Cisco Catalyst IE9300 高耐久性シリーズ スイッチ冗長プロトコル コンフィギュレーション ガイド

初版：2022 年 4 月 26 日

最終更新：2023 年 9 月 14 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

Full Cisco Trademarks with Software License

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

通信、サービス、およびその他の情報

通信、サービス、およびその他の情報

- シスコからタイムリーな関連情報を受け取るには、Cisco Profile Manager でサインアップしてください。
- 重要な技術によりビジネスに必要な影響を与えるには、Cisco Services [英語] にアクセスしてください。
- サービス リクエストを送信するには、Cisco Support [英語] にアクセスしてください。
- 安全で検証済みのエンタープライズクラスのアプリケーション、製品、ソリューション、およびサービスを探して参照するには、Cisco DevNet にアクセスしてください。
- 一般的なネットワーク、トレーニング、認定関連の出版物を入手するには、Cisco Press にアクセスしてください。
- 特定の製品または製品ファミリの保証情報を探すには、Cisco Warranty Finder にアクセスしてください。

シスコバグ検索ツール

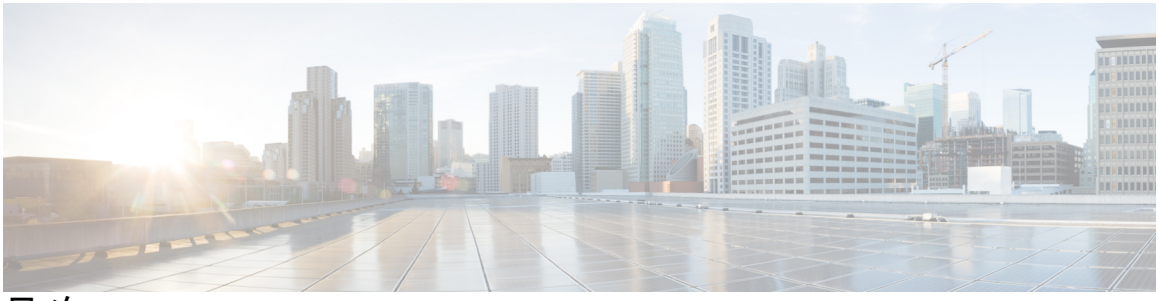
Ciscoシスコバグ検索ツール（BST）は、シスコ製品とソフトウェアの障害と脆弱性の包括的なリストを管理するシスコバグ追跡システムへのゲートウェイです。BST は、製品とソフトウェアに関する詳細な障害情報を提供します。

マニュアルに関するフィードバック

シスコのテクニカルドキュメントに関するフィードバックを提供するには、それぞれのオンラインドキュメントの右側のペインにあるフィードバックフォームを使用してください。

バイアスフリー言語

この製品のマニュアルセットは、偏向のない言語を使用するように配慮されています。このドキュメントセットでの偏向のない言語とは、年齢、障害、性別、人種的アイデンティティ、民族的アイデンティティ、性的指向、社会経済的地位、およびインターセクショナリティに基づく差別を意味しない言語として定義されています。製品ソフトウェアのユーザインターフェイスにハードコードされている言語、基準ドキュメントに基づいて使用されている言語、または参照されているサードパーティ製品で使用されている言語によりドキュメントに例外が存在する場合があります。



目 次

Full Cisco Trademarks with Software License iii

通信、サービス、およびその他の情報 iv

シスコバグ検索ツール iv

マニュアルに関するフィードバック iv

バイアスフリー言語 v

第 1 章 **Parallel Redundancy Protocol** 1

PRP について 1

スイッチのロール 3

PRP チャネル 3

混合トラフィックと監視フレーム 3

監視フレームの VLAN タグ 4

前提条件 5

注意事項と制約事項 6

デフォルト設定 9

PRP チャネルとグループを作成する 9

例 11

監視フレームの VLAN タギングを使用した PRP チャネルの設定 12

スタティックエントリをノードテーブルと VDAN テーブルに追加する 15

すべてのノードテーブルと VDAN テーブルのダイナミックエントリのクリア 16

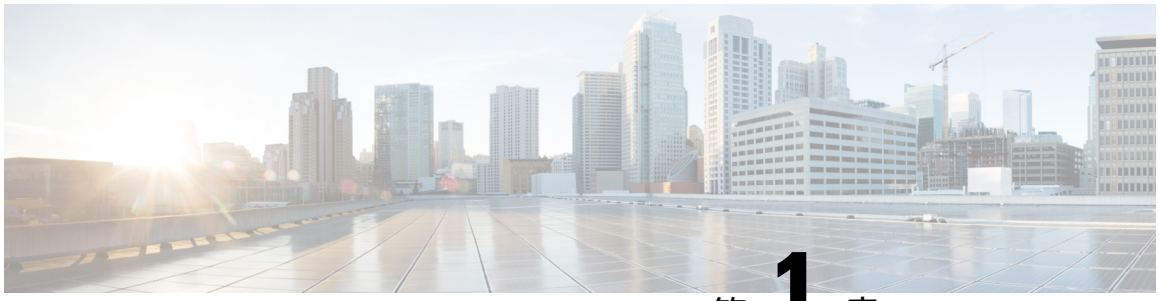
PRP チャネルおよびグループの無効化 17

Syslog のエラーおよび警告メッセージ 17
PRP ロギング間隔の設定 18
設定例 19
設定の確認 30
関連資料 32
機能の履歴 33

第 2 章 PRP を介した PTP 35
PRP を介した PTP 35
サポートされる PTP のプロファイルとクロックモード 38
PRP RedBox のタイプ 39
LAN-A および LAN-B の障害検出と処理 45
PRP を介した PTP の CLI コマンド 45
show ptp clock running 46
show prp channel detail 46
show prp statistics ptpPacketStatistics 46
show ptp lan port int 47
ptp clock boundary domain 47
PRP を介した PTP 機能の履歴 48

第 3 章 Redundancy Ethernet Protocol 49
Resilient Ethernet Protocol 49
リンク完全性 51
高速コンバージェンス 52
VLAN ロード バランシング 52
スパニングツリー インタラクション 54
Resilient Ethernet Protocol（REP）ネゴシエート 54
REP ポート 55
Resilient Ethernet Protocol の設定 56
REP のデフォルト設定 56
REP の設定ガイドラインと制限事項 56
REP 管理 VLAN を設定する 59

REP インターフェイスの設定 60
VLAN ロード バランシングの手動によるプリエンプションの設定 64
REP の SNMP トラップ設定 65
Resilient Ethernet Protocol Fast 66
REP Fast の設定 67
Resilient Ethernet Protocol 設定のモニタリング 68
Resilient Ethernet Protocol の機能履歴 70



第 1 章

Parallel Redundancy Protocol

- PRP について （1 ページ）
- 前提条件 （5 ページ）
- 注意事項と制約事項 （6 ページ）
- デフォルト設定 （9 ページ）
- PRP チャネルとグループを作成する （9 ページ）
- 監視フレームの VLAN タギングを使用した PRP チャネルの設定 （12 ページ）
- スタティックエントリをノードテーブルと VDAN テーブルに追加する （15 ページ）
- すべてのノードテーブルと VDAN テーブルのダイナミックエントリのクリア （16 ページ）
- PRP チャネルおよびグループの無効化 （17 ページ）
- Syslog のエラーおよび警告メッセージ （17 ページ）
- 設定例 （19 ページ）
- 設定の確認 （30 ページ）
- 関連資料 （32 ページ）
- 機能の履歴 （33 ページ）

PRP について

Parallel Redundancy Protocol（PRP）は、国際規格 IEC 62439-3 で定義されています。PRP は、イーサネットネットワークでヒットレス冗長性（障害後の回復時間ゼロ）を提供するように設計されています。

（注） PRP は、Cisco IOS XE Cupertino 17.7.1 以降の IE-9320-26S2C-E と IE-9320-26S2C-A、Cisco IOX XE Dublin 17.12.1 以降の IE-9320-22S2C4X-A と IE-9320-22S2C4X-A のように、複数の Cisco Catalyst IE9300 高耐久性シリーズ スイッチ でサポートされています。

ネットワーク障害から回復するために、RSTP、REP、MRP などのプロトコルを使用してメッシュトポロジまたはリングトポロジで接続されたネットワーク要素によって冗長性を提供できます。この場合、ネットワーク障害が発生するとネットワーク内の一部が再構成され、トラ

フィックが再び流れるようになります（通常、ブロックされたポートを開くことによって）。これらの冗長性スキームでは、ネットワークが回復し、トラフィックが再び流れるまでに数ミリ秒から数秒かかることがあります。

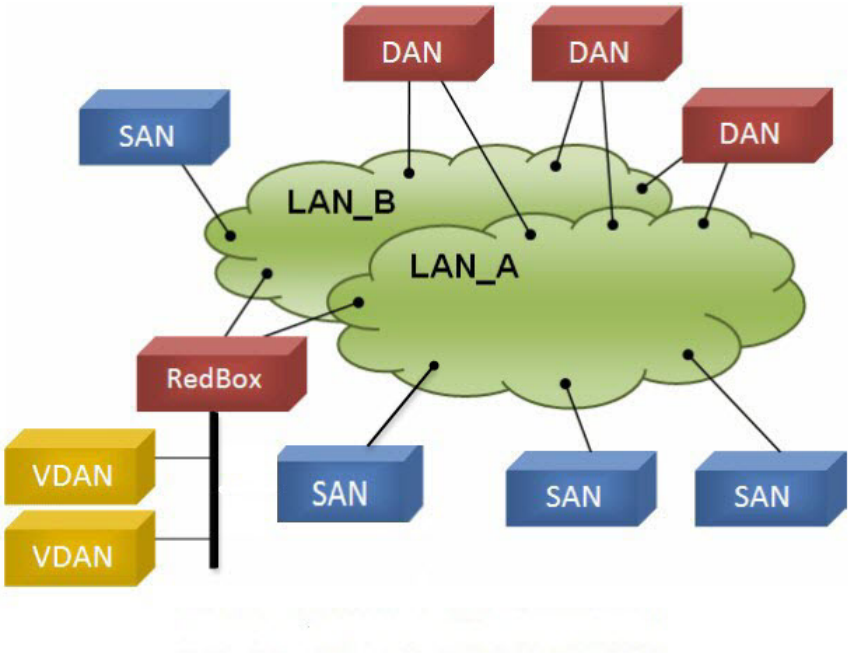
PRP は異なる方式を使用します。この方式では、2 つのネットワーク インターフェイスを 2 つの独立した分離されたパラレルネットワーク（LAN-A と LAN-B）に接続することで、（ネットワーク要素ではなく）エンドノードが冗長性を実装します。これらのデュアル接続ノード（DAN）のそれぞれには、ネットワーク内の他のすべての DAN への冗長パスがあります。

DAN は、2 つのネットワーク インターフェイスを介して 2 つのパケットを宛先ノードに同時に送信します。宛先ノードが重複パケットを容易に区別できるように、シーケンス番号を含む冗長制御トレーラ（RCT）が各フレームに追加されます。宛先 DAN は最初のパケットを正常に受信すると RCT を削除してパケットを消費します。2 番目のパケットが正常に到着した場合、そのパケットは破棄されます。パスの 1 つで障害が発生した場合、トラフィックは中断されることなくもう一方のパスに流れ続け、回復時間ゼロが求められます。

LAN-A または LAN-B のいずれかにのみ接続するネットワーク内の非冗長エンドポイントは、シングル接続ノード（SAN）と呼ばれます。

冗長ボックス（RedBox）は、2 つのネットワークポートがなく、PRP を実装していないエンドノードが冗長性を実装する必要がある場合に使用されます。このようなエンドノードは、デバイスに代わって 2 つの異なるネットワークへの接続を提供する RedBox に接続できます。RedBox の背後にあるノードは、DAN などの他のノードに見えるため、「仮想 DAN（VDAN）」と呼ばれます。RedBox 自体は DAN であり、VDAN に代わってプロキシとして機能します。

図 *1 : PRP* 冗長ネットワーク



冗長性を管理し、他の DAN の存在を確認するために、DAN は定期的に監視フレームを送信し、他の DAN が送信した監視フレームを評価できます。

スイッチのロール

IE-9320-26S2C-A、IE-9320-26S2C-E、IE-9320-22S2C4X-A、および IE-9320-22S2C4X-A スイッチは、2 つの各 LAN へのギガビット イーサネット ポート接続を使用した RedBox 機能を実装しています。

PRP チャネル

PRP チャネルまたはチャネルグループは、2 つのギガビット イーサネット インターフェイス（アクセス、トランクまたはルーテッド）を単一のリンクに集約する論理インターフェイスです。チャネルグループでは、小さい番号のギガビット イーサネット メンバー ポートがプライマリポートで、LAN-A に接続します。大きい番号のポートはセカンダリポートで、LAN-B に接続します。

これらのメンバーポートの少なくとも 1 つが稼働し続け、トラフィックを送信する限り、PRP チャネルも稼働したままになります。両方のメンバーポートがダウンした場合、チャネルもダウンします。サポートされる PRP チャネルグループの総数は、スイッチごとに 2 つです。次の表に示すように、各スイッチシリーズの各グループに使用できるインターフェイスは固定されています。

PRP チャネル番号	IE9300 シリーズ
PRP チャネル 1	Gi1/0/21（LAN-A）および Gi1/0/22（LAN-B）
PRP チャネル 2	Gi1/0/23（LAN-A）および Gi1/0/24（LAN-B）

混合トラフィックと監視フレーム

RedBox PRP チャネルグループから出力されるトラフィックは、混合可能、つまり宛先を SAN（LAN-A または LAN-B でのみ接続）または DAN にすることができます。SAN のパケットの複製を防ぐため、スイッチは受信した DAN エントリのスーパバイザフレームから、および SAN の非 PRP（通常トラフィック）フレームから送信元 MAC アドレスを学習し、これらのアドレスをノード テーブルに保存します。PRP チャネルから SAN の MAC アドレスにパケットを転送すると、スイッチはエントリを検索し、パケットを複製する代わりに送信先 LAN を決定します。

