

Examen du protocole Ethernet résilient

Table des matières

[Introduction](#)

[Plates-formes prises en charge](#)

[Informations générales](#)

[Pourquoi le protocole Ethernet résilient \(Resilient Ethernet Protocol, REP\)?](#)

[Avantages](#)

[Limites](#)

[Opération de protocole](#)

[Segments](#)

[Couche d'état de lien](#)

[Responsabilités](#)

[États du port](#)

[Détails des paquets](#)

[Couche d'inondation de matériel \(Hardware Flood Layer, HFL\)](#)

[BPA](#)

[Considérations](#)

[Comportement des BPA](#)

[Assistance matérielle](#)

[EPA](#)

[Statistiques de segment](#)

[Détection de l'état complet de segment](#)

[Amorçage de l'équilibrage de charge VLAN](#)

[Format PDU](#)

[Dépannage](#)

[Enquête sur un lien rompu](#)

[Autres ports \(ALT\)](#)

[Dépannage des contiguïtés du REP](#)

[Débogages](#)

[Débogages utiles](#)

[Débogages moins utiles](#)

[Informations connexes](#)

Introduction

Ce document décrit une présentation du protocole REP (Resilient Ethernet Protocol).

Plates-formes prises en charge

- Commutateurs de série Metro (3750ME et ME3400) de l'unité commerciale des commutateurs de bureau (DSBU), version 12.2(40)SE et ultérieures
- Commutateur Cisco de gamme Catalyst 4500, version 12.2(44)SG et ultérieures

- Commutateur Cisco de gamme Catalyst 6500 démarrant dans le logiciel Whitney2 (12.2SXI)
- Routeur Cisco de gamme Catalyst 7600 démarrant dans l'outil Cobra (12.2SRC)

Informations générales

Pourquoi le protocole Ethernet résilient (Resilient Ethernet Protocol, REP)?

Le protocole Ethernet résilient (REP) vient remplacer le protocole Spanning Tree (STP) dans certaines conceptions de réseaux de couche 2 en particulier. La spécification STP la plus récente porte le nom Multiples Spanning Trees (MST) et est définie dans 802.1Q-2005. Les utilisateurs qui veulent une solution de rechange à MST ont ces préoccupations légitimes :

- STP considère un domaine relié par un pont comme unité. En conséquence, une panne locale est réparée si vous changez l'état d'un lien arbitrairement distant. L'imprévisibilité apparente du protocole STP est seulement atténuée si vous segmentez le domaine lié par un pont en petites segments indépendants. Malheureusement, cela est complexe, voire impossible, à réaliser sans la suppression de certaines fonctions clés du Spanning Tree (comme la prévention des boucles dans tous les scénarios).
- La convergence STP peut sembler lente pour les fournisseurs de services qui attendent des temps de récupération de 50 millisecondes (ms), ce qui est courant dans les technologies de commutation de circuits. Cette lenteur n'est pas due au protocole lui-même ; les plates-formes nécessitent une optimisation pour exécuter le protocole STP de manière plus efficace. En attendant, il faut de nouvelles solutions qui permettent de contourner les limites des plateformes.
- La configuration d'équilibrage de charge MST n'est pas flexible. Pour que la configuration MST effectue l'équilibrage de charge des instances, tous les ponts doivent faire partie de la même région. Les régions sont définies par la configuration utilisateur et il n'est pas possible de modifier la configuration MST sur un commutateur sans introduire une certaine reconvergence dans le réseau. Ce problème est contournable au moyen d'une préconfiguration attentive et, de façon limitée, par l'utilisation d'autres protocoles tels que le protocole VTP (VLAN Trunk Protocol) v3.

