Überprüfung des Resilient Ethernet Protocol

Inhalt

Einleitung

Dieses Dokument beschreibt eine Übersicht über das Resilient Ethernet Protocol (REP).

Unterstützte Plattformen

- Desktop Switching Business Unit (DSBU) Metro Switches (3750ME und ME3400), Version 12.2(40)SE und höher
- Cisco Catalyst Switch der Serie 4500, Version 12.2(44)SG und höher

- Cisco Catalyst Switch der Serie 6500 ab Whitney2 (12.2SXI)
- Cisco Catalyst Router der Serie 7600 ab Cobra (12.2SRC)

Hintergrundinformationen

Warum REP?

REP ist ein Protokoll, das in bestimmten Layer-2-Netzwerkdesigns das Spanning Tree Protocol (STP) ersetzt. Die aktuellste STP-Spezifikation ist Multiple Spanning Trees (MST), definiert in 802.1Q-2005. Benutzer, die eine Alternative zu MST wünschen, haben folgende berechtigte Bedenken:

- STP betrachtet eine Bridge-Domäne als Ganzes. Als Ergebnis wird ein lokaler Ausfall wiederhergestellt, wenn Sie den Zustand einer willkürlich entfernten Verbindung ändern. Die offensichtliche Unvorhersehbarkeit von STP wird nur gemindert, wenn Sie die Bridge-Domäne in kleine, unabhängige Teile segmentieren. Leider ist dies komplex, wenn nicht gar unmöglich, ohne die Entfernung einiger wichtiger Funktionen aus dem Spanning Tree (wie Loop Prevention in allen Szenarien) zu erreichen.

- Die STP-Konvergenz kann für Service Provider, die Wiederherstellungszeiten von 50 Millisekunden (ms) erwarten, die bei Schaltungstechnologien üblich sind, langsam erscheinen. Diese Langsamkeit wird nicht durch das Protokoll selbst verursacht. Die Plattformen müssen optimiert werden, um STP effizienter ausführen zu können. In der Zwischenzeit muss es neue Lösungen geben, die Plattformbeschränkungen umgehen.

- Die MST Load Balancing-Konfiguration ist nicht flexibel. Damit das MST eine Instanz-Lastverteilung erreichen kann, müssen alle Bridges Teil derselben Region sein. Regionen werden durch die Benutzerkonfiguration definiert, und es ist nicht möglich, die MST-Konfiguration auf einem Switch zu ändern, ohne dass eine gewisse Rekonvergenz im Netzwerk eingeführt wird. Dies könnte durch eine sorgfältige Vorkonfiguration und in begrenztem Umfang durch die Verwendung anderer Protokolle wie VLAN Trunk Protocol (VTP) v3 umgangen werden.

Vorteile

Hier einige der Vorteile von REP:

- REP bietet folgende Konvergenzzeiten:
  - 3750ME konvergiert zwischen 20 ms und 79 ms
  - ME3400 konvergiert zwischen 40 ms und 70 ms
- Funktioniert mit aktueller Hardware
- Berechenbare, blockierte Ports
- Einfache Konfiguration

Einschränkungen

Hier einige der Einschränkungen von REP:

- Kein Plug-and-Play
- Kein Schutz vor Fehlkonfigurationen (einfache Erstellung von Schleifen)
- Geringes Maß an Redundanz (kann nur einem Verbindungsausfall standhalten)
- Globale Topologie kann nicht erkannt werden (nur Segmenttopologie)
- Proprietäre Cisco Lösungen

Protokollbetrieb

Segmente

REP verwendet ein Segment als minimalen Netzwerk-Baustein. Ein Segment ist einfach eine Ansammlung von Ports, die miteinander verkettet sind. Nur zwei Ports können zu einem bestimmten Segment auf einer Bridge gehören, und jeder Segment-Port kann maximal einen externen Nachbarn haben. Die Definition des Segments erfolgt vollständig über die Benutzerkonfiguration. Das Segment wird durch zwei **Edge-Ports** abgeschlossen, die ebenfalls vom Benutzer festgelegt werden. Das REP-Protokoll, das auf Segmenten ausgeführt wird, ist so minimal wie möglich und garantiert nur diese Eigenschaften:

- Wenn alle Ports im Segment online und betriebsbereit sind, wird der Datenverkehr für jedes VLAN über einen einzelnen Port logisch blockiert.
- Wenn mindestens ein Port im Segment aus irgendeinem Grund nicht betriebsbereit ist, werden alle anderen betrieblichen Ports für alle VLANs weitergeleitet.
- Bei einem Verbindungsausfall wird die Blockierung aller verbleibenden Ports so schnell wie möglich aufgehoben. Wenn der letzte ausgefallene Port wieder betriebsbereit ist und ein logisch blockierter Port pro VLAN ausgewählt wird, muss dies ebenfalls zu einer möglichst geringen Unterbrechung des Netzwerks führen.

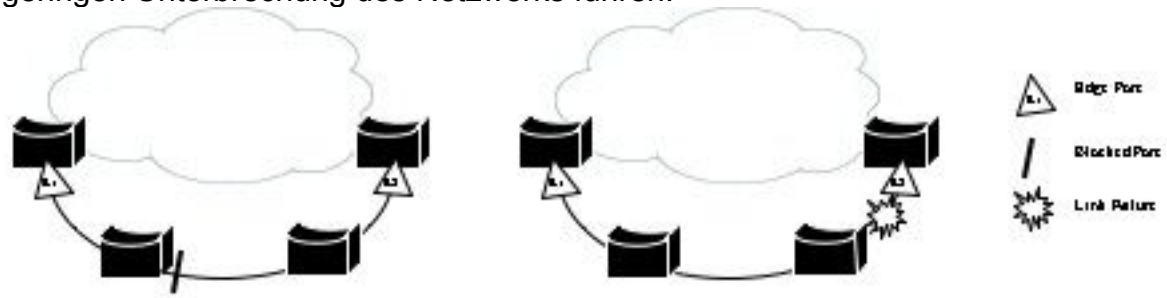

Abbildung 1. Ein Segment als einfacher Baustein

Abbildung 1 zeigt ein Beispiel für ein Segment mit sechs Ports, die über vier Bridges verteilt sind. Die konfigurierten Edge-Ports E1 und E2 sind im Diagramm mit einem Dreieck und der logisch blockierte Port mit einem Balken dargestellt. Wenn alle Ports betriebsbereit sind (siehe Abbildung links), wird ein einzelner Port blockiert. Bei einem Netzwerkausfall, wie im Diagramm rechts gezeigt, wechselt der logisch blockierte Port zurück in den Weiterleitungsstatus.

Wenn das Segment offen ist, wie in Abbildung 1 dargestellt, bietet es nie Verbindungen zwischen seinen beiden Edge-Ports. Es wird angenommen, dass die Verbindung zwischen REP-Edge-Switches außerhalb des Segments vorhanden ist (über STP). Bei einer optionalen Konfiguration wird eine STP Topology Change Notification (TCN) generiert, wenn im REP-Segment ein Fehler auftritt, um die Konvergenz zu beschleunigen.

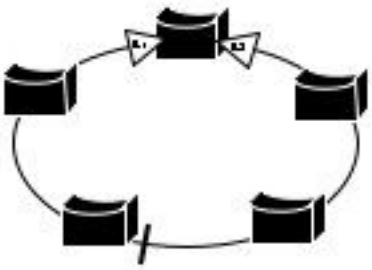

Abbildung 2. Ein Segment kann in einen Ring gewickelt werden.

Wenn sich die beiden Edge-Ports auf demselben Switch befinden (siehe Abbildung 2), wird das Segment in einen Ring gewickelt. In diesem Fall besteht eine Verbindung zwischen den Edge-Ports über das Segment. Mit dieser Konfiguration können Sie eine redundante Verbindung zwischen zwei beliebigen Switches im Segment erstellen.