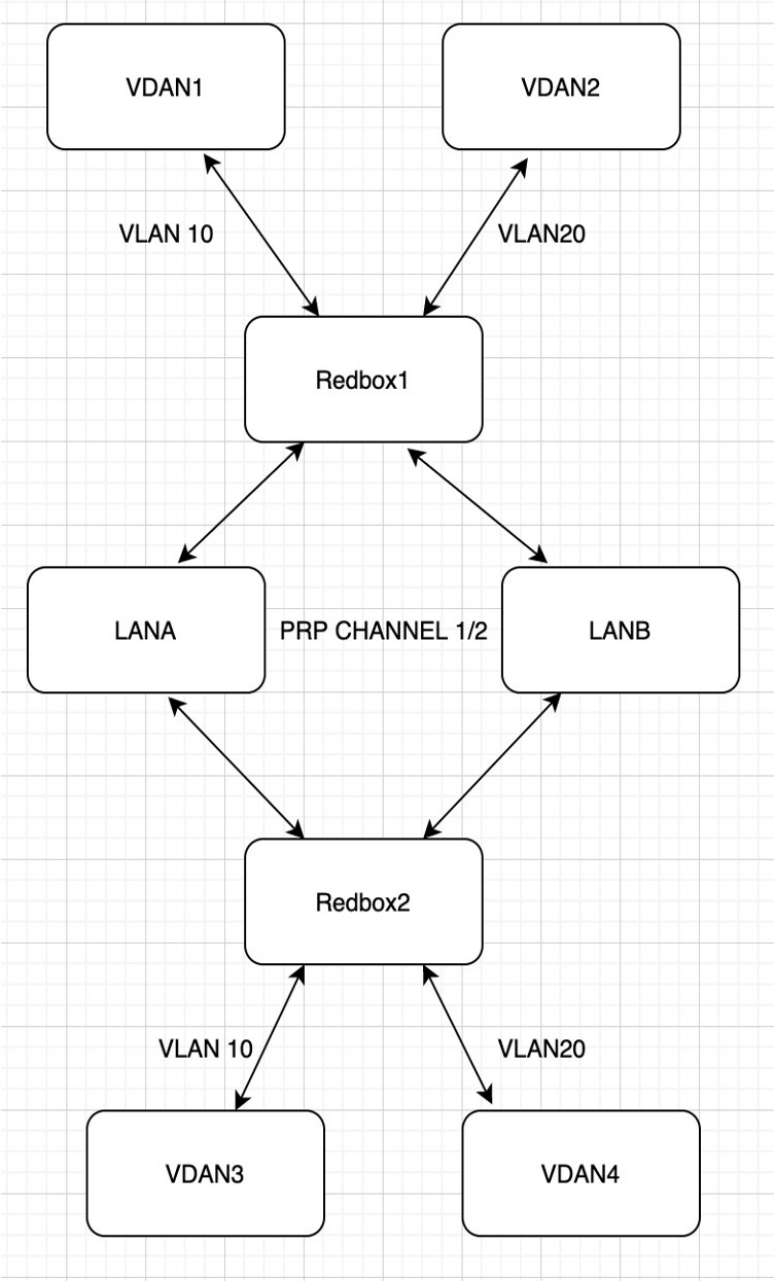
VDAN の RedBox では、これらの VDAN の代理で監視フレームを送信する必要があります。他のすべてのポートに着信し、PRP チャネルポートを送信するトラフィックの場合、スイッチは、送信元 MAC アドレスを学習して VDAN テーブルに追加し、それらのアドレスに対応する監視フレームの送信を開始します。学習された VDAN エントリにはエージングが適用されます。

x の説明に従って、ノードテーブルと VDAN テーブルにスタティックエントリを追加できます。ノードテーブルと VDAN テーブルを表示したり、エントリを消去したりすることもできます。y および z を参照してください。

監視フレームの VLAN タグ

Cisco Catalyst IE9300 高耐久性シリーズ スイッチ は、監視フレームの VLAN タギングをサポートします。PRP VLAN タギングでは、PRP インターフェイスをトランクモードに設定する必要があります。この機能を使用すると、PRP チャネルの監視フレームで VLAN ID を指定できます。

次の設定例では、PRP チャネル 1 インターフェイスがトランクモードに設定され、VLAN 10 および 20 が許可されています。監視フレームは VLAN ID 10 を使用してタグ付けされます。RedBox1 は、VDAN に代わり PRP VLAN ID を使用して監視フレームを送信しますが、VDAN からの通常のトラフィックは、PRP トランクの VLAN 設定に基づいて PRP チャネルを通過します。



設定の詳細については、監視フレームの VLAN タギングを使用した PRP チャネルの設定 （12 ページ）を参照してください。

前提条件

- IE-9320-26S2C-A、IE-9320-26S2C-E、IE-9320-22S2C4X-A、または IE-9320-22S2C4X-A スイッチ

- Network Essentials または Network Advantage ライセンス
- 2 チャネル PRP をサポートする Cisco IOS XE 17.7.1 以降

注意事項と制約事項

ガイドライン

- PRP DAN と RedBox では 6 バイトの PRP トレーラをパケットに追加するため、最大伝送ユニット（MTU）サイズが 1500 の一部のスイッチでは、PRP パケットがドロップされる可能性があります。すべてのパケットがPRPネットワークを通過できるようにするには、PRP LAN-A と LAN-B ネットワーク内のスイッチの MTU サイズを次のように 1506 に増やします。
  - **system mtu 1506**
  - **system mtu jumbo 1506**
- 監視フレーム VLAN タギングを設定するには、インターフェイスをトランクモードで設定する必要があります。

（注） 監視フレームVLANタグ設定が存在する場合、PRPインターフェイスにアクセスモードを設定できません。監視フレームVLANタギングを使用してPRPインターフェイスにアクセスモードを設定しようとすると、次のメッセージが表示されます。

```
%PRP_MSG-4-PRP_VLANTAG: Warning: Do not configure access
 mode for PRP interfaces with tagged supervision frames.
```

- PRP チャネルには、アクティブな状態で冗長性を維持するために、チャネル内に 2 つのアクティブポートが設定されている必要があります。
- チャネルグループ内の両方のインターフェイスに、同じ設定が必要です。
- レイヤ 3 の場合は、PRP チャネルインターフェイスで IP アドレスを設定する必要があります。
- PRP が有効になっているインターフェイスでは、LLDP と CDP を無効にする必要があります。
- 特にインターフェイスに media-type sfp がある場合は、PRP が有効になっているインターフェイスで UDLD を無効にする必要があります。
- **spanning-tree bpdufilter enable** コマンドは、prp-channel インターフェイスで必須です。スパニングツリー BPDU フィルタは、すべての入出力 BPDU トラフィックをドロップしま

す。このコマンドは、ネットワーク内に独立したスパニングツリードメイン（ゾーン）を作成するために必要です。

- **spanning-tree portfast edge trunk** コマンドは、prp-channel インターフェイスでは任意ですが、強く推奨されます。これにより、PRP LAN-A および LAN-B のスパニング ツリー コンバージェンス時間が改善されます。
- PRP 統計情報の場合は、**show interface prp-channel** [**1**|**2**] コマンドを使用します。**show interface gi1/0/21** などの物理インターフェイスの show コマンドでは、PRP 統計情報を提供しません。
- Cisco Catalyst IE9300 高耐久性シリーズ スイッチ では、次の例に示すように **int Gi1/0/23** または **int Gi1/0/24** を使用します。

```
switch(config)#int Gi1/0/23
switch(config-if)#shut
%Interface GigabitEthernet1/0/23 is configured in PRP-channel group, shutdown not
permitted!
```

- PRP 機能は、CIP プロトコルを使用して管理できます。PRP では、次の CIP コマンドを使用できます。
  - show cip object prp <*0-2*>
  - show cip object nodetable <*0-2*>

制限事項

- PRP は、IE-9320-26S2C-A、IE-9320-26S2C-E、IE-9320-22S2C4X-A、IE-9320-22S2C4X-A スイッチでのみサポートされます。
- PRP トラフィック負荷は、ギガビット イーサネット インターフェイス チャネルの帯域幅の 90% を超えることはできません。
- ロードバランシングはサポートされていません。
- **show prp channel detail** コマンドを入力すると、レイヤタイプ = L3 セクションのプロトコルステータスが誤って表示されます。正しいプロトコルステータスについては、出力の Ports in the group セクションを参照してください。

  次に、Cisco Catalyst IE9300 高耐久性シリーズ スイッチ の出力例を示します。

  .

```
show prp channel detail

PRP-channel: PR1
------------
 Layer type = L2
 Ports: 2 Maxports = 2
 Port state = prp-channel is Inuse
 Protocol = Enabled
Ports in the group:
  1) Port: Gi1/0/21
   Logical slot/port = 1/21 Port state = Inuse
```

```
 Protocol = Enabled
  2) Port: Gi1/0/22
   Logical slot/port = 1/22 Port state = Inuse
 Protocol = Enabled

PRP-channel: PR2
------------
 Layer type = L2
 Ports: 2 Maxports = 2
 Port state = prp-channel is Inuse
 Protocol = Enabled
Ports in the group:
  1) Port: Gi1/0/23
   Logical slot/port = 1/23 Port state = Inuse
 Protocol = Enabled
  2) Port: Gi1/0/24
   Logical slot/port = 1/24 Port state = Inuse
 Protocol = Enabled
```

- 個々の PRP インターフェイスがダウンしても、**show interface status** でリンクの UP ステータスを引き続き表示します。これは、ポートのステータスが PRP モジュールによって制御されるためです。**show prp channel** コマンドを使用して、リンクのステータスを確認します。これにより、リンクがダウンしているかどうかがわかります。

  次の例は、**show prp channel** コマンドの出力を示しています。

```
show prp channel 2 detail

PRP-channel: PR2
------------
 Layer type = L2
 Ports: 2 Maxports = 2
 Port state = prp-channel is Inuse
 Protocol = Enabled
Ports in the group:
  1) Port: Gi1/0/23
   Logical slot/port = 1/23 Port state = Inuse
 Protocol = Enabled
  2) Port: Gi1/0/24
   Logical slot/port = 1/24 Port state = Inuse
 Protocol = Enabled
```

ノードテーブルと VDAN テーブル

- スイッチは、ノードテーブルで最大 512（SAN+DANP）件のエントリをサポートします。
- 静的ノード/VDAN の最大数は 16 です。
- ハッシュの衝突により、MAC アドレスの数が制限される場合があります。ノードテーブルでノードから MAC アドレスを学習するためのリソースが不足している場合、スイッチはデフォルトでそのノードを DAN として扱います。
- リロード後（MAC アドレスが学習される前）、スイッチは、学習前のノードを一時的に DAN として扱い、ノードから入力パケットまたは監視フレームを受信してノードテーブルにエントリを入力するまで、出力パケットを複製します。

- スイッチは、VDAN テーブルで最大 512 件の VDAN エントリをサポートします。VDAN テーブルがいっぱいの場合、スイッチは新しい VDANS の監視フレームを送信できません。

デフォルト設定

デフォルトでは、PRP チャネルは、作成するまでスイッチに存在しません。PRP チャネル （3 ページ）で説明されているように、PRP 用に設定できるインターフェイスは固定されています。

PRP チャネルとグループを作成する

スイッチで PRP チャネルおよびグループを作成して有効にするには、次の手順に従います。

始める前に

- PRP チャネル （3 ページ）の説明に従って、各スイッチタイプでサポートされている特定のインターフェイスを確認します。
- 前提条件 （5 ページ）と注意事項と制約事項 （6 ページ）を確認してください。
- PRP チャネルを作成する前に、PRP チャネルのメンバーインターフェイスが、FlexLinks、EtherChannel、REP などの冗長プロトコルに参加していないことを確認します。

手順の概要

1. グローバル コンフィギュレーション モードを開始します。
2. PRP チャネルグループにギガビット イーサネット インターフェイスを 2 つ割り当てます。チャネル 1 の場合は、次のように入力します。
3. （任意）レイヤ 2 トラフィックの場合は、**switchport** と入力します。（デフォルト）：
4. （任意）非トランキングでタグのない、単一の VLAN レイヤ 2（アクセス）インターフェイスを設定します。
5. （任意）ギガビット イーサネット インターフェイスの VLAN を作成します。
6. （任意）スイッチで高精度時間プロトコル（PTP）を無効にします。
7. 冗長チャネルのループ検出を無効にします。
8. 冗長チャネルの UDLD を無効にします。
9. サブインターフェイスモードを開始し、PRP チャネルグループを作成します。
10. PRP チャネルを起動します。
11. PRP インターフェイスを指定し、インターフェイスモードを開始します。
12. prp-channel インターフェイスで bpdufilter を設定します。
13. （任意）LAN-A/B ポートを設定して、FORWARD モードにすばやく移行します。

手順の詳細

ステップ 1 グローバル コンフィギュレーション モードを開始します。

configure terminal

ステップ 2 PRP チャネルグループにギガビット イーサネット インターフェイスを 2 つ割り当てます。チャネル 1 の場合は、次のように入力します。

interface range GigabitEthernet1/1/0/21-22

チャネル 2 の場合は、次のように入力します。

interface range GigabitEthernet21/0/23-24

no interface prp-channel 1|2 コマンドを使用して、定義されたインターフェイスで PRP を無効にし、インターフェイスをシャットダウンします。

（注） Gi1/0/22 インターフェイスの前に Gi1/0/21 インターフェイスを適用する必要があります。シスコでは、**interface range** コマンドを使用することを推奨しています。同様に、PRP チャネル 2 の Gi1/0/24 の前に Gi1/0/23 インターフェイスを適用する必要があります。