Avantages

Voici certains des avantages du protocole REP :

- Le protocole REP offre les temps de convergence suivants :
 - 3750ME converge entre 20 ms et 79 ms.
 - ME3400 converge entre 40 ms et 70 ms.
- Fonctionne avec le matériel actuel
- Ports prévisibles et bloqués
- Configuration simple

Limites

Voici certaines des limites du protocole REP :

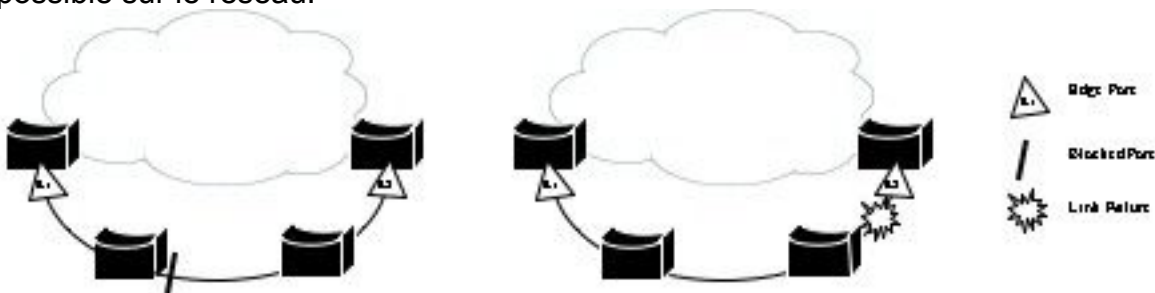
- N'est pas prêt à l'emploi
- N'offre aucune protection contre la configuration incorrecte (susceptible à la création de boucles)
- Offre une redondance limitée (seulement capable de résister à une panne de lien)
- Ne peut pas découvrir la topologie globale (se limite à la topologie de segment)
- Appartient à Cisco

Opération de protocole

Segments

Le protocole REP utilise un segment comme module minimal de réseau. Un segment est simplement une collection de ports liés entre eux. Seulement deux ports peuvent appartenir à un segment donné sur un pont, et chaque port de segment peut comporter un maximum d'un voisin extérieur. La définition du segment est entièrement réalisée par configuration utilisateur. Le segment se termine par deux **ports de périphérie qui sont également déterminés par l'utilisateur**. Le protocole REP qui s'exécute sur des segments est aussi minimal que possible et garantit seulement les propriétés suivantes :

- Si tous les ports du segment sont en ligne et fonctionnels, un seul d'entre eux bloque logiquement le trafic pour chaque réseau local virtuel (VLAN).
- Si au moins un port du segment n'est pas fonctionnel pour une raison quelconque, tous les autres ports fonctionnels procèdent à un transfert pour tous les VLAN.
- En cas de panne de lien, le déblocage de tous les ports fonctionnels restants s'effectue aussi vite que possible. De même, lorsque le dernier port défaillant redevient opérationnel, lorsqu'un port bloqué logiquement par VLAN est sélectionné, il doit provoquer le moins de perturbations possible sur le réseau.



segment comme module simple

Figure 1. Un

La figure 1 affiche un exemple d'un segment qui comprend six ports répartis sur quatre ponts. Les ports de périphérie configurés E1 et E2 sont représentés par des triangles dans le diagramme, et le port logiquement bloqué est représenté par une barre. Quand tous les ports sont fonctionnels, comme démontré à gauche, un port unique est bloqué. Quand il y a une panne dans le réseau, comme démontré du côté droit du diagramme, le port logiquement bloqué retourne à un état de transfert.

Quand le segment est ouvert, comme représenté dans la figure 1, il n'offre aucune connectivité entre ses deux ports de périphérie. On présume que la connectivité entre les commutateurs de périphérie du REP se fait à l'extérieur du segment (par STP). La configuration facultative entraîne une notification de changement de topologie STP (TCN) si une panne se produit dans le segment

REP, afin d'accélérer la convergence.

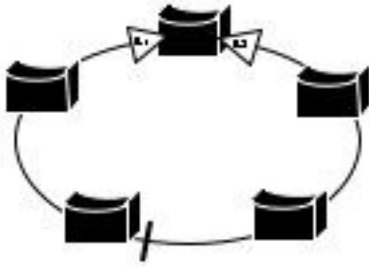


Figure 2. Un segment peut former une boucle.

Quand les deux ports de périphérie se trouvent sur le même commutateur, comme démontré dans la figure 2, le segment forme une boucle. Dans ce cas, il y a une connectivité entre les ports de périphérie par l'intermédiaire du segment. En effet, cette configuration permet de créer une connexion redondante entre n'importe quelle paire de commutateurs dans le segment.

Si vous utilisez des combinaisons de segments ouverts et fermés, comme représenté dans la figure 1 et la figure 2, vous pouvez réaliser diverses conceptions de réseaux.