Wenn Sie, wie in Abbildung 1 und Abbildung 2 dargestellt, Kombinationen aus offenen und geschlossenen Segmenten verwenden, können Sie eine Vielzahl unterschiedlicher Netzwerkdesigns erzielen.

Verbindungsstatusschicht

Verantwortlichkeiten

- Herstellen einer Verbindung mit einem eindeutigen Nachbarn
- Überprüfen Sie regelmäßig die Integrität der Verbindung mit dem Nachbarn.
- Nachrichten für Zustandssysteme höherer Layer senden und empfangen.
- Vom Nachbarn empfangene Bestätigungsdaten.
- Limit-Raten von Protokoll-Dateneinheiten (PDUs).

Hafenstaaten

Wenn ein Port für REP konfiguriert ist, erhält er die folgenden Status:

- Fehlgeschlagener Status (Blockierung)
- Es wurde eine Nachbarbeziehung hergestellt:
- Alternativer Port (blockiert, aber aktiv)
- Wahl des verlorenen Access Points (AP):
- Offener Port (wenn ein anderer Port den 'AP' gewählt hat)

Ein Port kann unter diesen Bedingungen nicht in Betrieb genommen werden:

- Kein Nachbar auf Port erkannt
- Mehr als ein Nachbar auf Port erkannt
- Der Nachbar bestätigt die Nachrichten nicht (ACK).

Paketdetails

Standardmäßig sendet REP Hello-Pakete an eine MAC-Adresse der Bridge-Protokoll-Dateneinheit (BPDU) im nativen VLAN (nicht markiert), sodass sie von Geräten verworfen werden, die diese Funktion nicht ausführen. Jede LSL-PDU (Link Status Layer) enthält sowohl die Sequenznummer der gesendeten PDU als auch die Remote-Sequenznummer der zuletzt empfangenen PDU. Dadurch wird eine zuverlässige Übertragung zwischen den Ports sichergestellt. Jeder Nachbar

speichert eine Kopie jeder PDU, bis eine ACK empfangen wird. Wenn keine ACK empfangen wird, wird sie nach Ablauf eines Zeitgebers erneut gesendet.

Die eigentliche LSL PDU enthält:

- ProtokollVersion (aktuell 0)
- SegmentID
- RemotePortID
- LokalePort-ID
- LokaleFolgenummer
- RemoteSeqNumber
- TLVs höherer Layer

LSL-Pakete werden in jedem Hello-Intervall oder wenn ein Protokoll einer höheren Schicht es anfordert, gesendet. Wenn die LSL-PDU erstellt wird, füllt sie zunächst ihre eigenen Felder aus, z. B. SegmentID und LocalPortID. Anschließend werden die Protokollwarteschlangen der höheren Ebene durchsucht, z. B. "Block Port Advertisement" (BPA) oder "End Port Advertisement" (EPA), um festzustellen, ob zusätzliche Daten in die Warteschlange gestellt werden müssen.

Hardware-Überlastungsschicht (HFL)

Die HFL ist das REP-Modul, das eine schnelle Konvergenz nach Verbindungsausfällen ermöglicht. Es sendet keine PDUs wie LSL an die BPDU-MAC-Adresse, sondern sendet Multicast-PDUs an eine spezielle MAC-Adresse (0100.0ccc.ccce) auf dem REP-Verwaltungs-VLAN. Auf diese Weise wird es in der Hardware an alle Switches im Segment geleitet.

Das HFL-Paketformat ist einfach:

- Protokollversion (immer noch 0)
- SegmentID
- Höhere TLVs (Layer Type Length)

Zu diesem Zeitpunkt sind die einzigen TLVs, die über HFL gesendet werden, BPAs.

BPA

BPAs werden von APs gesendet, um die blockierten VLANs zusammen mit ihrer Portpriorität anzukündigen. Dadurch kann das Segment über Verbindungsausfälle informiert werden, und es wird sichergestellt, dass pro VLAN nur ein Access Point pro Segment vorhanden ist. Dies ist nicht leicht zu erreichen.