ステップ 3 （任意）レイヤ 2 トラフィックの場合は、**switchport** と入力します。（デフォルト）：

switchport

（注） レイヤ 3 トラフィックの場合は、**no switchport** と入力します。

ステップ 4 （任意）非トランキングでタグのない、単一の VLAN レイヤ 2（アクセス）インターフェイスを設定します。

switchport mode access

ステップ 5 （任意）ギガビット イーサネット インターフェイスの VLAN を作成します。

switchport access vlan <*value*>

（注） この手順は、レイヤ 2 トラフィックにのみ必要です。

ステップ 6 （任意）スイッチで高精度時間プロトコル（PTP）を無効にします。

no ptp enable

デフォルトでは PTP が有効になっています。PTP を実行する必要がない場合は、無効にできます。

ステップ 7 冗長チャネルのループ検出を無効にします。

no keepalive

ステップ 8 冗長チャネルの UDLD を無効にします。

udld port disable

ステップ 9 サブインターフェイスモードを開始し、PRP チャネルグループを作成します。

prp-channel-group *prp-channel group*

prp-channel group：1 または 2 の値

ステップ 2 で割り当てた 2 つのインターフェイスがこのチャネルグループに割り当てられます。

このコマンドの **no** 形式はサポートされていません。

ステップ 10 PRP チャネルを起動します。

no shutdown

ステップ 11 PRP インターフェイスを指定し、インターフェイスモードを開始します。

interface prp-channel *prp-channel-number*

prp-channel-number：1 または 2 の値

ステップ 12 prp-channel インターフェイスで bpdufilter を設定します。

spanning-tree bpdufilter enable

スパニングツリー BPDU フィルタは、すべての入力および出力 BPDU トラフィックをドロップします。このコマンドは、ネットワーク内に独立したスパニングツリードメイン（ゾーン）を作成するために必要です。

ステップ 13 （任意）LAN-A/B ポートを設定して、FORWARD モードにすばやく移行します。

spanning-tree portfast edge trunk

この項はオプションですが、強く推奨されます。これにより、PRP RedBox と LAN-A および LAN-B スイッチエッジポートでのスパニング ツリー コンバージェンス時間が改善されます。また、RedBox PRP インターフェイスに直接接続されている LAN_A/LAN_B ポートでこのコマンドを設定することを強くお勧めします。

例

次に、PRPチャネルを作成する方法、PRPチャネルグループを作成する方法、そのグループに 2 つのポートを割り当てる方法の例を示します。

```
switch# configure terminal
switch(config)# interface range GigabitEthernet1/0/21-22
switch(config-if)# no keepalive
switch(config-if)# udld port disable
switch(config-if)# prp-channel-group 1
switch(config-if)# no shutdown
switch(config-if)# exit
switch(config)# interface prp-channel 1
switch(config)# spanning-tree bpdufilter enable
```

```
switch# configure terminal
switch(config)# interface range GigabitEthernet1/0/21-22
switch(config-if)# switchport
switch(config-if)# switchport mode access
switch(config-if)# switchport access vlan 2
switch(config-if)# no ptp enable
```

```
switch(config-if)# no keepalive
switch(config-if)# udld port disable
switch(config-if)# prp-channel-group 1
switch(config-if)# no shutdown
switch(config-if)# exit
switch(config)# interface prp-channel 1
switch(config)# spanning-tree bpdufilter enable
```

次に、レイヤ 3 で設定されたスイッチで PRP チャネルを作成する方法の例を示します。

```
switch# configure terminal
switch(config)# interface range GigabitEthernet1/0/21-22
switch(config-if)# no switchport
switch(config-if)# no ptp enable
switch(config-if)# no keepalive
switch(config-if)# udld port disable
switch(config-if)# prp-channel-group 1
switch(config-if)# no shutdown
switch(config-if)# exit
switch(config)# interface prp-channel 1
switch(config)# spanning-tree bpdufilter enable
switch(config)# ip address 192.0.0.2 255.255.255.0
```

監視フレームの VLAN タギングを使用した PRP チャネルの設定

VLAN タグ付き監視フレームを使用したスイッチで PRP チャネルおよびグループを作成して有効にするには、次の手順に従います。

始める前に

- PRP チャネル （3 ページ）の説明に従って、各スイッチタイプでサポートされている特定のインターフェイスを確認します。
- 前提条件 （5 ページ）と注意事項と制約事項 （6 ページ）を確認してください。
- PRP チャネルを作成する前に、PRP チャネルのメンバーインターフェイスが、FlexLinks、EtherChannel、REP などの冗長プロトコルに参加していないことを確認します。

手順の概要

1. グローバル コンフィギュレーション モードを開始します。
2. PRP チャネルグループにギガビット イーサネット インターフェイスを 2 つ割り当てます。チャネル 1 の場合は、次のように入力します。
3. インターフェイスが複数の VLAN のトラフィックを伝送できるように、PRP インターフェイスをトランク管理モードに設定します。
4. トランクインターフェイスの許可 VLAN を設定します。
5. （任意）スイッチで高精度時間プロトコル（PTP）を無効にします。
6. 冗長チャネルのループ検出を無効にします。

7. 冗長チャネルの UDLD を無効にします。
8. サブインターフェイスモードを開始し、PRP チャネルグループを作成します。
9. PRP チャネルを起動します。
10. PRP インターフェイスを指定し、インターフェイスモードを開始します。
11. prp-channel インターフェイスで bpdufilter を設定します。
12. 監視フレームの VLAN タグで使用する VLAN ID を設定します。
13. （任意）監視フレームの VLAN タグに設定するサービスクラス（COS）値を設定します。
14. インターフェイスの VLAN タギングを有効にします。
15. （任意）LAN-A/B ポートを設定して、FORWARD モードにすばやく移行します。

手順の詳細

ステップ 1 グローバル コンフィギュレーション モードを開始します。

configure terminal

ステップ 2 PRP チャネルグループにギガビット イーサネット インターフェイスを 2 つ割り当てます。チャネル 1 の場合は、次のように入力します。

interface range {{GigabitEthernet1/0/21-22}

チャネル 2 の場合は、次のように入力します。

interface range {{GigabitEthernet1/0/23-24}

no interface prp-channel 1|2 コマンドを使用して、定義されたインターフェイスで PRP を無効にし、インターフェイスをシャットダウンします。

（注） Gi1/0/22 インターフェイスの前に Gi1/0/21 インターフェイスを適用する必要があります。シスコでは、**interface range** コマンドを使用することを推奨しています。同様に、PRP チャネル 2 の Gi1/0/24 の前に Gi1/0/23 インターフェイスを適用する必要があります。

ステップ 3 インターフェイスが複数の VLAN のトラフィックを伝送できるように、PRP インターフェイスをトランク管理モードに設定します。

switchport mode trunk

ステップ 4 トランクインターフェイスの許可 VLAN を設定します。

switchport trunk allowed vlan *value*

value：許可される 0 ～ 4095 の VLAN 番号、またはカンマで区切られた VLAN のリスト。

ステップ 5 （任意）スイッチで高精度時間プロトコル（PTP）を無効にします。

no ptp enable

デフォルトでは PTP が有効になっています。PTP を実行する必要がない場合は、無効にできます。

ステップ 6 冗長チャネルのループ検出を無効にします。

no keepalive

ステップ 7 冗長チャネルの UDLD を無効にします。

udld port disable

ステップ 8 サブインターフェイスモードを開始し、PRP チャネルグループを作成します。

prp-channel-group *prp-channel group*

prp-channel group：1 または 2 の値

ステップ 2 で割り当てた 2 つのインターフェイスがこのチャネルグループに割り当てられます。

このコマンドの **no** 形式はサポートされていません。

ステップ 9 PRP チャネルを起動します。

no shutdown

ステップ 10 PRP インターフェイスを指定し、インターフェイスモードを開始します。

interface prp-channel *prp-channel-number*

prp-channel-number：1 または 2 の値

ステップ 11 prp-channel インターフェイスで bpdufilter を設定します。

spanning-tree bpdufilter enable

スパニングツリー BPDU フィルタは、すべての入出力 BPDU トラフィックをドロップします。このコマンドは、ネットワーク内に独立したスパニングツリードメイン（ゾーン）を作成するために必要です。

ステップ 12 監視フレームの VLAN タグで使用する VLAN ID を設定します。

prp channel-group *prp-channel-number* **supervisionFrameOption vlan-id** *value*

prp-channel-number：1 または 2 の値

value：0 ～ 4095 の VLAN 番号

ステップ 13 （任意）監視フレームの VLAN タグに設定するサービスクラス（COS）値を設定します。

prp channel-group *prp-channel-number* **supervisionFrameOption vlan-cos** *value*

value：1 ～ 7 で指定します。デフォルトは 1 です。

ステップ 14 インターフェイスの VLAN タギングを有効にします。

prp channel-group *prp-channel-number* **supervisionFrameOption vlan-tagged** *value*

prp-channel-number：1 または 2 の値

ステップ 15 （任意）LAN-A/B ポートを設定して、FORWARD モードにすばやく移行します。

spanning-tree portfast edge trunk

この項はオプションですが、強く推奨されます。これにより、PRP RedBox と LAN-A および LAN-B スイッチエッジポートでのスパニング ツリー コンバージェンス時間が改善されます。また、RedBox PRP

インターフェイスに直接接続されている LAN_A/LAN_B ポートでこのコマンドを設定することを強く推奨します。

例

```
REDBOX1# configure terminal
REDBOX1(config)#int range GigabitEthernet1/0/21-22
REDBOX1(config-if)#switchport mode trunk
REDBOX1(config-if)#switchport trunk allowed vlan 10,20
REDBOX1(config-if)# no ptp enable
REDBOX1(config-if)# no keepalive
REDBOX1(config-if)# udld port disable
REDBOX1(config-if)# no shutdown
REDBOX1(config-if)# prp-channel-group 1
REDBOX1(config-if)# exit
REDBOX1(config)#prp channel-group 1 supervisionFrameOption vlan-tagged
REDBOX1(config)#prp channel-group 1 supervisionFrameOption vlan-id 10
REDBOX1(config)# spanning-tree bpdufilter enable
REDBOX1(config-if)#spanning-tree portfast edge trunk
```

スタティックエントリをノードテーブルと VDAN テーブルに追加する

ノードテーブルまたはVDANテーブルにスタティックエントリを追加するには、このセクションの手順に従います。

手順の概要

1. グローバル コンフィギュレーション モードを開始します。
2. チャネルグループのノードテーブルに追加するMACアドレスを指定し、ノードがDANであるかSAN（LAN-A または LAN-B のいずれかに接続）であるかを指定します。
3. VDAN テーブルに追加する MAC アドレスを指定します。

手順の詳細

ステップ 1 グローバル コンフィギュレーション モードを開始します。

configure terminal

例：

```
switch# configure terminal
switch(config-if)# prp channel-group 1 nodeTableMacaddress 0000.0000.0001 lan-a
```

ステップ 2 チャネルグループのノードテーブルに追加する MAC アドレスを指定し、ノードが DAN であるか SAN（LAN-A または LAN-B のいずれかに接続）であるかを指定します。

prp channel-group *prp-channel group* **nodeTableMacaddress** *mac-address* {dan | lan-a | lan-b}

prp-channel group：1 または 2 の値

mac-address：ノードの MAC アドレス

（注）　エントリを削除するには、コマンドの **no** 形式を使用します。

ステップ 3 VDAN テーブルに追加する MAC アドレスを指定します。

prp channel-group *prp-channel group* **vdanTableMacaddress** *mac-address*

prp-channel group：1 または 2 の値

mac-address：ノードまたは VDAN の MAC アドレス

（注）　エントリを削除するには、コマンドの **no** 形式を使用します。

すべてのノードテーブルと VDAN テーブルのダイナミックエントリのクリア

手順の概要

1. 次のコマンドを入力して、ノードテーブル内のダイナミックエントリをすべてクリアします。
2. 次のコマンドを入力して、VDANテーブル内のダイナミックエントリをすべてクリアします。

手順の詳細

ステップ 1 次のコマンドを入力して、ノードテーブル内のダイナミックエントリをすべてクリアします。

clear prp node-table [**channel-group** *group*]

ステップ 2 次のコマンドを入力して、VDAN テーブル内のダイナミックエントリをすべてクリアします。

clear prp vdan-table [**channel-group** *group*]

チャネルグループを指定しない場合は、すべての PRP チャネルグループでダイナミックエントリがクリアされます。

（注） **clear prp node-table** コマンドと **clear prp vdan-table** コマンドは、ダイナミックエントリのみをクリアします。スタティックエントリをクリアするには、スタティックエントリをノードテーブルと VDAN テーブルに追加する （15 ページ）に表示される **nodeTableMacaddress** コマンドまたは **vdanTableMacaddress** コマンドの **no** 形式を使用します。

PRP チャネルおよびグループの無効化

手順の概要

1. グローバル コンフィギュレーション モードを開始します。
2. PRP チャネルを無効にします。
3. インターフェイス モードを終了します。

手順の詳細

ステップ 1 グローバル コンフィギュレーション モードを開始します。

configure terminal

ステップ 2 PRP チャネルを無効にします。

no interface prp-channel *prp-channel-number*

prp-channel-number：1 または 2 の値

ステップ 3 インターフェイス モードを終了します。

exit

Syslog のエラーおよび警告メッセージ

エラーと警告が syslog になるように IE-9320-26S2C-A、IE-9320-26S2C-E、IE-9320-22S2C4X-A、および IE-9320-22S2C4X-A スイッチを設定できます。この設定により、syslog を Simple Network Management Protocol（SNMP）トラップに変換して、適切なアラートとメンテナンスを行うことができます。

次のエラーと警告を、syslog になるように設定できます。

- 不正な LAN ID A

  ポート A で受信した、不正な LAN 識別子を持つフレームの数。

- 不正な LAN ID B

ポート B で受信した、不正な LAN 識別子を持つフレームの数。

- LAN A の警告

  LAN A の PRP ポートに潜在的な問題があります（パケット損失状態/不正な LAN パケット数の増加）。
- LAN B の警告

  LAN B の PRP ポートに潜在的な問題があります（パケット損失状態/不正な LAN パケット数の増加）。
- パケット A のサイズ超過
- パケット B のサイズ超過

手順リストのパラメータは、CLI コマンド **sh prp statistics ingressPacketStatistics** の出力からキャプチャされます。

CLI コマンドを使用して、syslog が生成される間隔を 60 ～ 84,400 秒の範囲で設定します。デフォルトは 300 秒です。詳細については、このガイドのPRP ロギング間隔の設定 （18 ページ）のセクションを参照してください。

PRP ロギング間隔の設定

エラーと警告から PRP syslog を作成するためのロギング間隔を設定するには、次の手順を実行します。デフォルトは 300 秒ですが、60 ～ 84,400 秒の間で値を選択することも可能です。