Couche d'état de lien

Responsabilités

- Établissez une connectivité avec un voisin unique.
- Vérifiez périodiquement l'intégrité de la connexion avec le voisin.
- Envoyez et recevez des messages pour des ordinateurs de couche supérieure.
- Reconnaissez les données reçues de la part du voisin.
- Taux limitatifs des unités de données du protocole (PDU).

États du port

Quand un port est configuré pour le REP, il passe par les états suivants :

- État défaillant (blocage)
- Relation de voisinage formée :
- Port de remplacement (en état de blocage, mais fonctionnel)
- Choix de point d'accès (AP) perdu :
- Port ouvert (si un autre port a choisi le « AP »)

Un port n'est pas fonctionnel dans les conditions suivantes :

- Aucun voisin n'est détecté sur le port.
- Plus d'un voisin est détecté sur le port.
- Le voisin ne reconnaît pas (ACK) les messages.

Détails des paquets

Par défaut, le REP envoie des paquets d'accueil à une adresse MAC de classe Bridge Protocol Data Unit (BPDU) sur le VLAN natif (non-marqué), de sorte que les appareils n'exécutant pas la fonctionnalité les ignorent. Chaque unité de données de protocole LSL (Link Status Layer) inclut à la fois le numéro de séquence de l'unité de données de protocole envoyée et le numéro de

séquence distant de la dernière unité de données de protocole reçue. Ceci assure une transmission fiable entre les ports. Chaque voisin conserve une copie de chaque PDU envoyé jusqu'à ce qu'une reconnaissance (ACK) soit reçue. Si aucun ACK n'est reçu, le PDU est renvoyé de nouveau après l'expiration du chronomètre.

Le PDU LSL lui-même comprend les propriétés suivantes :

- ProtocolVersion (actuellement 0)
- SegmentID
- RemotePortID
- LocalPortID
- LocalSeqNumber
- RemoteSeqNumber
- TLV de couche supérieure

Des paquets LSL sont envoyés à chaque intervalle d'accueil ou quand un protocole de couche supérieure le demande. Quand le PDU en langage LSL est établi, il remplit d'abord ses propres champs, comme SegmentID et LocalPortID. Ensuite, il examine les files d'attente de protocoles de couche supérieure, comme le protocole Block Port Advertisement (BPA) ou encore End Port Advertisement (EPA), afin de voir si des données supplémentaires doivent être mises en file d'attente.

Couche d'inondation de matériel (Hardware Flood Layer, HFL)

Le HFL est le module du REP qui facilite la convergence rapide après des pannes de lien. Il n'envoie pas de PDU à l'adresse MAC BPDU comme LSL, mais envoie plutôt des PDU de multidiffusion à une adresse MAC spéciale (0100.0ccc.cccc) sur le VLAN d'administration REP. De cette façon, il inonde le matériel et rejoint tous les commutateurs dans le segment.

Le format de paquet HFL est simple :

- Version de protocole (encore 0)
- SegmentID
- Éléments Type-Longueur-Valeur (TLV) de couche supérieure

À ce moment, les seuls TLV envoyés par HFL sont des BPA.

BPA

Des BPA sont envoyés par AP afin d'annoncer les VLAN qu'ils bloquent, ainsi que leur priorité de port. Cela permet de notifier le segment des défaillances de liaison et garantit qu'il n'y a qu'un seul point d'accès par segment par VLAN. Un tel état est difficile à atteindre.

Considérations

Dans une topologie stable, les choix d'AP sont simples. Un port qui se connecte au réseau commence par servir d'AP pour tous les VLAN (blocage). Quand il reçoit un BPA d'un autre port avec une plus haute priorité, il peut procéder au déblocage en toute sécurité. Quand un port sur le segment échoue, ce même processus est utilisé afin de débloquent les autres ports. Tous les ports défaillants génèrent une priorité de port plus élevée (avec un **bit défaillant** dans la priorité) que les AP actuels, ce qui entraîne le déblocage de l'AP actuel.