Überlegungen

In einer stabilen Topologie sind die AP-Wahlen einfach. Ein online geschalteter Port startet als Access Point für alle VLANs (blockiert). Wenn er einen BPA von einem anderen Port mit einer höheren Priorität empfängt, weiß er, dass die Blockierung sicher aufgehoben werden kann. Wenn ein Port im Segment ausfällt, wird der gleiche Prozess verwendet, um die Blockierung der anderen Ports aufzuheben. Alle fehlerhaften Ports generieren eine höhere Portpriorität (mit einem **fehlerhaften Bit** in der Priorität) als die aktuellen APs, wodurch die Blockierung des aktuellen APs aufgehoben wird.

Probleme treten jedoch auf, wenn dieser Link wieder aktiviert wird. In diesem Fall wird das

fehlerhafte Bit der Priorität gelöscht, und die Priorität kehrt zum Normalwert zurück. Obwohl dieser Port seine neue Priorität kennt, können andere Teile des Segments veraltete BPA-Informationen von diesem Port erhalten. In diesem Diagramm wird dieses Szenario veranschaulicht:

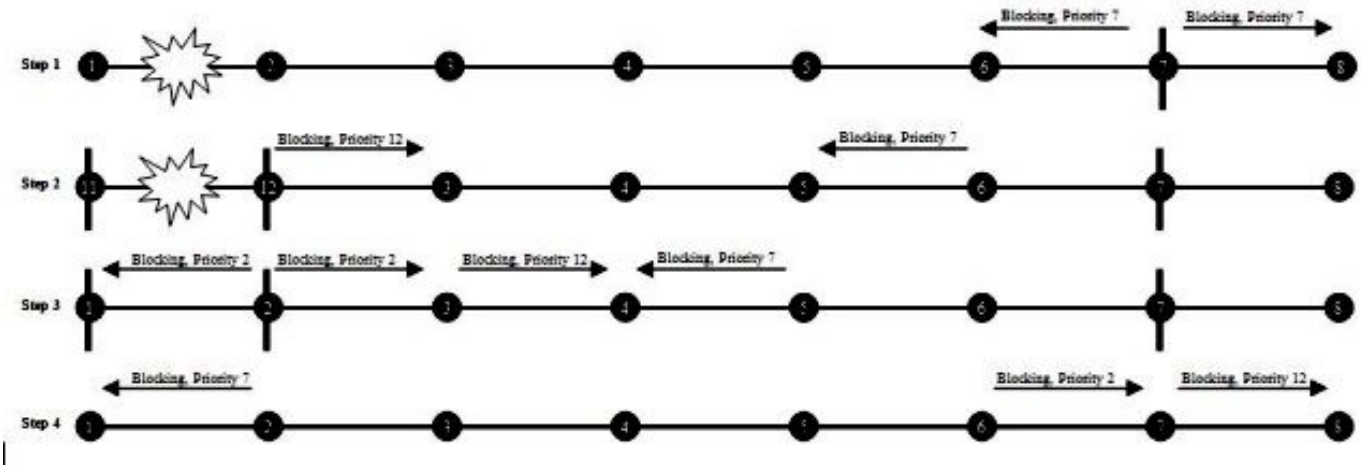

Abbildung 3: Veraltete Informationen, die das Segment öffnen

Zu Beginn dieses Szenarios blockiert Port 7 und kündigt seine Priorität als 7 an. Als Nächstes wird die Verbindung zwischen 11 und 12 unterbrochen, sodass 12 einen BPA sendet, der anzeigt, dass er mit einer Priorität von 12 blockiert. Bevor diese blockierenden Ports den BPA des anderen Ports erhalten, wird Port 12 wieder aktiviert und ist betriebsbereit. Bald darauf empfängt Port 12 den BPA von Port 7 mit Priorität 7 und löst die Blockierung auf. Port 7 empfängt dann das veraltete BPA von Port 12 mit Priorität 12, sodass die Blockierung aufgehoben wird. Dies verursacht eine Schleife. Diese Race Condition ist der Grund, warum BPA **Schlüssel** verwendet.