始める前に

コンフィギュレーション プロンプトで、次のコマンドを入力します。**prp logging-interval *interval_in_seconds***

デフォルトの間隔である 300 秒を選択する場合は、値を入力しないでください。デフォルトの 300 秒以外のロギング間隔を指定する場合は、値を 1 つだけ入力します。

例：

```
cl_2011#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
cl_2011(config)#prp logging-interval 120
```

スイッチは、Syslog のエラーおよび警告メッセージ （17 ページ）セクションに記載されている PRP エラーと警告から syslog を生成します。

例

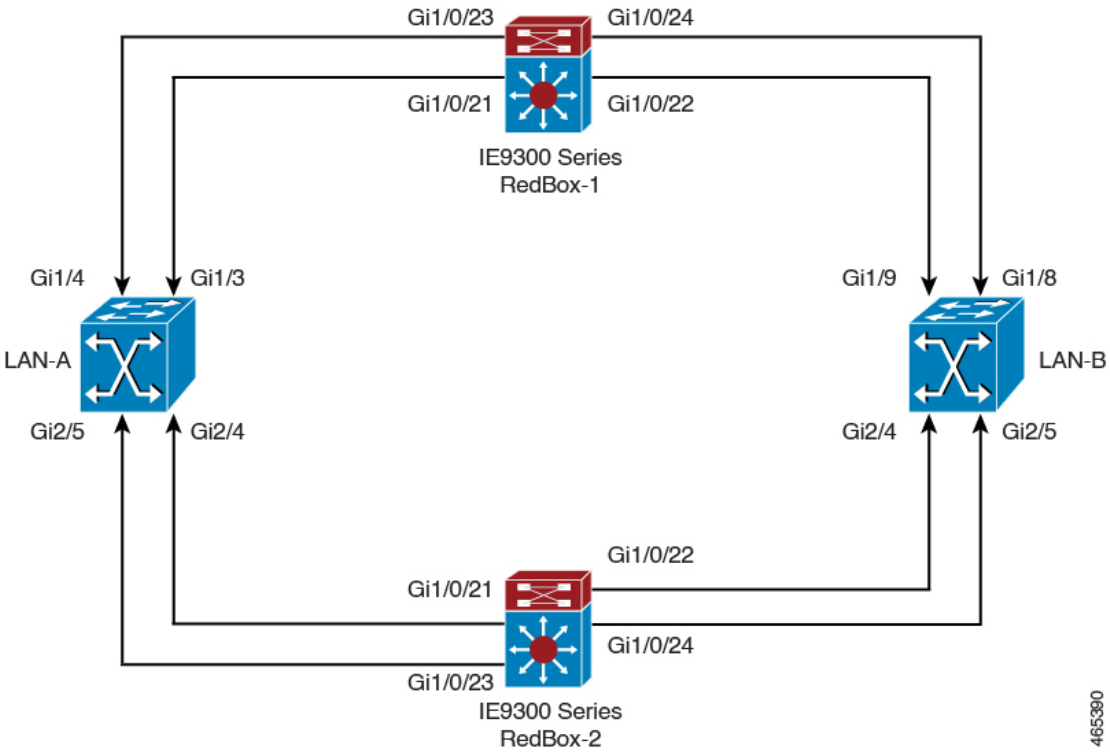
次のテキストは、ロギング間隔を設定した結果の出力例を示しています。

```
*Sep 28 13:18:27.623: %PRP_WRONG_LAN-5-WRONG_LAN: PRP channel 2, LAN A is connected to
LAN B on its peer
```

```
*Sep 28 13:18:27.623: %PRP_WRONG_LAN-5-WRONG_LAN: PRP channel 2, LAN B is connected to
LAN A on its peer
*Sep 28 13:18:27.623: %PRP_WARN_LAN-5-WARN_LAN: PRP channel 2, PRP LAN warning is set
on LAN B
*Sep 28 13:18:27.623: %PRP_OVERSIZE_PKT-5-OVERSIZE_LAN: PRP channel 2, PRP oversize
packet warning is set on LAN A
```

設定例

次の図は、Cisco Catalyst IE9300 高耐久性シリーズ スイッチが動作する可能性のあるネットワーク構成を示しています。この例のコマンドでは、その構成をサポートする機能とスイッチの設定を強調表示しています。



この例では、2 つの LAN（LAN-A と LAN-B）、および 2 つの PRP チャネルを設定します。トポロジ内では、Cisco Catalyst IE9300 高耐久性シリーズ スイッチが RedBox-1 として識別され、もう 1 つの Cisco Catalyst IE9300 高耐久性シリーズ スイッチが RedBox-2 として識別されます。

次に、LAN-A の設定を示します。

```
diagnostic bootup level minimal
!
!
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
memory free low-watermark processor 88589
!
```

```
!
alarm-profile defaultPort
 alarm not-operating
 syslog not-operating
 notifies not-operating
!
!
!
transceiver type all
 monitoring
vlan internal allocation policy ascending
!
!
!
!
!
!
!
!
!
!
!
!
!
!
interface GigabitEthernet1/1
 shutdown
!
interface GigabitEthernet1/2
 shutdown
!
interface GigabitEthernet1/3
 shutdown
!
interface GigabitEthernet1/4
 switchport access vlan 25
 switchport mode access
!
interface GigabitEthernet1/5
 switchport access vlan 35
 switchport mode access
!
interface GigabitEthernet1/6
 shutdown
!
interface GigabitEthernet1/7
 shutdown
!
interface GigabitEthernet1/8
 shutdown
!
interface GigabitEthernet1/9
 shutdown
!
interface GigabitEthernet1/10
 shutdown
!
interface AppGigabitEthernet1/1
!
interface GigabitEthernet2/1
 shutdown
!
interface GigabitEthernet2/2
 shutdown
```

```
!
interface GigabitEthernet2/3
 shutdown
!
interface GigabitEthernet2/4
 switchport access vlan 25
 switchport mode access
!
interface GigabitEthernet2/5
 switchport access vlan 35
 switchport mode access
!
interface GigabitEthernet2/6
 shutdown
!
interface GigabitEthernet2/7
 shutdown
!
interface GigabitEthernet2/8
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan35
 no ip address
!
interface Vlan25
 no ip address
```

LAN-B の設定を次に示します。

```
diagnostic bootup level minimal
!
!
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
memory free low-watermark processor 88589
!
!
alarm-profile defaultPort
 alarm not-operating
 syslog not-operating
 notifies not-operating
!
!
!
transceiver type all
 monitoring
vlan internal allocation policy ascending
!
!
!
!
!
!
!
!
!
!
!
!
```

```
!
!
interface GigabitEthernet1/1
 shutdown
!
interface GigabitEthernet1/2
 shutdown
!
interface GigabitEthernet1/3
 shutdown
!
interface GigabitEthernet1/4
 shutdown
!
interface GigabitEthernet1/5
 shutdown
!
interface GigabitEthernet1/6
 shutdown
!
interface GigabitEthernet1/7
 shutdown
!
interface GigabitEthernet1/8
 switchport access vlan 25
 switchport mode access
 shutdown
!
interface GigabitEthernet1/9
 switchport access vlan 35
 switchport mode access
!
interface GigabitEthernet1/10
 shutdown
!
interface AppGigabitEthernet1/1
!
interface GigabitEthernet2/1
 shutdown
!
interface GigabitEthernet2/2
 shutdown
!
interface GigabitEthernet2/3
 shutdown
!
interface GigabitEthernet2/4
 switchport access vlan 35
 switchport mode access
!
interface GigabitEthernet2/5
 switchport access vlan 25
 switchport mode access
!
interface GigabitEthernet2/6
 shutdown
!
interface GigabitEthernet2/7
 shutdown
!
interface GigabitEthernet2/8
 shutdown
!
interface Vlan1
```

```
 no ip address
 shutdown
!
interface Vlan35
 no ip address
!
interface Vlan25
 no ip address
```

RedBox-1 の設定は次のとおりです。

```
!
!
spanning-tree mode rapid-pvst
no spanning-tree etherchannel guard misconfig
spanning-tree extend system-id
memory free low-watermark processor 88589
!
!
alarm-profile defaultPort
 alarm not-operating
 syslog not-operating
 notifies not-operating
!
prp channel-group 1 supervisionFrameOption vlan-id 35
prp channel-group 1 supervisionFrameTime 25000
prp channel-group 1 supervisionFrameLifeCheckInterval 8500
prp channel-group 1 supervisionFrameRedboxMacaddress 34c0.f9e5.59ba
prp channel-group 2 supervisionFrameOption vlan-id 25
prp channel-group 2 supervisionFrameTime 9834
prp channel-group 2 supervisionFrameLifeCheckInterval 12345
prp channel-group 2 passRCT!
!
transceiver type all
 monitoring
vlan internal allocation policy ascending
!
!
!
!
!
!
!
!
!
!
!
!
!
!
interface PRP-channel1
 switchport access vlan 35
 switchport mode access
 spanning-tree bpdufilter enable
!
interface PRP-channel2
 switchport access vlan 25
 switchport mode access
 spanning-tree bpdufilter enable
!
interface GigabitEthernet1/0/21
 switchport access vlan 35
 switchport mode access
 no ptp enable
 udld port disable
```

```
 no keepalive
 prp-channel-group 1
 spanning-tree bpdufilter enable
!
interface GigabitEthernet1/0/22
 switchport access vlan 35
 switchport mode access
 no ptp enable
 udld port disable
 no keepalive
 prp-channel-group 1
!
interface GigabitEthernet1/0/23
 switchport access vlan 25
 no ptp enable
 prp-channel-group 2
 spanning-tree bpdufilter enable
!
interface GigabitEthernet1/0/24
switchport access vlan 25
no ptp enable
prp-channel-group 2
spanning-tree bpdufilter enable

!
interface AppGigabitEthernet1/1
!
interface GigabitEthernet1/0/23
 switchport access vlan 25
 switchport modeaccess
 no ptp enable
 udld port disable
 no keepalive
 prp-channel-group 2
 spanning-tree bpdufilter enable
!
interface GigabitEthernet1/0/24
 switchport access vlan 25
 switchport mode access
 no ptp enable
 udld port disable
 no keepalive
 prp-channel-group 2
 spanning-tree bpdufilter enable

!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan35
 ip address 35.35.35.1 255.255.255.0
!
interface Vlan25
 ip address 25.25.25.1 255.255.255.0
!
interface Vlan100
 ip address 15.15.15.149 255.255.255.0
!
ip http server
ip http authentication local
ip http secure-server
ip forward-protocol nd
!
```

```
ip tftp source-interface Vlan100
ip tftp blocksize 8192
!
```

RedBox-2 の設定は次のとおりです。

```
!
spanning-tree mode rapid-pvst
no spanning-tree etherchannel guard misconfig
spanning-tree extend system-id
memory free low-watermark processor 88589
!
!
alarm-profile defaultPort
 alarm not-operating
 syslog not-operating
 notifies not-operating
!
prp channel-group 1 supervisionFrameOption vlan-id 35
prp channel-group 1 supervisionFrameTime 776
prp channel-group 1 supervisionFrameLifeCheckInterval 15000
prp channel-group 1 passRCT
prp channel-group 2 supervisionFrameOption vlan-id 25
prp channel-group 2 supervisionFrameTime 9834
prp channel-group 2 supervisionFrameLifeCheckInterval 12345
prp channel-group 2 passRCT

!
!
!
transceiver type all
 monitoring
vlan internal allocation policy ascending
lldp run
!
!
!
!
!
!
!
!
!
!
!
!
!
interface PRP-channel1
 switchport access vlan 35
 switchport mode access
 spanning-tree bpdufilter enable
!
interface PRP-channel2
 switchport access vlan 25
 switchport mode access
 spanning-tree bpdufilter enable
!
interface GigabitEthernet1/1
 shutdown
!
interface GigabitEthernet1/2
 shutdown
!
```

```
interface GigabitEthernet1/0/21
 switchport access vlan 35
 switchport mode access
 no ptp enable
 udld port disable
 no keepalive
 prp-channel-group 1
 spanning-tree bpdufilter enable
!
interface GigabitEthernet1/0/22
 switchport access vlan 35
 switchport mode access
 no ptp enable
 udld port disable
 no keepalive
 prp-channel-group 1
 spanning-tree bpdufilter enable
!
interface GigabitEthernet1/5
!
interface GigabitEthernet1/6
 description **** tftp connection ****
 switchport access vlan 100
 switchport mode access
 shutdown
!
interface GigabitEthernet1/7
!
interface GigabitEthernet1/8
!
interface GigabitEthernet1/0/23
 description *** PRP 2 channel *****
 switchport access vlan 25
 switchport mode access
 no ptp enable
 no keepalive
 prp-channel-group 2
 spanning-tree bpdufilter enable
!
interface GigabitEthernet1/0/24
 description *** PRP 2 channel *****
 switchport access vlan 25
 switchport mode access
 no ptp enable
 no keepalive
 prp-channel-group 2
 spanning-tree bpdufilter enable
!
interface AppGigabitEthernet1/1
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan35
 ip address 35.35.35.2 255.255.255.0
!
interface Vlan25
 ip address 25.25.25.2 255.255.255.0
!
interface Vlan100
 ip address 15.15.15.169 255.255.255.0
!
ip http server
```

```
ip http authentication local
ip http secure-server
ip forward-protocol nd
!
ip tftp source-interface Vlan100
ip tftp blocksize 8192
!
!
!
```