Les problèmes se produisent, cependant, quand ce lien se réactive. Le cas échéant, le **bit défectueux sur la priorité s'efface, et la priorité retourne à l'état normal**. Bien que ce port connaisse sa nouvelle priorité, d'autres parties du segment peuvent avoir des informations BPA périmées de ce port. Le diagramme suivant présente ce scénario :

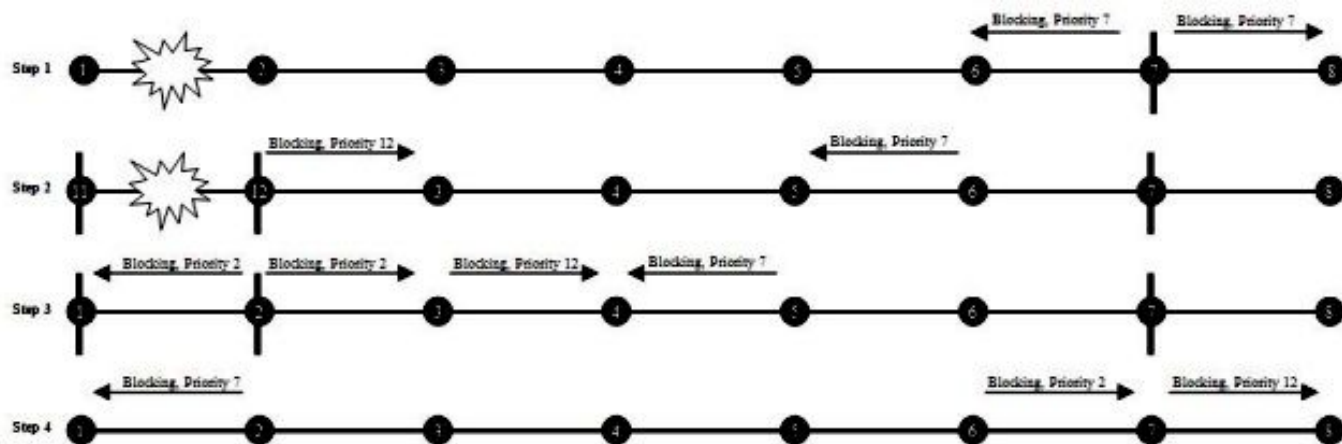


Figure 3. Informations périmées qui ouvrent le segment

Au début de ce scénario, le port 7 bloque et annonce sa priorité comme étant 7. Ensuite, le lien entre 11 et 12 se rompt, ce qui amène 12 à envoyer un BPA indiquant qu'il bloque avec une priorité de 12. Avant que ces ports bloquants ne reçoivent le BPA de l'autre port, le port 12 revient et est opérationnel. Peu après, le port 12 reçoit le BPA du port 7 avec la priorité 7, pour qu'il se débloque. Le port 7 obtient ensuite le BPA périmé du port 12 avec la priorité 12, pour qu'il se débloque. Ceci entraîne une boucle. Un tel contexte de compétitivité explique pourquoi le BPA utilise des **clés**.

Comportement des BPA

Chaque port calcule une priorité de port avec ces informations :

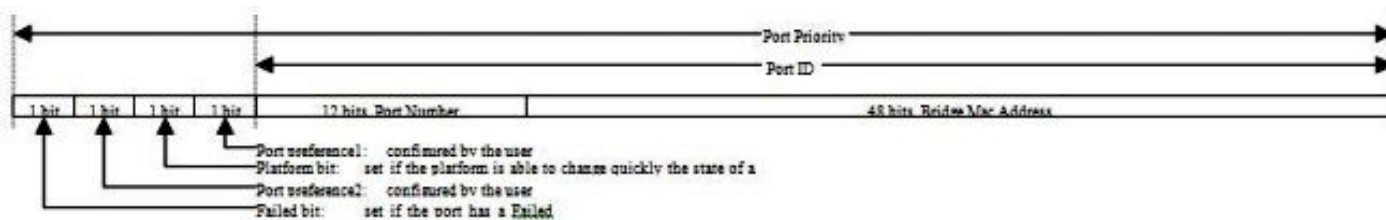


Figure 4. priorité de port

Il est maintenant évident pourquoi les ports défectueux constituent toujours les AP choisis dans le segment. Quand un port défectueux passe à l'état de port de remplacement, il génère une clé unique fondée sur son ID de port et un nombre aléatoire, et l'annonce avec son ID de port. Un AP se débloque uniquement s'il reçoit un message d'un port bloqué qui inclut sa clé locale. Ce mécanisme aide à empêcher le scénario de compétitivité décrit dans la section précédente. Voici des diagrammes qui affichent ce qui se produit quand les ports s'activent et se désactivent :