BPA-Verhalten

Jeder Port berechnet eine Port-Priorität mit den folgenden Informationen:

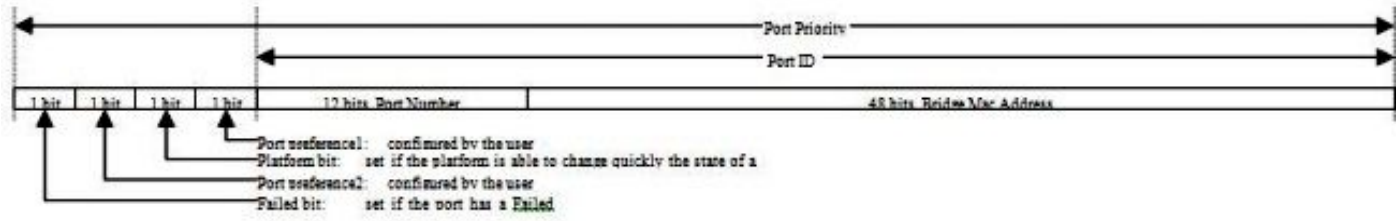

Abbildung 4: Port-Priorität

Es ist nun offensichtlich, warum ausgefallene Ports immer als APs für das Segment ausgewählt werden. Wenn ein Port von Failed zu Alternate wechselt, generiert er einen eindeutigen Schlüssel, der auf seiner Port-ID und einer Zufallszahl basiert, und gibt diesen zusammen mit seiner Port-ID bekannt. Die Blockierung wird von einem Access Point nur aufgehoben, wenn er eine Nachricht von einem blockierten Port empfängt, der seinen lokalen Schlüssel enthält. Dieser Mechanismus hilft dabei, das im vorherigen Abschnitt beschriebene Szenario der Race-Bedingung zu vermeiden. Die folgenden Diagramme zeigen, was passiert, wenn Ports ein- und ausfallen:

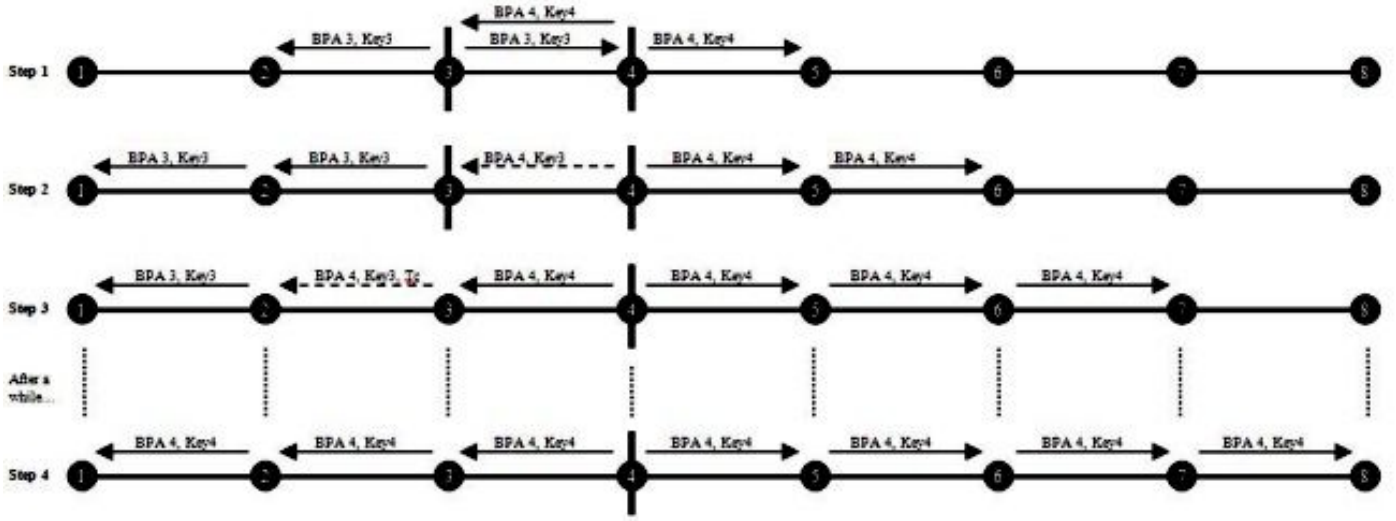

Abbildung 5: BPA-Betrieb bei Verbindungsaufbau

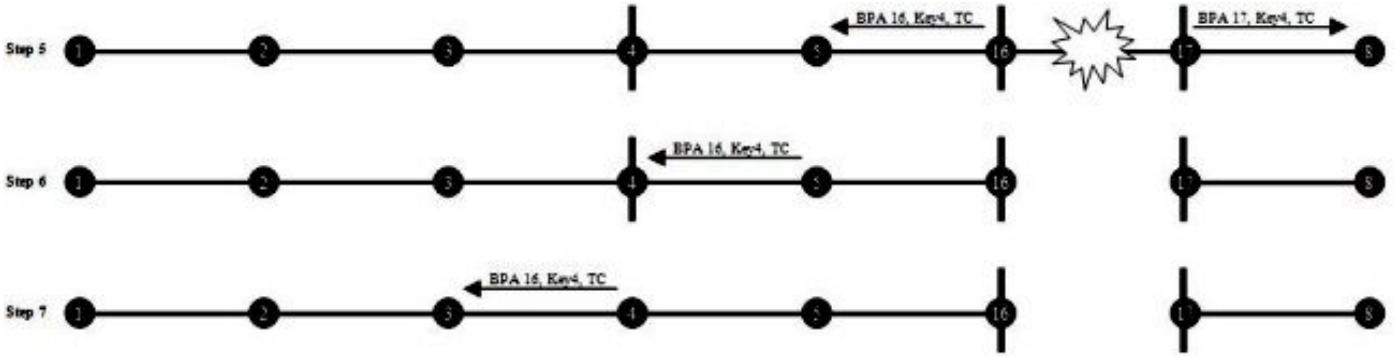

Abbildung 6: BPA-Betrieb nach Verbindungsausfall

Hardware-Unterstützung

Tritt in einem Segment ein Verbindungsausfall auf, wird ein BPA über HFL an den Rest des Segments weitergeleitet. Damit dies in vollem Umfang funktioniert, muss das Administrations-VLAN auf allen Segment-Ports sowie zwischen Edge-Ports außerhalb des Segments übertragen werden. BPA sendet diese Informationen auch über LSL, da HFL keinen zuverlässigen Transport garantieren kann. Bei Problemen mit der HFL-Bereitstellung stellt LSL sicher, dass eine Rekonvergenz stattfindet.

WPA

Ein Endport ist entweder ein Edge-Port oder ein ausgefallener Port. Wenn ein Segment auf beiden Seiten durch einen Edge-Port terminiert wird, gilt es als vollständig, und ein VLAN-Lastenausgleich ist möglich. Wenn ein Segment durch einen ausgefallenen Port terminiert wird, ist kein Load Balancing möglich, da alle Ports offen sind.

Endports senden regelmäßig EPAs, die über LSL weitergeleitet werden. Diese Meldungen:

- Statistiken über das Segment verbreiten
- Erkennen der Bedingung "Segment abgeschlossen"
- Initiierung des VLAN-Lastenausgleichs

Segmentstatistik

Jeder Endport sendet ein periodisches EPA, das Informationen über sich selbst über LSL enthält.

