PortName edge Role
---------------- ---------- ---- ----
SwitchA Fa0/2 Pri Open
SwitchC Fa1/0/23 Open
SwitchC Fa1/0/2 Alt
SwitchD Fa0/23 Open
SwitchD Fa0/2 Open
SwitchB Fa1/0/23 Sec Open
```

Observe que el puerto que falló anteriormente permanece como el AP y continúa bloqueándose. Esto es porque las elecciones AP suceden solamente entre los puertos bloqueados. Cuando este enlace falló, el resto de los puertos en la topología se abrieron. Cuando el enlace se reconectó, SwitchC y SwitchD enviaron comandos BPA con sus prioridades. SwitchC F1/0/2 tenía una prioridad más alta, así que se convirtió en el AP. Esto permanece hasta que otro puerto en la topología falle, o hasta que se realice un reemplazo.

Puertos Alternativos (ALT)

Un puerto ALT bloquea alguna o todas las VLAN. Si hay una falla en el segmento REP, no hay ningún puerto ALT; todos los puertos están abiertos. Así es como el REP puede proporcionar una ruta activa para el tráfico de datos cuando se produce un error.

En un segmento REP completo (cuando no hay error), puede haber uno o dos puertos. Si se habilita el balanceo de carga VLAN, habrá dos puertos ALT en el segmento (uno de los puertos ALT bloquea un conjunto de VLAN específicas, mientras que el otro, que está siempre en el borde primario, bloquea el conjunto de VLAN complementarias. Si el balanceo de carga VLAN no se habilita, habrá un solo puerto ALT en el segmento, que bloqueará todas las VLAN.

El orden en el que los puertos se conectan y las prioridades de puerto integradas determinan qué puerto del segmento se convierte en un puerto ALT. Si usted desea que un puerto determinado sea el puerto ALT, configúrelo con la palabra clave preferida. Aquí tiene un ejemplo:

```
interface gig3/10
rep segment 3 edge preferred
```

Suponga que gig3/1 es el borde primario, y usted quiere configurar el balanceo de carga del VLAN:

```
interface gig3/1
rep segment 3 edge primary
rep block port preferred vlan 1-150
```

Con esta configuración, después del remplazo, el puerto gig3/10 se convertirá en puerto ALT que bloquea las VLAN 1 a 150, y el puerto gig3/1 se convertirá en un puerto ALT que bloquea las

VLAN 151 a 4094.

El remplazo puede realizarse de forma manual mediante el comando rep preempt segment 3, o de forma automática si configura rep preempt delay <seconds> en el puerto de borde primario.

Cuando un segmento se restablece después de una falla deenlace, uno de los dos puertos adyacentes se convierte en puerto ALT. Entonces, después del remplazo, la ubicación de los puertos se define según lo especificado por la configuración.

Troubleshooting de Adyacencias

Ingrese este comando para comprobar si hay una adyacencia:

```
SwitchC#show interface fa1/0/23 rep
Interface Seg-id Type LinkOp Role
---------------------- ------ -------------- ----------- ----
FastEthernet1/0/23 1 TWO_WAY Open
```

Ingrese este comando para obtener más información:

```
SwitchC#show interface fa1/0/23 rep detail
FastEthernet1/0/23 REP enabled
Segment-id: 1 (Segment)
PortID: 001900175959C680
Preferred flag: No
Operational Link Status: TWO_WAY
Current Key: 000400175959C6808335
Port Role: Open
Blocked VLAN: <empty>
Admin-vlan: 1
Preempt Delay Timer: disabled
Configured Load-balancing Block Port: none
Configured Load-balancing Block VLAN: none
STCN Propagate to: none
LSL PDU rx: 255547, tx: 184557
HFL PDU rx: 3, tx: 2
BPA TLV rx: 176096, tx: 2649
BPA (STCN, LSL) TLV rx: 0, tx: 0
BPA (STCN, HFL) TLV rx: 0, tx: 0
EPA-ELECTION TLV rx: 870, tx: 109
EPA-COMMAND TLV rx: 2, tx: 2
EPA-INFO TLV rx: 45732, tx: 45733
```

Depuraciones

La de las depuraciones imprimen demasiada información, que resulta de poca utilidad. A continuación se detalla la lista completa (algunos están disponibles solo con servicio interno):

```
SwitchB#debug rep ?
all all debug options
bpa-event bpa events
bpasm BPA state machine
database protocol database
epasm EPA state machine
error protocol errors
failure-recovery switchover events
lslsm LSL state machine
```

```
misc miscellaneous
packet protocol PDU
prsm Port Role state machine
showcli show debug info
```

Depuraciones útiles

Estas son algunas de las depuraciones útiles:

- **debug rep showcli** (necesita servicio interno) - Esta depuración imprime mucha información adicional cuando ingresa los comandos regulares **show rep**.
- **debug rep error** - Esta depuración tiene el potencial de ser muy útil.
- **debug rep failure-recovery** - Este debug imprime los mensajes que pasan cuando se rompe un link.