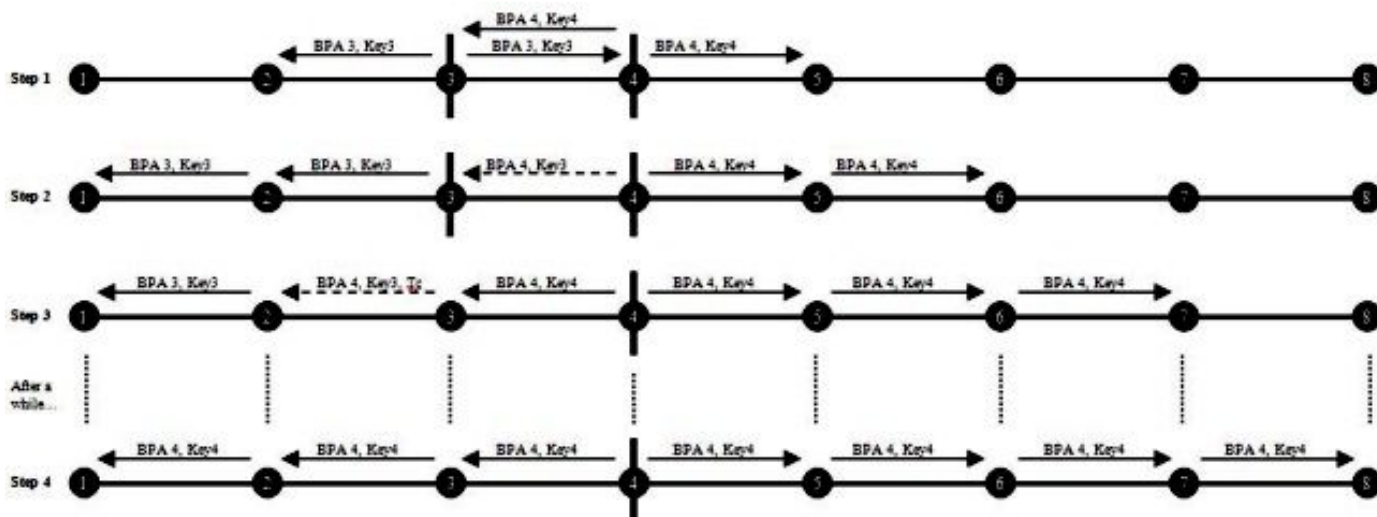


Figure 5. Exécution de BPA dans le lien

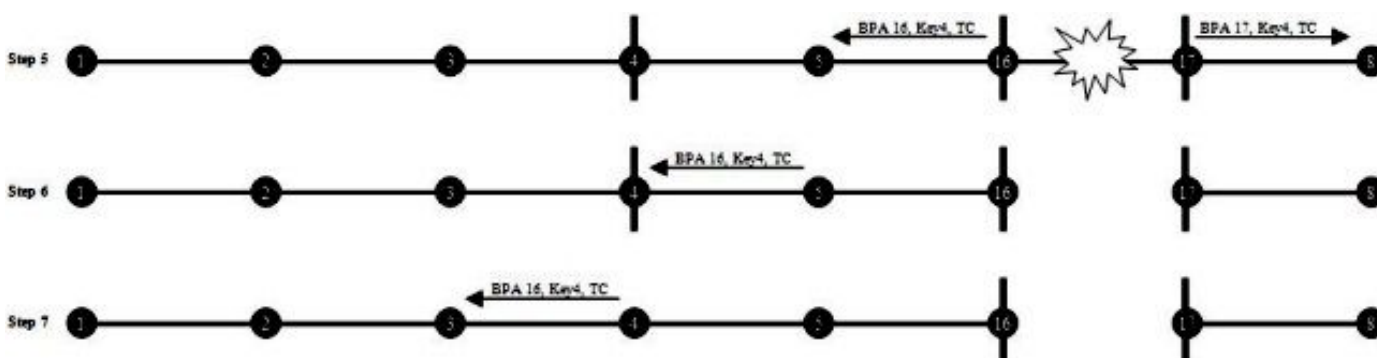


Figure 6. Exécution de BPA après panne de lien

Assistance matérielle

Quand une panne de lien survient dans un segment, un BPA inonde le reste du segment par HFL. Pour que cette opération soit entièrement efficace, le VLAN administrateur doit être porté sur tous les ports de segment et entre entre les ports de périphérie en dehors de du segment. BPA envoie également ces informations via LSL, car HFL ne peut pas garantir un transport fiable. S'il y a des problèmes avec la livraison HFL, le LSL assure une reconvergence.

EPA

Un port de fin est un port de périphérie ou un port défectueux. Quand un segment se termine par deux ports de périphérie, il est considéré comme complet, ce qui rend possible l'équilibrage de charge VLAN. Quand un segment se termine par un port défectueux, aucun équilibrage de charge n'est possible, car tous les ports sont ouverts.

Les ports de fin envoient périodiquement des EPA, qui sont retransmis par LSL. Les messages suivants :

- Propager des statistiques sur le segment
- Détecter l'état de segment complet
- Amorçage de l'équilibrage de charge VLAN

Statistiques de segment

Chaque port de fin envoie un EPA périodique qui contient des informations sur lui-même par LSL.

Chaque port intermédiaire ajoute ses propres informations et relaie l'EPA. Puisque ces messages se déplacent dans deux directions, chaque commutateur REP participant est informé sur le segment REP en entier. Les informations contenues dans l'EPA comprennent :

- ID de pont
- Identifiant et statut des deux ports participants dans le REP

Détection de l'état complet de segment

Chaque port de périphérie envoie un message spécial de sélection EPA avec sa propre priorité de périphérie et une clé spéciale (non liée à la clé BPA). Le premier port qui reçoit ce message indique sa propre priorité de port dans ce message et le retransmet au prochain commutateur. Chaque commutateur le long du chemin compare sa propre priorité de port à celle de l'EPA et la remplace par la sienne si la priorité est plus élevée. Quand le port de périphérie reçoit un EPA, il compare la priorité de périphérie à sa propre priorité. Si l'EPA reçu a une priorité plus élevée, le port de périphérie envoie son message EPA suivant avec la clé à la périphérie primaire. Ce mécanisme aide à atteindre deux buts :