Jeder Zwischenanschluss fügt seine eigenen Informationen hinzu und leitet das EPA weiter. Da sich diese Meldungen in beide Richtungen bewegen, verfügt jeder REP-teilnehmende Switch über Kenntnisse des gesamten REP-Segments. Zu den im WPA enthaltenen Informationen gehören:

- Bridge-ID
- Port-ID und Status für beide REP-teilnehmenden Ports

Segment erkennen - Bedingung abgeschlossen

Jeder Edge-Port sendet eine spezielle WPA-Nachricht mit einer eigenen Edge-Priorität und einem speziellen Schlüssel (nicht mit dem BPA-Schlüssel verwandt). Der erste Port, der dies empfängt, legt seine eigene Port-Priorität in dieser Nachricht fest und leitet sie an den nächsten Switch weiter. Jeder Switch auf dem Pfad vergleicht seine eigene Port-Priorität mit der im EPA und ersetzt sie durch ihre eigene, wenn die Priorität höher ist. Wenn der Edge-Port ein EPA empfängt, vergleicht er die Edge-Priorität mit der eigenen. Wenn das empfangene EPA eine höhere Priorität hat, sendet der Edge-Port seine nächste EPA-Nachricht mit dem Schlüssel an den primären Edge. Mit diesem Mechanismus lassen sich zwei Ziele erreichen:

- Stellt sicher, dass das Segment vollständig ist
- Stellt beiden Edge-Ports Informationen über den Zwischenport mit der höchsten Priorität bereit.

Initiieren des VLAN-Lastenausgleichs

Der VLAN-Lastenausgleich wird mit zwei verschiedenen APs erreicht, die verschiedene VLANs blockieren. Der primäre Edge ist für den Access Point auf mindestens einer Teilmenge der VLANs zuständig und sendet eine EPA-Nachricht, die den Port mit der höchsten Priorität anweist, den Rest zu blockieren. Die Informationen über den Zwischenhafen mit der höchsten Priorität wurden bereits mit der WPA-Wahlnachricht abgerufen. Der Nachrichtentyp, der hierfür generiert wird, ist ein EPA-Befehls-TLV, der eine Bitmap der VLANs enthält, die der Port mit der höchsten Priorität blockieren muss.

PDU-Format

WPA-Überschrift:

- Typ=EPA
- Instanznr.
- Optionale TLVs

Wahl TLV:

- EdgePriorität
- Kantenschlüssel
- BestePortPriorität

Befehl TLV:

- AusgewähltePortPriorität
- Ausgewählte VLANs

Informationen TLV:

- Bridge-ID
- Zwei Port-IDs
- Port-Rollen

Fehlerbehebung

Untersuchung unterbrochener Verbindungen

Hier ist ein Beispiel für eine gute 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
```

Hier ist ein Beispiel, bei dem etwas kaputt ist:

```
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
```

So sah es früher aus:

```
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
```

Geben Sie diesen Befehl ein, um weitere Details zu der fehlgeschlagenen Verbindung zwischen SwitchC und SwitchD zu erhalten:

```
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>
```

So sieht es aus, wenn Sie den Link wieder hochfahren:

```
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
```

Beachten Sie, dass der zuvor ausgefallene Port als Access Point erhalten bleibt und weiterhin blockiert wird. Der Grund hierfür ist, dass AP-Wahlen nur zwischen blockierten Ports stattfinden. Wenn diese Verbindung fehlschlug, öffneten sich alle anderen Ports in der Topologie. Als die Verbindung hergestellt wurde, sendeten SwitchC und SwitchD BPAs mit ihren Prioritäten. Switch C F1/0/2 hatte eine höhere Priorität und wurde somit zum AP. Dieser Vorgang wird fortgesetzt, bis ein anderer Port in der Topologie ausfällt oder eine **Zwangstrennung** durchgeführt wird.

Alternative Ports (ALT)

Ein ALT-Port blockiert einige oder alle VLANs. Wenn im REP-Segment ein Fehler auftritt, gibt es keinen ALT-Port. Alle Ports sind offen. Auf diese Weise kann REP einen aktiven Pfad für den Datenverkehr bereitstellen, wenn ein Fehler auftritt.

In einem kompletten REP-Segment (wenn kein Fehler vorliegt) gibt es entweder einen ALT-Port oder zwei ALT-Ports. Wenn VLAN-Lastenausgleich aktiviert ist, gibt es zwei ALT-Ports im Segment. Einer der ALT-Ports blockiert einen bestimmten Satz von VLANs, und der andere ALT-Port, der sich immer am primären Edge befindet, blockiert den komplementären Satz von VLANs. Wenn VLAN Load Balancing nicht aktiviert ist, gibt es einen einzelnen ALT-Port im Segment, der alle VLANs blockiert.

Die Reihenfolge, in der die Ports online gehen, und die integrierten Portprioritäten bestimmen, welcher Port im Segment ein ALT-Port wird. Wenn Sie einen bestimmten Port als ALT-Port festlegen möchten, konfigurieren Sie ihn mit dem **bevorzugten** Schlüsselwort. Hier ein Beispiel:

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

Angenommen, **gig3/1** ist das primäre Edge, und Sie möchten den VLAN-Lastenausgleich konfigurieren:

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

Bei dieser Konfiguration ist Port **gig3/10** nach der Freischaltung ein ALT-Port, der die VLANs 1 bis

150 blockiert, und Port gig3/1 ein ALT-Port, der die VLANs 151 bis 4094 blockiert.

Die Freischaltung erfolgt entweder manuell mit dem Befehl **rep preempt segment 3** oder automatisch, wenn Sie die **Freischaltungsverzögerung *<seconds>*** unter dem primären Edge-Port konfigurieren.

Wenn ein Segment nach einem Verbindungsausfall wieder instand gesetzt wird, wird einer der beiden Ports neben dem Ausfall als ALT-Port angezeigt. Nach der Freischaltung wird die Position der ALT-Ports entsprechend der Konfiguration festgelegt.

Fehlerbehebung bei REP-Adjacencies

Geben Sie den folgenden Befehl ein, um festzustellen, ob eine Adjacency vorhanden ist:

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

Geben Sie diesen Befehl ein, um weitere Informationen zu erhalten:

```
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
```

Fehlerbehebung

Die meisten Debugs geben zu viel aus, um nützlich zu sein. Hier ist die vollständige Liste (einige nur bei internem Service verfügbar):

```
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
```

Nützliche Debugs

Hier einige nützliche Fehlerbehebungen:

- **debug rep showcli (**benötigt service internal) - Dieses Debugging gibt viele zusätzliche Informationen aus, wenn Sie die regulären Befehle **show rep** eingeben.
- **debug rep error** - Dieses Debugging kann sehr nützlich sein.
- **debug rep failure-recovery** - Bei diesem Debugging werden Nachrichten ausgegeben, die verstreichen, wenn eine Verbindung unterbrochen wird.

```
*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** - Dieses Debugging eignet sich zur Fehlerbehebung von Adjacencies, die sich nicht bilden. Es bietet Ihnen eine Play-by-Play, was passiert bei link up/down.

```
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** - Dieses Debug bietet nützliche Informationen bei Topologieänderungen. Wenn das Segment stabil ist, wird nichts gedruckt.

Die folgende Ausgabe wird ausgegeben, wenn ein Port offline geht:

```
*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
```

Hier ist die Ausgabe, wenn ein Port online geht:

```
*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
```

Weniger hilfreiche Debugs

- **debug rep bpa-event** - Dieses Debugging informiert Sie darüber, wann Sie eine BPA erhalten und was Sie damit machen. Es hat vier Linien pro Sekunde.

```
[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** - Dieses Debug-Tool zeigt an, was der BPA-Statuscomputer tut, wenn ein BPA empfangen wird. Er hat drei Zeilen pro Sekunde.

```
*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 -** Mit diesem Debugging wird die Verarbeitung von LSL-Nachrichten auf niedriger Ebene ausgelöst.

```
*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)
```

Zugehörige Informationen

- Technischer Support und Downloads von Cisco

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.