VLAN タギングの例

次に、監視フレームの VLAN タギング用に設定された PRP チャネルインターフェイスを使用するスイッチの設定例を示します。

```
PRP_IE9300#sh running-config
Building configuration...

Current configuration : 8171 bytes
!
! Last configuration change at 05:19:31 PST Mon Mar 22 2021
!
version 17.5
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service call-home
no platform punt-keepalive disable-kernel-core
no platform punt-keepalive settings
no platform bridge-security all
!
hostname PRP_IE9300
!
!
no logging console
enable password Cisco123
!
no aaa new-model
clock timezone PST -8 0
rep bpduleak
ptp mode e2etransparent
!
!
!
!
!
!
!
ip dhcp pool webuidhcp
   cip instance 1
!
!
!
login on-success log
!
!
!
crypto pki trustpoint SLA-TrustPoint
 enrollment pkcs12
 revocation-check crl
!
crypto pki trustpoint TP-self-signed-559094202
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-559094202
```

```
 revocation-check none
 rsakeypair TP-self-signed-559094202
!
!
!
diagnostic bootup level minimal
!
!
!
spanning-tree mode rapid-pvst
no spanning-tree etherchannel guard misconfig
spanning-tree extend system-id
memory free low-watermark processor 89983
!
!
alarm-profile defaultPort
 alarm not-operating
 syslog not-operating
 notifies not-operating
!
prp channel-group 1 supervisionFrameOption vlan-tagged
prp channel-group 1 supervisionFrameOption vlan-id 30
prp channel-group 1 supervisionFrameTime 500
prp channel-group 1 supervisionFrameLifeCheckInterval 24907
prp channel-group 1 supervisionFrameRedboxMacaddress ecce.13eb.71a2
prp channel-group 2 supervisionFrameOption vlan-tagged
prp channel-group 2 supervisionFrameOption vlan-id 40
prp channel-group 2 supervisionFrameTime 0
prp channel-group 2 supervisionFrameLifeCheckInterval 0
prp channel-group 2 supervisionFrameRedboxMacaddress f8b7.e2e5.c1f9
!
!
!
transceiver type all
 monitoring
vlan internal allocation policy ascending
lldp run
!
!
!
!
!
!
!
!
!
!
!
!
!
!
interface PRP-channel1
 switchport mode trunk
 switchport trunk allowed vlan 30,40

 spanning-tree bpdufilter enable
!
interface PRP-channel2
 switchport mode trunk
 switchport trunk allowed vlan 30,40
 no keepalive
 spanning-tree bpdufilter enable
!
interface GigabitEthernet1/0/21
```

```
 switchport mode trunk
 switchport trunk allowed vlan 30,40
 no ptp enable
 udld port disable
 no keepalive
 prp-channel-group 1
 spanning-tree bpdufilter enable
!
interface GigabitEthernet1/0/22
 switchport mode trunk
 switchport trunk allowed vlan 30,40
 no ptp enable
 udld port disable
 no keepalive
 prp-channel-group 1
 spanning-tree bpdufilter enable

!
interface AppGigabitEthernet1/1
!
interface GigabitEthernet1/0/23
 switchport mode trunk
 switchport trunk allowed vlan 30,40
 no ptp enable
 udld port disable
 no keepalive
 prp-channel-group 2
 spanning-tree bpdufilter enable
!
interface GigabitEthernet1/0/24
 switchport mode trunk
 switchport trunk allowed vlan 30,40
 no ptp enable
 udld port disable
 no keepalive
 prp-channel-group 2
 spanning-tree bpdufilter enable
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan30
 ip address 30.30.30.1 255.255.255.0
!
interface Vlan40
 ip address 40.40.40.1 255.255.255.0
!
interface Vlan197
 ip address 9.4.197.30 255.255.255.0
!
ip http server
ip http authentication local
ip http secure-server
ip forward-protocol nd
!
ip tftp source-interface Vlan197
ip tftp blocksize 8192
!
!
!
!
!
!
```

```
control-plane
!
!
line con 0
 exec-timeout 0 0
 stopbits 1
line aux 0
line vty 0 4
 login
 transport input ssh
line vty 5 15
 login
 transport input ssh
!
call-home
 ! If contact email address in call-home is configured as sch-smart-licensing@cisco.com
 ! the email address configured in Cisco Smart License Portal will be used as contact
email address to send SCH notifications.
 contact-email-addr sch-smart-licensing@cisco.com
 profile "CiscoTAC-1"
  active
  destination transport-method http
!
!
!
!
!
!
!
!
!
!
!
end

PRP_IE9300#
```

設定の確認

ここでは、PRPの設定を確認するために使用できるコマンドと、それらのコマンドの例を示します。

コマンド	目的
show prp channel {**1** | **2** [**detail** | **status** | **summary**] | **detail** | **status** | **summary**}	指定したPRPチャネルに対する設定の詳細を表示します。
show prp control {**VdanTableInfo** | **ptpLanOption** | **ptpProfile** | **supervisionFrameLifeCheckInterval** | **supervisionFrameOption** | **supervisionFrameRedboxMacaddress** | **supervisionFrameTime**}	PRPの制御情報、VDANテーブル、および監視フレームに関する情報を表示します。
show prp node-table [**channel-group** <**group**> | **detail**]	PRPノードテーブルを表示します。

コマンド	目的
show prp statistics {**egressPacketStatistics** | **ingressPacketStatistics** | **nodeTableStatistics** | **pauseFrameStatistics** | **ptpPacketStatistics**}	PRP コンポーネントの統計情報が表示されます。
show prp vdan-table [**channel-group** <**group**> | **detail**]	PRP VDAN テーブルを表示します。
show interface prp-channel {**1** | **2**}	PRP メンバーのインターフェイスに関する情報を表示します。

（注） カウンタ情報は誤解を招く可能性があるため、これらのインターフェイスが PRP チャネルメンバーである場合は、**show interface G1/0/21** コマンドまたは **show interface G1/0/22** コマンドを使用して PRP 統計情報を読み取らないでください。代わりに、**show interface prp-channel** [**1** | **2**] コマンドを使用します。

次の例は、PRP チャネルのインターフェイスの 1 つがダウンしている場合の、**show prp channel** の出力を示しています。

```
show prp channel 2 detail
PRP-channel: PR2
------------
Layer type = L2
Ports: 2 Maxports = 2
Port state = prp-channel is Inuse
Protocol = Enabled
Ports in the group:
1) Port: Gi1/0/23
Logical slot/port = 1/0/23 Port state = Inuse
Protocol = Enabled
2) Port: Gi1/0/24
Logical slot/port = 1/0/24 Port state = Not-Inuse (link down)
Protocol = Enabled
```

次に、PRP ノードテーブルおよび PRP VDAN テーブルを表示する方法の例を示します。

```
Switch#show prp node-table
PRP Channel 1 Node Table
==================================
   Mac Address   Type  Dyn   TTL
---------------- ----- --- --------
 B0AA.7786.6781  lan-a  Y     59
 F454.3317.DC91  dan    Y     60
==================================
Channel 1 Total Entries: 2
Switch#show prp vdan-table
PRP Channel 1 VDAN Table
============================
   Mac Address   Dyn   TTL
---------------- --- -------
 F44E.05B4.9C81   Y     60
============================
Channel 1 Total Entries: 1
```

次に、PRP チャネルに VLAN タギングを追加した場合と追加しない場合の、**show prp control supervisionFrameOption** コマンドの出力例を示します。`VLAN value` フィールドの 1 は VLAN タギングが有効であることを意味し、値 0 は VLAN タギングが無効であることを意味します。

```
REDBOX1#show prp control supervisionFrameoption
 PRP channel-group 1 Super Frame Option
  COS value is 7
  CFI value is 0
  VLAN value is 1
  MacDA value is 200
  VLAN id value is 30
PRP channel-group 2 Super Frame Option
  COS value is 0
  CFI value is 0
  VLAN value is 0
  MacDA value is 0
  VLAN id value is 0

REDBOX1#
```

次に、エラーと警告が syslog になるようにスイッチが設定されているかどうかを判断するコマンドの例を示します。

```
switch #sh prp control logging-interval
 PRP syslog logging interval is not configured
```

次に、ロギング間隔をデフォルトの 300 秒に設定するコマンドの例を示します。

```
switch #conf t
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)#prp logging-interval
switch(config)#do sh prp control logging-interval
 PRP syslog logging interval is 300 in seconds
```

次に、ロギング間隔を 600 秒に設定するコマンドの例を示します。

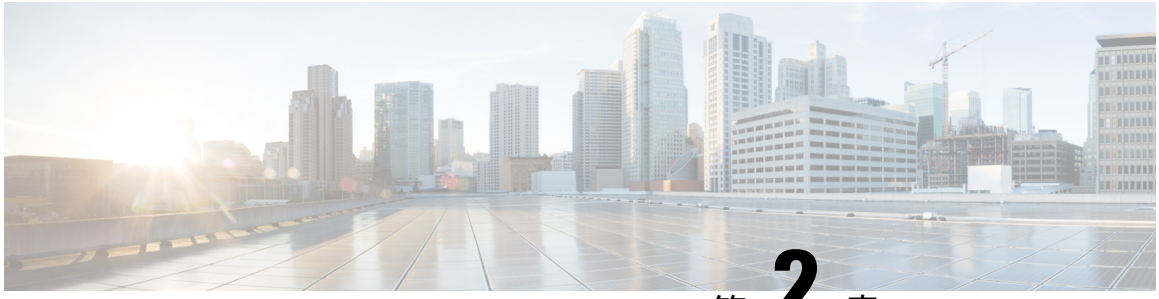
```
switch(config)#prp logging-interval 600
 PRP syslog logging interval is 600 in seconds

switch(config)#
```

関連資料

リリースノート、インストール手順、およびコンフィギュレーション ガイドを含むその他ドキュメントは、cisco.com の『Cisco Catalyst IE9300 Rugged Series Switches』ページで入手できます。

機能の履歴

リリース	機能名	機能情報
Cisco IOS XE Dublin 17.12.1	Parallel Redundancy Protocol	この機能は、Cisco Catalyst IE9300 高耐久性シリーズ スイッチ の IE-9320-22S2C4X-A および IE-9320-22S2C4X-A で使用可能になりました。
	PRP を介した PTP	この機能は、Cisco Catalyst IE9300 高耐久性シリーズ スイッチ の IE-9320-22S2C4X-A および IE-9320-22S2C4X-A で使用可能になりました。
Cisco IOS XE Cupertino 17.9.1	PRP を介した PTP	この機能は、Cisco Catalyst IE9300 高耐久性シリーズ スイッチ の IE-9320-26S2C-A および IE-9320-26S2C-E で使用可能になりました。
Cisco IOS XE Cupertino 17.7.1	Parallel Redundancy Protocol	この機能は、Cisco Catalyst IE9300 高耐久性シリーズ スイッチ の IE-9320-26S2C-A および IE-9320-26S2C-E で使用可能になりました。



第 2 章

PRP を介した PTP

- PRP を介した PTP （35 ページ）
- サポートされる PTP のプロファイルとクロックモード （38 ページ）
- PRP RedBox のタイプ （39 ページ）
- LAN-A および LAN-B の障害検出と処理 （45 ページ）
- PRP を介した PTP の CLI コマンド （45 ページ）
- PRP を介した PTP 機能の履歴 （48 ページ）

PRP を介した PTP

高精度時間プロトコル（PTP）は、パラレル冗長プロトコル（PRP）を介して Cisco Catalyst IE9300 高耐久性シリーズ スイッチ で動作できます。この機能は、Cisco IOS XE Cupertino 17.9.1 以降の IE-9320-26S2C-A および IE-9320-26S2C-E スイッチでサポートされています。これは、Cisco IOS XE Dublin 17.12.1 以降の IE-9320-22S2C4X-A および IE-9320-22S2C4X-A スイッチでサポートされています。

PRP は、PTP の冗長性を介してハイアベイラビリティを提供します。PTP の説明については、Cisco.com の『Precision Time Protocol Configuration Guide, Cisco Catalyst IE9300 Rugged Series Switches』を参照してください。

2 つの独立したパスを介したパラレル伝送による冗長性を実現する PRP 方式は、他のトラフィックとは異なり、PTP では機能しません。フレームで発生する遅延は 2 つの LAN で同じではなく、一部のフレームは LAN を通過する際にトランスペアレントクロック（TC）で変更されます。デュアル接続ノード（DAN）は、送信元が同じであっても、両方のポートから同じ PTP メッセージを受信しません。具体的には次のとおりです。

- Sync/Follow_Up メッセージは、補正フィールドを調整するために TC によって変更されます。
- LAN に存在する境界クロック（BC）は PRP に対応しておらず、冗長制御トレーラ（RCT）が付加されていない独自のアナウンスおよび同期フレームを生成します。
- 2 ステップのクロックごとに Follow_Up フレームが生成され、RCT は伝送されません。