- Faire en sorte que le segment est complet
- Fournir à chacun des deux ports de périphérie la connaissance du port intermédiaire ayant la plus haute priorité

Amorçage de l'équilibrage de charge VLAN

L'équilibrage de charge VLAN est réalisé avec deux AP différents qui bloquent des VLAN différents. La périphérie principale est et est responsable de l'AP sur au moins un sous-ensemble des VLAN, et elle envoie un message EPA qui indique au port de priorité la plus élevée de bloquer le reste. Les informations sur le port intermédiaire ayant la plus haute priorité ont déjà été récupérées avec le message de sélection EPA. Le type de message généré à cet effet est un élément TLV de commande EPA qui contient un bitmap des VLAN que le port à priorité supérieure doit bloquer.

Format PDU

En-tête EPA :

- Type=EPA
- No d'instance
- TLV facultatifs

TLV de sélection :

- edgePriority
- edgeKey
- BestPortPriority

TLV de commande :

- SelectedPortPriority
- VLAN sélectionnés

TLV d'information :

- ID de pont
- Identifiants des deux ports
- Rôles de port

Dépannage

Enquête sur un lien rompu

Voici un exemple d'une bonne topologie :

```
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
```

Voici un exemple d'élément rompu :

```
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
```

Voici son état antérieur :

```
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
```

Sélectionnez cette commande afin d'obtenir plus de détails sur le lien entre SwitchC et SwitchD ayant échoué :

```
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>
```

Voici à quoi ressemble le tout une fois que le lien est réactivé :

```
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
```

Notez que le port précédemment défaillant reste en tant que point d'accès et continue de se bloquer. La raison est que les choix d'AP ont lieu seulement entre les ports bloqués. Quand ce lien a échoué, tous autres ports dans la topologie se sont ouverts. Quand le lien a été réactivé, SwitchC et SwitchD ont envoyé des BPA avec leurs priorités. L'élément SwitchC F1/0/2 avait une priorité supérieure, donc est devenu AP. La situation demeure ainsi jusqu'à ce qu'un autre port dans la topologie échoue, ou qu'une **préemption** ait lieu.