```
*Mar  5 05:01:11.530: REP LSL-OP Rx EXT Local (Fa0/23 seg:1, tc:1, frs:0) prio:
*Mar 5 05:01:11.530: 0x80 0x00 0x19 0x00 0x17 0x59 0x59 0xC6
*Mar 5 05:01:11.530: 0x80
*Mar 5 05:01:11.530: REP Flush from Fa0/23 to REP, sending msg
*Mar 5 05:01:11.530: REP LSL-OP Rx INT Local (Fa0/2 seg:1, tc:1, frs:0) prio:
*Mar 5 05:01:11.530: 0x80 0x00 0x19 0x00 0x17 0x59 0x59 0xC6
*Mar 5 05:01:11.530: 0x80
*Mar 5 05:01:11.530: REP Flush from Fa0/2 to REP, sending msg
```

- **debug rep prsm** - Esta depuración es buena para resolver problemas de adyacencias que no se forman. Le informa en detalle qué sucede cuando un enlace se conecta o desconecta.

```
4d05h: %LINK-3-UPDOWN: Interface FastEthernet0/2, changed state to up
4d05h: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2,
changed state to up
*Mar 5 05:06:19.098: rep_pr Fa0/2 - pr: during state FAILED_PORT,
got event 5(no_ext_neighbor)
*Mar 5 05:06:19.098: @@@ rep_pr Fa0/2 - pr: FAILED_PORT ->
FAILED_PORT_NO_EXT_NEIGHBOR[Fa0/2]rep_pr_act_no_ext_neighbor@272:
PRSM->fp_no_ext_neighbor state
[Fa0/2]rep_pr_lsl_event_handler@448: REP_MSG_EXT_PEER_GONE rcvd

4d05h: %REP-4-LINKSTATUS: FastEthernet0/2 (segment 1) is operational
*Mar 5 05:06:22.236: rep_pr Fa0/2 - pr: during state FAILED_PORT_NO_EXT_
NEIGHBOR, got event 0(link_op)
*Mar 5 05:06:22.236: @@@ rep_pr Fa0/2 - pr:
FAILED_PORT_NO_EXT_NEIGHBOR ->
ALTERNATE_PORT[Fa0/2]rep_pr_act_ap@162: PRSM->alternate state
[Fa0/2]rep_pr_lsl_event_handler@431: REP_MSG_LINKOP_TRUE rcvd

*Mar  5 05:06:23.125:     rep_pr Fa0/2 - pr: during state ALTERNATE_PORT,
got event 2(pre_empt_ind)
*Mar 5 05:06:23.133: @@@ rep_pr Fa0/2 - pr: ALTERNATE_PORT -> UNBLOCK_VLANS_ACT
*Mar 5 05:06:23.133: rep_pr Fa0/2 - pr: during state UNBLOCK_VLANS_ACT,
got event 3(no_local_block_vlan)
*Mar 5 05:06:23.133: @@@ rep_pr Fa0/2 - pr: UNBLOCK_VLANS_ACT ->
OPEN_PORT[Fa0/2]rep_pr_act_op@252: PRSM->active state
[Fa0/2]rep_pr_act_uva@222: PRSM unblock vlans
[Fa0/2]rep_pr_sm_prempt_ind@374: Posting pre empt indication
```

- **debug rep epasm** - Este debug proporciona información útil durante los cambios de topología. Si el segmento está estable, no se imprime información.

A continuación se muestra la información que se imprime si un puerto se desconecta:

```
*Mar  5 04:48:31.463:     rep_epa_non_edge Fa0/2 - epa-non-edge: during state
INTERMEDIATE_PORT, got event 1(lr_eq_fp)*Mar 5 04:48:31.463: @@@ rep_epa_non_
edge Fa0/2 - epa-non-edge: INTERMEDIATE_PORT -> FAILED_PORT[Fa0/2]rep_epa_non_
edge_act_failed_port@164: Trigger archiving
[Fa0/23]rep_epa_set_peer_archive_flag@1084: set arch flag
[Fa0/2]rep_epa_non_edge_act_failed_port@171: no edge, failed port
*Mar 5 04:48:35.473: rep_epa_non_edge Fa0/2 - epa-non-edge: during state
FAILED_PORT, got event 0(epa_hello_tmo)
*Mar 5 04:48:35.473: @@@ rep_epa_non_edge Fa0/2 - epa-non-edge: FAILED_PORT ->
FAILED_PORT[Fa0/2]rep_epa_non_edge_act_periodic_tx@90: archiving on port down
[Fa0/2]rep_epa_copy_topology@913: deip=0x3396F18,pe=0,se=1,fp=0,ap=0,op=2
[Fa0/23]rep_epa_non_edge_handle_info_tlv@1560: archiving on internal flag
[Fa0/23]rep_epa_copy_topology@913: deip=0x33961F0,pe=1,se=0,fp=0,ap=1,op=3
[Fa0/2]rep_epa_non_edge_act_periodic_tx@102: epa non edge, send info tlv
[Fa0/23]rep_epa_set_peer_archive_flag@1084: set arch flag
[Fa0/2]rep_epa_non_edge_handle_election_tlv@325: archiving on seg cfg change
[Fa0/2]rep_epa_copy_topology@913: deip=0x3396F18,pe=0,se=1,fp=0,ap=0,op=2
[Fa0/2]rep_epa_set_peer_archive_flag@1084: set arch flag
[Fa0/23]rep_epa_non_edge_handle_election_tlv@325: archiving on seg cfg change
[Fa0/23]rep_epa_copy_topology@913: deip=0x33961F0,pe=1,se=0,fp=0,ap=1,op=3
[Fa0/2]rep_epa_non_edge_handle_info_tlv@1560: archiving on internal flag
[Fa0/2]rep_epa_copy_topology@913: deip=0x3396F18,pe=0,se=1,fp=0,ap=0,op=2
```

Este es el resultado cuando un puerto se conecta:

```
*Mar  5 04:49:39.982:     rep_epa_non_edge Fa0/2 - epa-non-edge: during state FAILED_PORT,
got event 2(lr_neq_fp)
*Mar 5 04:49:39.982: @@@ rep_epa_non_edge Fa0/2 - epa-non-edge: FAILED_PORT ->
INTERMEDIATE_PORT[Fa0/2]rep_epa_non_edge_stop_timer@123: epa non edge, stop the timer
[Fa0/2]rep_epa_copy_topology@913: deip=0x32E2FA4,pe=0,se=1,fp=0,ap=1,op=1
[Fa0/2]rep_epa_copy_to_stable_topology@1040: copy to stbl
[Fa0/23]rep_epa_copy_topology@913: deip=0x3ACFFB8,pe=1,se=0,fp=0,ap=0,op=4
[Fa0/23]rep_epa_copy_to_stable_topology@1040: copy to stbl
```

Depuraciones menos útiles

- **debug rep bpa-event** - Este debug le indica cuándo recibe un BPA y qué hace con él. Tiene cuatro líneas por segundo.

```
[Fa0/23]: BPA: Sending ext pak to bparx
[Fa0/2]: BPA: Enqueued internal pak
[Fa0/2]: BPA: Sending int msg to bparx
[Fa0/2]: BPA: Relay pak
[Fa0/2]: BPA: Enqueue ext pak
```

- **debug rep bpasm** - Esta depuración le indica qué hace la máquina de estado BPA cada vez que se recibe un BPA. Tiene tres líneas por segundo.

```
*Mar  5 04:44:23.857:     rep_bpa_rx BPA RX sm: during state BPA_RX_IDLE,
got event 0(bpa_rx_bpa_msg)
*Mar 5 04:44:23.857: @@@ rep_bpa_rx BPA RX sm: BPA_RX_IDLE -> BPA_RX_IDLE
[Fa0/23]: BPA Rx sm: Received bpa: <internal> 0, <vlan_detail> 0
[Fa0/23]: BPA Rx sm: Role 2: TC 0; Internal 0; Frm Remote Segment 0

*Mar  5 04:44:23.857:     rep_bpa_rx BPA RX sm: during state BPA_RX_IDLE,
got event 0 (bpa_rx_bpa_msg)
*Mar 5 04:44:23.857: @@@ rep_bpa_rx BPA RX sm: BPA_RX_IDLE -> BPA_RX_IDLE
[Fa0/2]: BPA Rx sm: Received bpa: <internal> 1, <vlan_detail> 0
[Fa0/2]: BPA Rx sm: Role 2: TC 0; Internal 1; Frm Remote Segment 0
```

- **debug rep lslsm -** Este debug vuelca el procesamiento de mensajes LSL de bajo nivel.

```
*Mar  5 05:03:10.564: REP Fa0/23 seq:4411 ACK'ed (ref: 1)
*Mar 5 05:03:10.564: REP Fa0/23 seq:4412 ACK'ed (ref: 1)
*Mar 5 05:03:10.564: REP LSL: Fa0/23 rx expected seq# (4744),
process it (TLV: 0).
*Mar 5 05:03:10.782: REP Fa0/2 seq:440 ACK'ed (ref: 1)
```

Información Relacionada

- Asistencia técnica y descargas de Cisco

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).