PRP を介した PTP

- TC は PRP に対応しておらず、ペイロードの後に続くメッセージ部分である RCT を転送する必要はありません。

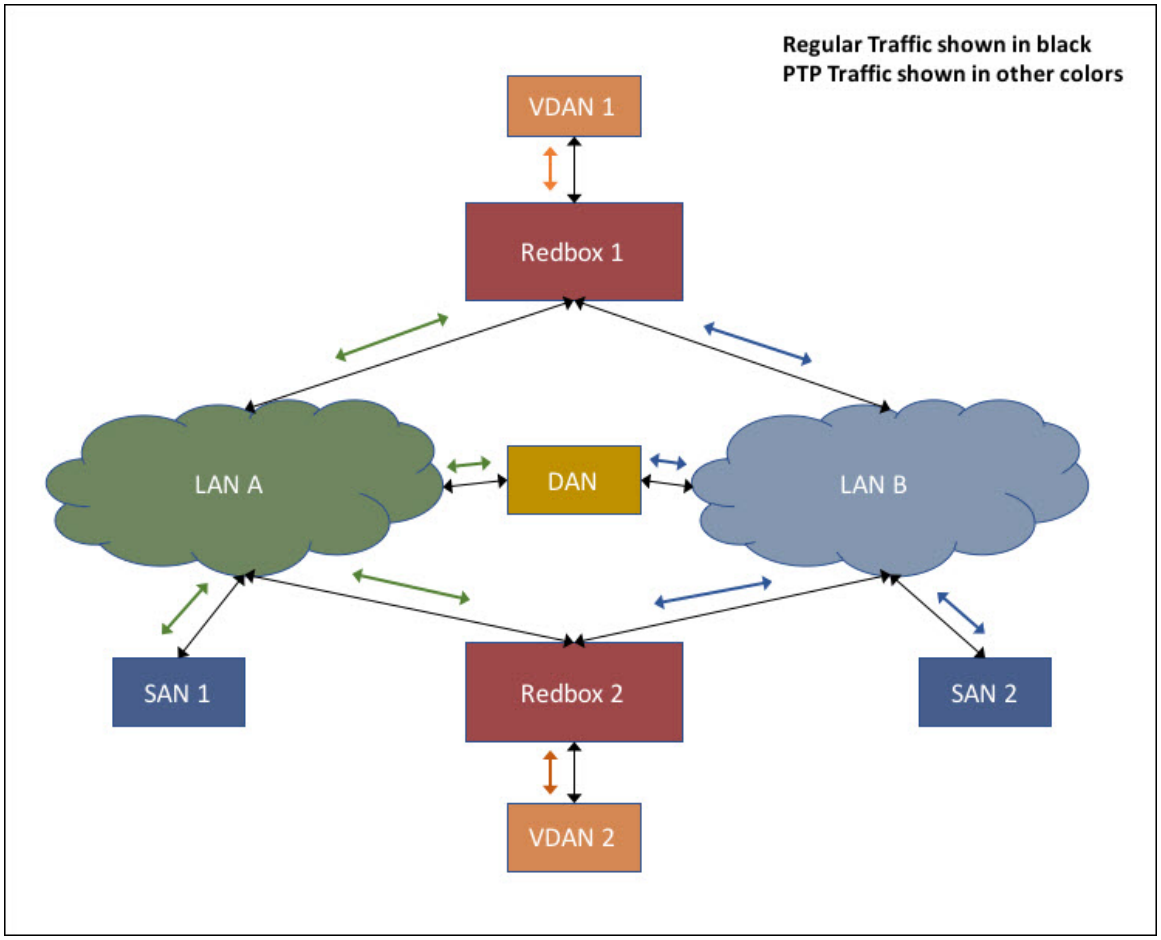
LAN-A および LAN-B を介した PTP をサポートする前は、PTP トラフィックは上記の PTP およびパラレル伝送の問題を回避するために、LAN-A でのみ許可されていました。ただし、LAN-A が停止すると、PTP 同期は失われていました。基礎となる PRP インフラストラクチャによって提供される冗長性の利点を PTP で活用できるようにするため、PRP ネットワーク上の PTP パケットは他のタイプのトラフィックとは異なる方法で処理されます。

PRP を介した PTP 機能の実装は、IEC 62439-3:2016『Industrial communication networks - High availability automation networks - Part 3: Parallel Redundancy Protocol (PRP) and High-availability Seamless Redundancy (HSR)』に詳細が示されている PRP を介した PTP の動作に基づきます。このアプローチでは、PTP パケットに RCT を付加せず、PTP パケットの PRP 重複/廃棄ロジックをバイパスすることで、上記の問題を解決します。

PRP を介した PTP のパケットフロー

次の図は、PRP を介した PTP の動作を示しています。

図 *2: PRP* を介した *PTP* のパケットフロー



PRP を介した PTP

この図では、VDAN 1 がグランドマスタークロック（GMC）です。デュアル接続デバイスは、両方の PRP ポートを介して PTP 同期情報を受信します。LAN-A ポートと LAN-B ポートは、GMC と同期された異なる仮想クロックを使用します。ただし、ローカルクロック（図では VDAN 2）を同期するために使用されるポート（図では時刻受信者）は 1 つだけです。LAN-A ポートが時刻受信者の場合、LAN-A ポートの仮想クロックが VDAN-2 の同期に使用されます。もう一方の PRP ポートである LAN-B は、PASSIVE と呼ばれます。LAN-B ポートの仮想クロックは引き続き同じ GMC に同期されますが、VDAN 2 の同期には使用されません。

LAN-A がダウンすると、LAN-B が時刻受信者の役割を引き継ぎ、RedBox 2 のローカルクロック同期を継続するために使用されます。RedBox 2 に接続された VDAN 2 は、以前と同様に RedBox 2 から PTP 同期の受信を継続します。同様に、図に示されているすべての DAN、VDAN、および RedBox も引き続き同期されます。SAN は冗長性を備えていません。この例では、LAN-A がダウンすると、SAN 1 は同期を失います。

この変更により、VDAN 2 は、LAN-A ポートの仮想クロックと LAN-B ポートの仮想クロックの間のオフセットが原因で、そのクロックに瞬間的な同期のずれが発生する場合があります。両方のクロックが同じ GMC に同期されているため、同期のずれはせいぜい数マイクロ秒です。このずれは、LAN-A ポートが時刻受信者に戻り、LAN-B ポートが PASSIVE になるときにも発生します。

（注） シスコは、従来のマスター/スレーブの命名法から移行しています。このドキュメントでは、代わりにグランドマスタークロック（GMC）または時刻源と時刻受信者という用語が使用されます。製品ソフトウェアのユーザーインターフェイスにハードコードされている言語、RFP のドキュメントに基づいて使用されている言語、または参照されているサードパーティ製品で使用されている言語によりドキュメントに例外が存在する場合があります。

サポートされる GMC の場所

GMC は、PRP を介した PTP のトポロジに次のいずれかのように配置できます。

- LAN A と LAN B の両方に接続されている RedBox（たとえば、前の図の RedBox 1）。
- VDAN（たとえば、前の図の VDAN 1）。
- DAN（たとえば、前の図の DAN）。

LAN-A または LAN-B 内のデバイスだけしか GMC と同期されないため、GMC は SAN として LAN-A または LAN-B に接続することはできません。

設定

PRP を介した PTP では、通常 PTP と PRP を個別に設定する方法以上の設定は必要ありません。また、この機能用に追加されたユーザーインターフェイスはありません。違いは、PRP を介した PTP 機能が登場する以前は、PTP が LAN-A 上でのみ機能していたことです。これが現在は両方の LAN で機能するようになりました。PRP を介した PTP を実装する前に、「注意事項と制約事項」を参照してください。

ネットワークに PRP を介した PTP を実装するためのワークフローの概要は次のとおりです。

1. PRP RedBox の場所を確認するには、このガイドの「PRP RedBox のタイプ」セクションを参照してください。PTP のモードとプロファイルに関する説明については、Cisco.com の『Precision Time Protocol Configuration Guide, Cisco Catalyst IE9300 Rugged Series Switches』を参照してください。
2. ステップ 1 で決定した PTP プロファイルを基に、Cisco.com の『Precision Time Protocol Configuration Guide, Cisco Catalyst IE9300 Rugged Series Switches』の説明に従って PTP を設定します。
3. 「PRP チャネルとグループの作成」の説明に従って、PRP を設定します。

（注） IE-9320-26S2C-A、IE-9320-26S2C-E、IE-9320-22S2C4X-A、および IE-9320-22S2C4X-A の各スイッチには、次の 4 つの PRP 対応ポートがあります。

- Gi1/0/21 および Gi1/0/22：PRP チャネル 1 に対応。
- Gi1/0/23 および Gi1/0/24：PRP チャネル 2 に対応。

サポートされる PTP のプロファイルとクロックモード

次の表に、さまざまな PTP のプロファイルとクロックモードに対する PRP を介した PTP サポートの概要を示します。サポートされていない PTP のプロファイルとクロックモードの組み合わせでは、PTP トラフィックが LAN-A のみを通過します。LAN-A は、番号の小さいインターフェイスです。PRP のインターフェイス番号については、「PRP チャネル」を参照してください。

PTP プロファイル	クロックモード	サポートの有無	IEC 62439-3 に準拠した PRP RedBox タイプ
エンドツーエンドの遅延要求/応答を示す Default プロファイル	BC	対応	E2E を使用するダブル接続 BC（DABC）としての PRP RedBox
	E2E TC	未対応	E2E を使用するダブル接続 TC（DATC）としての PRP RedBox
Power プロファイル	BC	対応	P2P を使用するダブル接続 BC（DABC）としての PRP RedBox
	P2P TC	対応	P2P を使用するダブル接続 TC（DATC）としての PRP RedBox

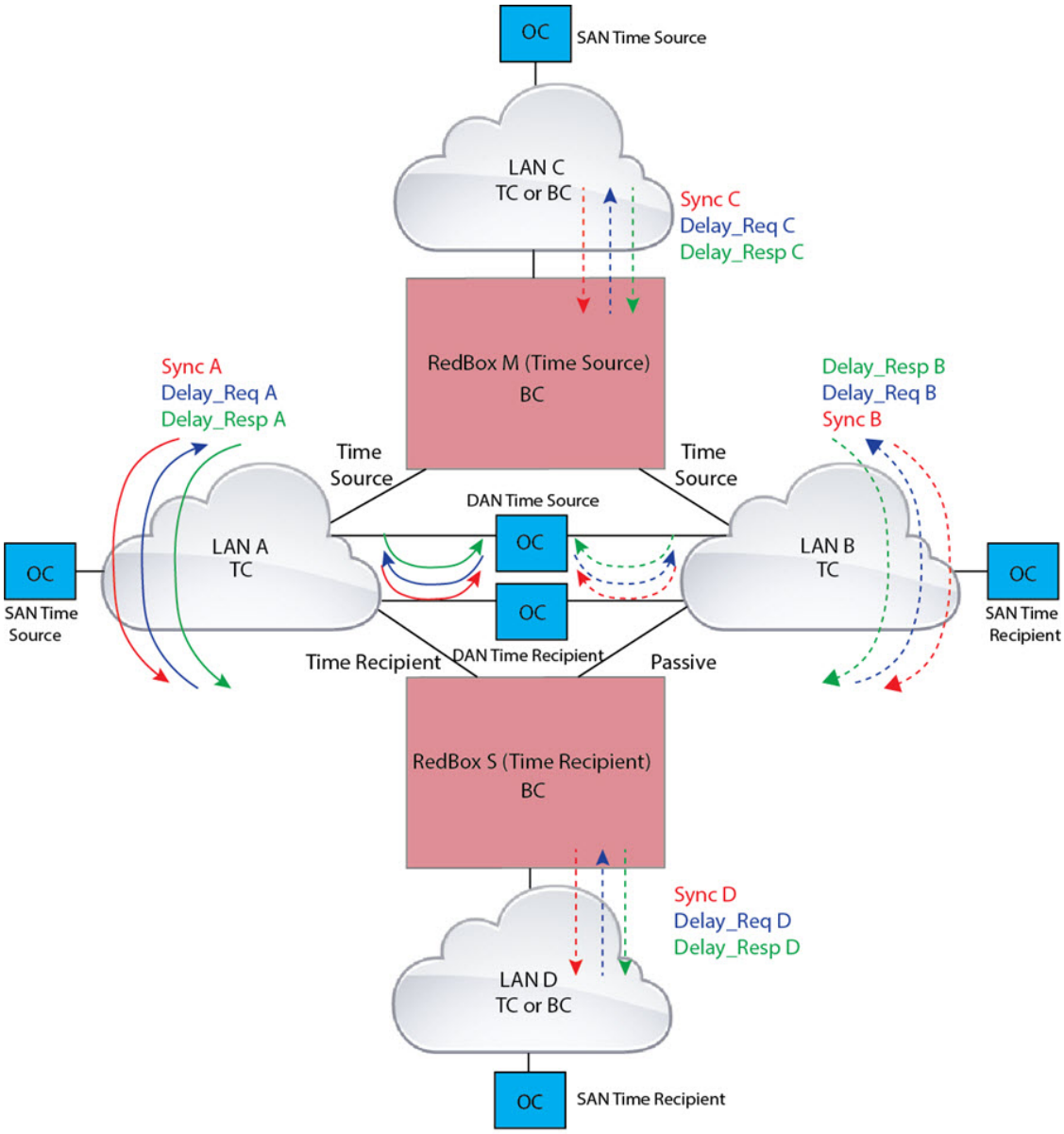
PRP RedBox のタイプ

スイッチは、PRP ネットワークで RedBox の役割を果たします。このセクションでは、IEC 62439-3 で定義されているように、PRP を介した PTP でサポートされる PRP RedBox のタイプについて説明します。

E2E を使用するダブル接続 BC（DABC）としての PRP RedBox

以下に示す設定では、2 つの RedBox（M と S など）が、エンドツーエンドの遅延測定メカニズムと IEEE1588v2 の Default プロファイルを使用する境界クロック（BC）として設定されています。RedBox M のベスト マスター クロック アルゴリズム（BMCA）で、時刻源に接続するポート A とポート B を決定します。Redbox M で実行されている PTP プロトコルは、ポート A と B の両方を時刻源ポートとして個別に扱い、両方のポートから同期メッセージや Follow_Up メッセージを個別に送信します。

図 *3 : E2E* を使用する *DABC* としての *PRP Redbox*



Redbox S では、通常の BMCA 操作でポート A を時刻受信者、ポート B を PASSIVE に決定します。ただし、ポート A と B が同じ PRP チャネルの一部であることが判明した場合は、ポート B が強制的に PASSIVE_SLAVE 状態になります。Redbox S のポート A とポート B の動作は、次のとおりです。

- ポート A は、通常の受信者ポートとして機能します。エンドツーエンドの遅延測定メカニズムを使用して、時刻源からの遅延とオフセットを計算します。計算された遅延とオフセットを使用して、ローカルクロックを同期します。