Autres ports (ALT)

Un port ALT bloque certains ou tous les VLAN. En cas de défaillance du segment REP, aucun port ALT n'est disponible ; tous les ports sont ouverts. C'est ainsi que le protocole REP peut fournir un chemin actif pour le trafic de données en cas de panne.

Dans un segment REP complet (sans panne), il y a soit un port ALT, soit deux ports ALT. Si l'équilibrage de charge VLAN est activé, il y a deux ports ALT dans le segment – un des ports ALT bloque un ensemble spécifié de VLAN, et l'autre port ALT, qui est toujours à la périphérie principale, bloque l'ensemble complémentaire de VLAN. Si l'équilibrage de charge VLAN n'est pas activé, il y a un seul port ALT dans le segment qui bloque tous les VLAN.

L'ordre dans lequel les ports sont mis en ligne et les priorités de port intégrées déterminent quel port du segment devient un port ALT. Si vous voulez qu'un port particulier devienne le port ALT, configurez-le avec le mot-clé **de votre choix**. Voici un exemple :

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

Supposez que **gig3/1** est la périphérie principale et que vous voulez configurer l'équilibrage de charge VLAN :

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

Selon cette configuration, après la préemption, le port **gig3/10** consiste en un port ALT qui bloque les VLAN 1 à 150, et le port **gig3/1** consiste en un port ALT qui bloque les VLAN 151 à 4094.

La préemption se fait soit manuellement avec la commande **rep preempt segment 3**, soit **automatiquement si vous configurez une suspension de la <seconds>** préemption rep sous le port de périphérie principal.

Quand un segment se rétablit après une panne de lien, un des deux ports situés à côté de la panne s'affiche comme port ALT. Puis, après la préemption, l'emplacement des ports ALT devient conforme aux spécifications de la configuration.

Dépannage des contiguïtés du REP

Entrez cette commande afin de voir s'il y a une contiguïté :

```
SwitchC#show interface fa1/0/23 rep
```

```
Interface Seg-id Type LinkOp Role
```

```
-----  
FastEthernet1/0/23 1 TWO_WAY Open
```

Entrez cette commande afin d'obtenir plus d'information :

```
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
```

Déboguages

La plupart des débogages ont une sortie trop importante pour être utiles. Voici la liste complète (certains sont seulement offerts avec le service interne) :

```
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
```

```
lsism LSL state machine
```

```
misc miscellaneous
```

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

Débogages utiles

Voici quelques débogages utiles :

- **debug rep showcli** (nécessite un service interne) - Ce débogage imprime beaucoup d'informations supplémentaires lorsque vous entrez les commandes **show rep** normales.
- **debug rep error** - Ce débogage peut être très utile.
- **debug rep failure-recovery** - Ce débogage imprime les messages qui passent lorsqu'une liaison est rompue.

```
*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** - Ce débogage est bon pour dépanner les contiguïtés qui ne se forment pas. Il offre un aperçu intégral de ce qui se déroule à la connexion/déconnexion d'un lien.

```
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_preempt_ind@374: Posting pre empt indication
```

- **debug rep epasm** - Ce débogage fournit des informations utiles lors des modifications de topologie. Rien n'est imprimé si le segment est stable.

Voici la sortie lorsqu'un port est déconnecté :

```

*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

```

Voici le résultat obtenu lorsqu'un port est mis en ligne :

```

*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

```

Débugages moins utiles

- **debug rep bpa-event** - Ce débogage vous indique quand vous recevez un BPA et ce que vous en faites. Il présente quatre lignes par seconde.

```

[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 bpsm** - Ce débogage vous indique ce que fait la machine d'état BPA chaque fois qu'un BPA est reçu. Il présente trois lignes par seconde.

```

*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 lsism** - Ce débogage vide le traitement des messages LSL de bas niveau.

```
*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)
```

Informations connexes

- [Assistance technique et téléchargements Cisco](#)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.