- ポート B は PASSIVE_SLAVE 状態です。エンドツーエンドの遅延測定メカニズムを使用して、時刻源からの遅延とオフセットを計算します。

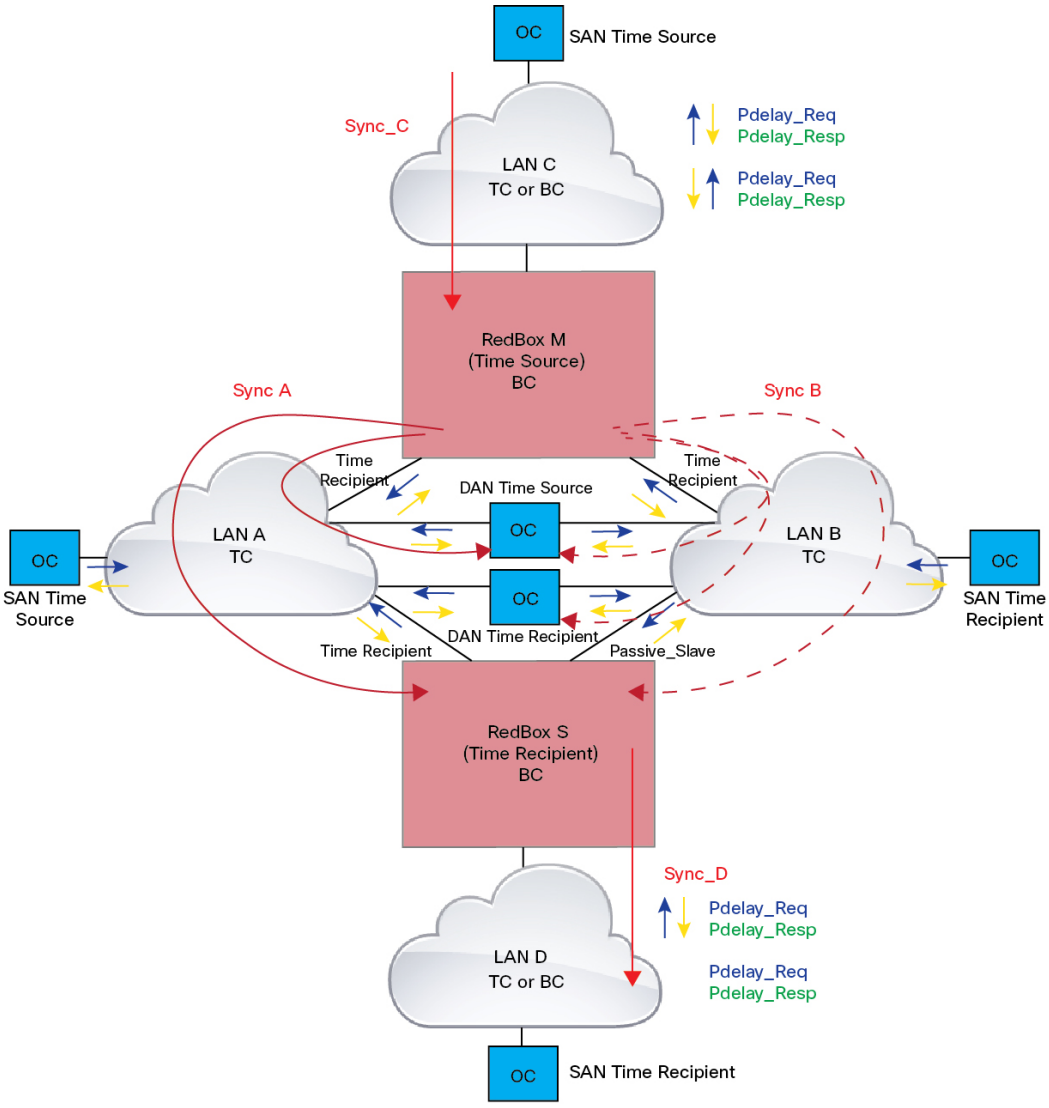
  これは、計算された遅延とオフセットを維持しますが、ローカルクロックの操作を実行しないという意味でパッシブです。遅延とオフセットの情報をすぐに利用できるようにすることで、ポートAで時刻源への接続が失われた場合に、そのロールを時刻受信者にシームレスに変更できます。

P2P を使用するダブル接続 BC（DABC）としての PRP RedBox

次の図は、Redbox M と Redbox S がピアツーピア（P2P）遅延測定メカニズムを使用する境界クロックとしてPowerプロファイルで実行するように設定されている例を示しています。この例で、GMC はLAN C を介して接続された通常のクロックです。すべてのクロックがピアツーピア遅延測定を実行するように設定され、ピア遅延は図に示すすべてのリンクで定期的に計算および維持されます。

Redbox M の BMCA は、時刻源に接続するポート A と B を決定します。Redbox M で実行されているPTPプロトコルは、ポートAとBの両方を時刻源ポートとして個別に扱い、両方のポートから同期メッセージや Follow_Up メッセージを個別に送信します。

図 *4 : P2P* を使用する *DABC* としての *PRP Redbox*



Redbox S では、通常の BMCA 操作でポート A を時刻受信者、ポート B を PASSIVE に決定します。ただし、ポート A と B が同じ PRP チャネルの一部であることが判明した場合は、ポート B が強制的に PASSIVE_SLAVE 状態になります。Redbox S のポート A とポート B の動作は、次のとおりです。

- ポート A は、通常の受信者ポートとして機能します。同期および Follow_Up メッセージとその補正フィールドを使用して、時刻源からの遅延とオフセットを計算し、ローカルクロックを同期します（E2E BC とは異なり、Delay_Req メッセージを生成する必要はありません。これは、PTP パスに沿ったすべてのリンク遅延と滞留時間が、Follow_Up メッセージの補正フィールドに蓄積されるためです）。

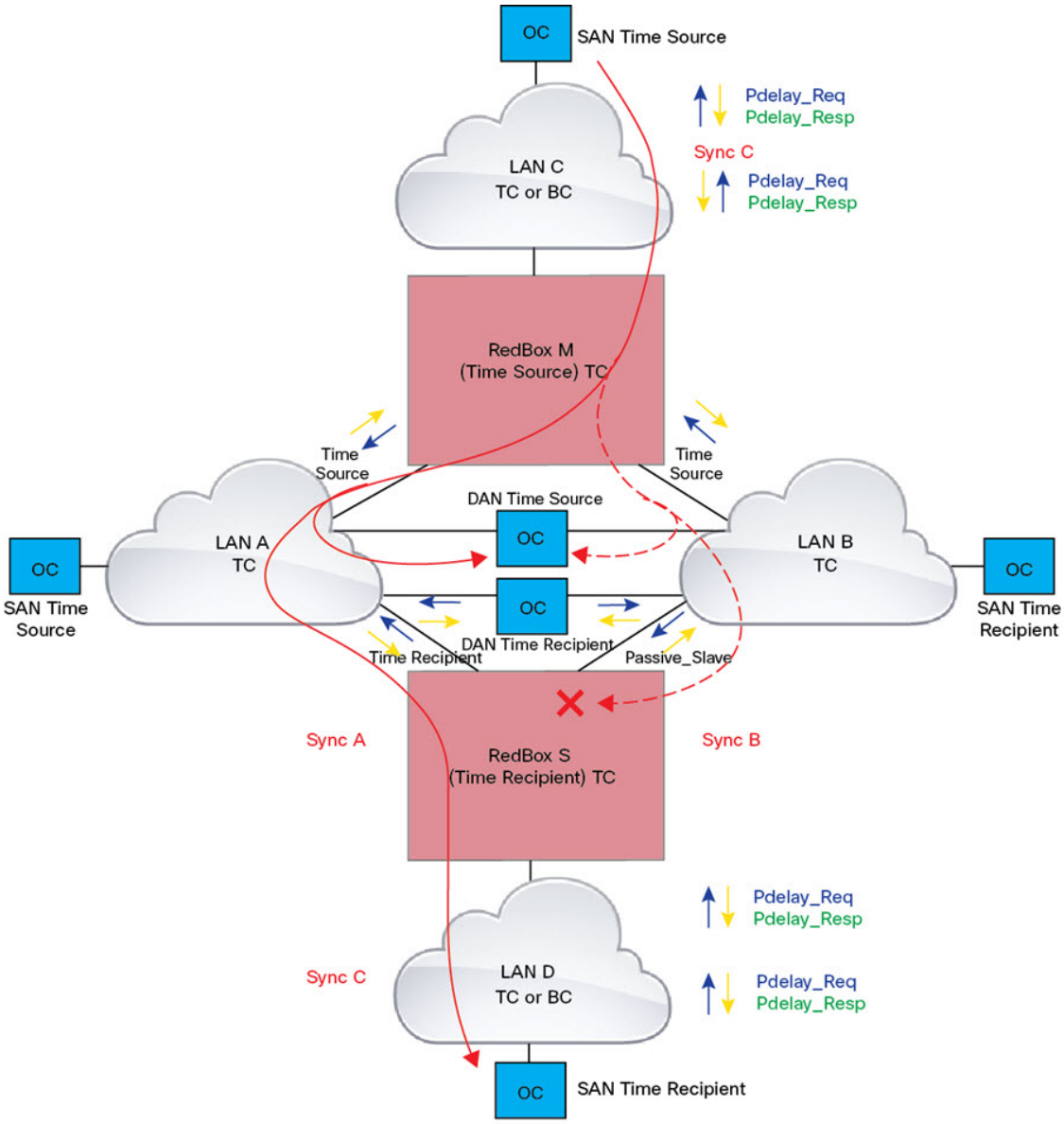
- ポート B は PASSIVE_SLAVE 状態です。ポート A と同様に時刻源からの遅延とオフセットを維持しますが、ローカルクロックに対する操作は実行しません。すべての同期情報を使用できるようにすることで、ポート A が GM との通信を失った場合に、新しい時刻受信者としてシームレスに引き継ぐことができます。

P2P を使用するダブル接続 TC（DATC）としての PRP RedBox

次の図は、Redbox M と Redbox S が Power プロファイルモードでトランスペアレントクロックとして動作するように設定されている例を示しています。この例で、GMC は LAN C を介して接続された通常のクロックです。すべてのクロックがピアツーピア遅延測定を実行するように設定され、ピア遅延は図に示すすべてのリンクで定期的に計算および維持されます。

P2P TC で BMCA を実行する必要はありませんが、Redbox M と Redbox S では BMCA を実行します。Redbox M の BMCA で、時刻源に接続するポート A と B を決定します。Redbox M は、ポート C で受信したすべての同期メッセージと Follow_Up メッセージをポート A と B に転送します。

図 *5 : P2P* を使用する *DATC* としての *PRP Redbox*



Redbox S では、前述のようにポート A を時刻受信者に、ポート B を PASSIVE_SLAVE に決定します。Redbox S のポート A とポート B の動作は、次のとおりです。

- ポート A は、通常の受信者ポートとして機能します。同期および Follow_Up メッセージとその補正フィールドを使用して、時刻源からの遅延とオフセットを計算し、ローカルクロックを同期します（E2E BC とは異なり、Delay_Req メッセージを生成する必要はありません。これは、PTP パスに沿ったすべてのリンク遅延と滞留時間が、Follow_Up メッセージの補正フィールドに蓄積されるためです）。

- ポート A と同様に、ポート B は時刻源からの遅延とオフセットを維持しますが、ローカルクロックに対する操作は実行しません。すべての同期情報を使用できるようにすることで、ポート A が GMC との通信を失った場合に、新しい時刻受信者としてシームレスに引き継ぐことができます。

LAN-A および LAN-B の障害検出と処理

LAN-A と LAN-B の障害は、「PRP RedBox のタイプ」で説明されているすべての RedBox タイプに対して同じ方法で検出および処理されます。

P2P を使用する DATC としての PRP RedBox と LAN C の SAN としての GMC に示されている例を使用すると、PTP に関連する LAN-A または LAN-B の障害は、次の理由で発生する可能性があります。

- LAN 内のデバイスがダウンした。
- LAN 内のリンクがダウンし、接続が失われた。
- PTP メッセージが LAN 内でドロップされた。

これらのイベントにより、RedBox S で PTP アナウンス受信タイムアウトが発生し、BMCA 計算がトリガーされます。アナウンス受信タイムアウトの詳細については、IEEE 1588v2 規格のセクション 7.7.3.1 を参照してください。

BMCA は、呼び出されると、PASSIVE_SLAVE ポートの状態を時刻受信者に変更し、時刻受信者を PASSIVE_SLAVE または PASSIVE または FAULTY に変更します。2 つの時刻受信者ポートまたは 2 つの PASSIVE_SLAVE ポートがある一時的なケースを回避するため、状態の変更はアトミックに行われます。

RedBox S が、新しい時刻受信者ポートを介して GMC に同期されるようになりました。同期への変更は、2 つの LAN で PTP パケットにより発生する遅延が大きく異なる場合や、LAN に非 PTP デバイスがある場合を除き、迅速かつシームレスに行う必要があります。

LAN D の SAN 時刻受信者も、RedBox S でのタイミングの変更を確認し、新しいクロックに統合する必要があります。これは、このクロックの GMC 変更イベントに似ていますが、前述のように、変更は通常シームレスです。

PRP を介した PTP の CLI コマンド

スイッチで PRP を介した PTP を有効にしている場合は、特定の **show** CLI コマンドを使用して、PRP に固有の PTP クロックデータを表示できます。

PTP に固有の CLI コマンドの詳細については、『Precision Time Protocol Configuration Guide, Cisco Catalyst IE9300 Rugged Series Switches』を参照してください。このガイドには、PRP に固有の CLI コマンドに関する情報が記載されています。

show ptp clock running

show ptp clock running コマンドは、実行中の PTP クロックの概要とそのポートに関する情報を表示します。コマンドを使用して、境界クロックが PHASE_ALIGNED（クロックがグランドマスタークロックと同期されている）であることを確認します。また、1 つのポートが Slave 状態で、もう 1 つのポートが Passive Slave 状態であることを確認します。

```
RedBox2#show ptp clock running
                    PTP Boundary Clock [Domain 0]  [Profile: default]
        State          Ports          Pkts sent      Pkts rcvd      Redundancy Mode
        PHASE_ALIGNED   2              168704         150444         Hot standby
                                PORT SUMMARY
                                                                        PTP Master
Name     Tx Mode      Role         Transport    State           Sessions     Port Addr
dyn1     mcast        negotiated   Ethernet     Slave           1            UNKNOWN
dyn2     mcast        negotiated   Ethernet     Passive Slave   1            UNKNOWN
```

show prp channel detail

両方のポートチャネルに関する詳細情報を表示するには、**show ptp channel detail** コマンドを使用します。Gi1/0/21 と Gi1/0/22 が Inuse 状態であることを確認します。

```
RedBox2#show prp channel detail
               PRP-channel listing:
               --------------------
PRP-channel: PR1
------------
 Layer type = L2
 Ports: 2       Maxports = 2
 Port state = prp-channel is Inuse
 Protocol = Enabled
Ports in the group:
  1) Port: Gi1/0/21
   Logical slot/port = 1/21     Port state = Inuse
        Protocol = Enabled
  2) Port: Gi1/0/22
   Logical slot/port = 1/22     Port state = Inuse
        Protocol = Enabled

PRP-channel: PR2
------------
 Layer type = L2
 Ports: 2       Maxports = 2
 Port state = prp-channel is Inuse
 Protocol = Enabled
Ports in the group:
  1) Port: Gi1/0/23
   Logical slot/port = 1/23     Port state = Inuse
        Protocol = Enabled
  2) Port: Gi1/0/24
   Logical slot/port = 1/24     Port state = Inuse
        Protocol = Enabled
```

show prp statistics ptpPacketStatistics

show prp statistics ptpPacketStatistics コマンドは、PRP が有効の場合にクロックポートに出入りする PTP パケットの数を表示します。また、入力レベルでのドロップも表示されます。

```
RedBox2#show prp statistics ptpPacketStatistics
 PRP channel-group 1 PTP STATS:
   ingress lan a: 250
   ingress drop lan a: 0
   ingress lan b: 377
   ingress drop_lan b: 0
   egress lan a: 185
   egress lan b: 188
 PRP channel-group 2 PTP STATS:
   ingress lan a: 384
   ingress drop lan a: 0
   ingress lan b: 388
   ingress drop_lan b: 0
   egress lan a: 191
   egress lan b: 193
RB2#
```

show ptp lan port int

show ptp lan port int コマンドは、LAN ポートのポートレベルの PTP 情報（PRP のポート状態など）を表示します。

次に、PRP チャネル 2 のポート gi1/0/23 のコマンドと出力例を示します。ポートが SLAVE 状態であることを確認します。

```
RedBox2#show ptp lan port int gi1/0/23
  PTP PORT DATASET: GigabitEthernet1/0/23
    Port identity: clock identity: 0x84:eb:ef:ff:fe:61:70:3f
    Port identity: port number: 3
    PTP version: 2
    Port state: SLAVE
    Peer delay request interval(log mean): 0
    Peer mean path delay(ns): 0
    Sync fault limit: 10000
    Rogue master block: FALSE
    Ingress phy latency: 725
    Egress phy latency: 0
```

次に、PRP チャネル 1 のポート gi1/0/24 のコマンドと出力の例を示します。ポートが PASSIVE_SLAVE 状態であることを確認します。

```
RedBox2#show ptp lan port int gi1/0/24
  PTP PORT DATASET: GigabitEthernet1/0/24
    Port identity: clock identity: 0x84:eb:ef:ff:fe:61:70:3f
    Port identity: port number: 4
    PTP version: 2
    Port state: PASSIVE_SLAVE
    Peer delay request interval(log mean): 0
    Peer mean path delay(ns): 2
    Sync fault limit: 10000
    Rogue master block: FALSE
    Ingress phy latency: 725
    Egress phy latency: 0
```

ptp clock boundary domain

Default プロファイルの PTP クロック境界ドメインまたは Power プロファイルの PTP クロック境界ドメインを設定できます。いずれかのドメインを設定する場合は、両方の PRP メンバーインターフェイスを PTP クロックに追加する必要があります。

次に、Default プロファイルの PTP クロック境界ドメインを設定する例を示します。

```
ptp clock boundary domain 0 profile default
clock-port dyn1
transport ipv4 multicast interface Gi1/0/21
clock-port dyn2
transport ipv4 multicast interface Gi1/0/22
```

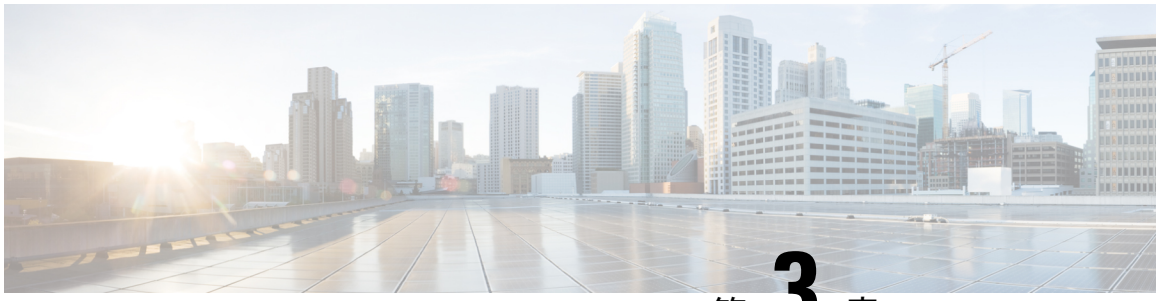
次に、Power プロファイルの PTP クロック境界ドメインを設定する例を示します。

```
ptp clock boundary domain 0 profile power
clock-port dyn1
transport ethernet multicast interface Gi1/0/21
clock-port dyn2
transport ethernet multicast interface Gi1/0/22
```

PRP を介した PTP 機能の履歴

以下の表に、このガイドに記載されている機能のリリースおよび関連情報を示します。この機能は、特に明記されていない限り、最初のリリース以降のすべてのリリースで使用できます。

リリース	機能	機能情報
Cisco IOS XE Dublin 17.12.1	パラレル冗長プロトコル（PRP）を介した高精度時間プロトコル（PTP）	この機能は、このリリースより Cisco Catalyst IE9300 高耐久性シリーズ スイッチの IE-9320-22S2C4X-A および IE-9320-22S2C4X-A で使用できるようになりました。
Cisco IOS XE Cupertino 17.9.x	PRP を介した PTP	この機能は、このリリースより Cisco Catalyst IE9300 高耐久性シリーズ スイッチの IE-9320-26S2C-A および IE-9320-26S2C-E で使用できるようになりました。



第 3 章

Redundancy Ethernet Protocol

- Resilient Ethernet Protocol （49 ページ）
- Resilient Ethernet Protocol の設定 （56 ページ）
- Resilient Ethernet Protocol Fast （66 ページ）
- Resilient Ethernet Protocol 設定のモニタリング （68 ページ）
- Resilient Ethernet Protocol の機能履歴 （70 ページ）

Resilient Ethernet Protocol

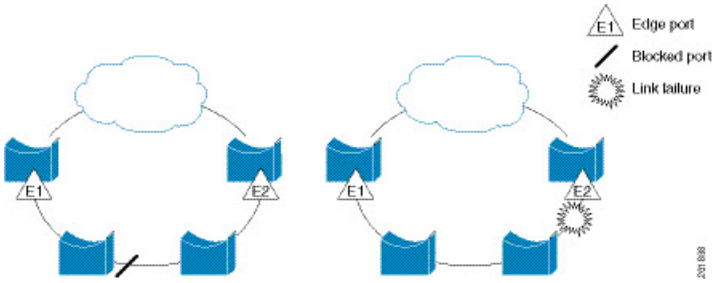
Resilient Ethernet Protocol（REP）はシスコ独自のプロトコルで、スパニングツリー プロトコル（STP）に代わるプロトコルとして、ネットワーク ループの制御、リンク障害の処理、コンバージェンス時間の改善を実現します。REPは、セグメントに接続されているポートのグループを制御することで、セグメントがブリッジングループを作成するのを防ぎ、セグメント内のリンク障害に応答します。REPは、より複雑なネットワークを構築するための基盤を提供し、VLAN ロード バランシングをサポートします。

（注） REP は、Network Essentials ライセンスの Cisco Catalyst IE9300 高耐久性シリーズ スイッチ は、Cisco IOS XE Cupertino 17.9.x 以降のリリースでサポートされています。

REP セグメントは相互接続されたポートのチェーンで、セグメント ID が設定されます。各セグメントは、標準（非エッジ）セグメント ポートと、2 つのユーザ設定のエッジ ポートで構成されています。1 スイッチに、同じセグメントに属することができるポートは 2 つまでで、各セグメント ポートにある外部ネイバーは1つだけです。セグメントは共有メディアを経由できますが、どのリンクでも同じセグメントに属することができるポートは 2 つだけです。REP は、トランク ポートでのみサポートされます。

次の図に、4 つのスイッチにまたがる 6 つのポートで構成されているセグメントの例を示します。ポート E1 および E2 がエッジ ポートとして設定されています。（左側のセグメントのように）すべてのポートが動作可能の場合、斜線で表しているように単一ポートがブロックされます。ブロックされたポートは、代替ポート（ALT ポート）とも呼ばれます。ネットワークに障害が発生した場合、ブロックされたポートがフォワーディング ステートに戻り、ネットワークの中断を最小限に抑えます。

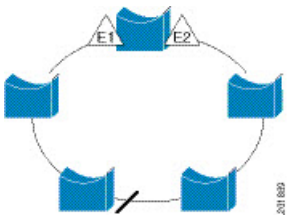
図 *6 : REP* オープン セグメント



上の図に示されたセグメントはオープンセグメントで、2 つのエッジポート間は接続されていません。REP セグメントはブリッジング ループの原因とならないため、セグメント エッジを安全に任意のネットワークに接続できます。セグメント内のスイッチに接続されているすべてのホストには、エッジポートを通じて残りのネットワークに接続する方法が2つありますが、いつでもアクセス可能なのは 1 つだけです。いずれかのセグメントまたは REP セグメントのいずれかのポートに障害が発生した場合、REP はすべての ALT ポートのブロックを解除し、他のゲートウェイ経由で接続できるようにします。

下の図に示すセグメントはリングセグメントとも呼ばれるクローズドセグメントで、同じルータ上に両方のエッジポートがあります。この設定を使用すると、セグメント内の任意の2ルータ間で冗長接続を形成することができます。

図 *7 : REP* リング セグメント



REP セグメントには、次のような特徴があります。

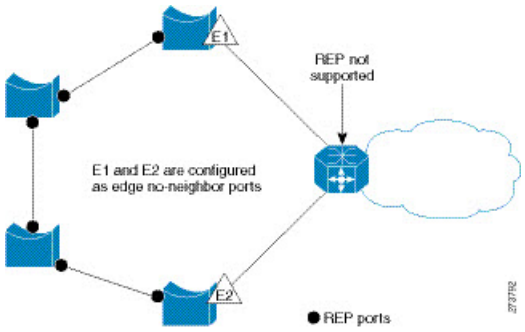
- セグメント内の全ポートが動作可能な場合、1ポート（ALTポートと呼ばれる）が各VLANでブロックステートとなります。VLANロードバランシングが設定されている場合は、セグメント内の 2 つの ALT ポートが VLAN のブロックステートを制御します。
- ポートが動作不能になり、リンク障害が発生すると、すべてのポートがすべての VLAN トラフィックを転送して、接続性を確保します。
- リンク障害の場合、できるだけ早期に代替ポートのブロックが解除されます。障害リンクが復旧すると、ネットワークの中断を最小限に抑えるようにVLAN単位で論理的にブロックされたポートが選択されます。

REP セグメントに基づいて、ほとんどのネットワークタイプを構成することができます。

アクセスリングトポロジでは、次の図に示すように、ネイバースイッチで REP がサポートされない場合があります。この場合、そのスイッチ側のポート（E1 と E2）を非ネイバーエッジ

ポートとして設定できます。非ネイバーエッジポートは、STP トポロジ変更通知（TCN）をアグリゲーションスイッチに送信するように設定できます。

図 *8*：非ネイバー エッジ ポート



REP には次のような制限事項があります。

- 各セグメント ポートを設定する必要があります。設定を間違えると、ネットワーク内でフォワーディング ループが発生します。
- REP はセグメント内の単一障害ポートだけを管理できます。REP セグメント内の複数ポート障害の場合、ネットワークの接続が失われます。
- 冗長ネットワーク内だけに REP を設定します。冗長性のないネットワークに REP を設定すると、接続が失われます。

リンク完全性

REP は、リンク完全性の確認にエッジ ポート間でエンドツーエンド ポーリング機能を使用しません。ローカル リンク障害検出を実装しています。REP リンク ステータス レイヤ（LSL）が REP 対応ネイバーを検出して、セグメント内の接続性を確立します。ネイバーが検出されるまで、インターフェイス上ですべての VLAN がブロックされます。ネイバーが特定されたあと、REP が代替ポートとなるネイバー ポートと、トラフィックを転送するポートを決定します。

セグメント内のポートごとに、一意のポート ID が割り当てられます。ポート ID フォーマットは、スパニングツリーアルゴリズムで使用されるものと類似しており、ポート番号（ブリッジ上で一意）と、関連 MAC アドレス（ネットワーク内で一意）から構成されます。セグメント ポートが起動すると、ポートの LSL がセグメント ID およびポート ID を含むパケットの送信を開始します。ポートは、同じセグメント内のネイバーとのスリーウェイ ハンドシェイクを実行したあとで、動作可能と宣言されます。

次のような場合、セグメント ポートは動作可能になりません。

- ネイバーに同じセグメント ID がない
- 複数のネイバーに同じセグメント ID がある
- ネイバーがピアとして、ローカル ポートに確認応答しない

各ポートは、直近のネイバーと隣接関係を確立します。ネイバーとの隣接関係が確立されると、代替ポートとして機能する、セグメントのブロックされたポートを決定するようにポートが相互にネゴシエートします。その他のすべてのポートのブロックは解除されます。デフォルトでは、REP パケットはブリッジ プロトコル データ ユニットクラスの MAC アドレスに送信されます。パケットは、シスコ マルチキャスト アドレスにも送信され得ますが、セグメントに障害が発生した場合にブロックされたポートのアドバタイズ（BPA）メッセージの送信だけに使用されます。パケットは、REP が動作していない装置によって廃棄されます。

高速コンバージェンス

REP は、物理リンク ベースで動作し、VLAN 単位ベースでは動作しません。すべての VLAN に対して 1 つの hello メッセージしか必要ないため、プロトコル上の負荷が軽減されます。指定セグメント内の全スイッチで継続的に VLAN を作成し、REP トランク ポート上に同じ許容 VLAN を設定することを推奨します。ソフトウェアでのメッセージのリレーによって発生する遅延を回避するために、REP ではいくつかのパケットを通常のマルチキャスト アドレスにフラッディングします。これらのメッセージはハードウェア フラッド レイヤ（HFL）で動作し、REP セグメントだけではなくネットワーク全体にフラッディングされます。セグメントに属していないスイッチは、これらのメッセージをデータ トラフィックとして扱います。ドメイン全体または特定のセグメントの管理 VLAN を設定することで、これらのメッセージのフラッディングを制御することができます。

VLAN ロード バランシング

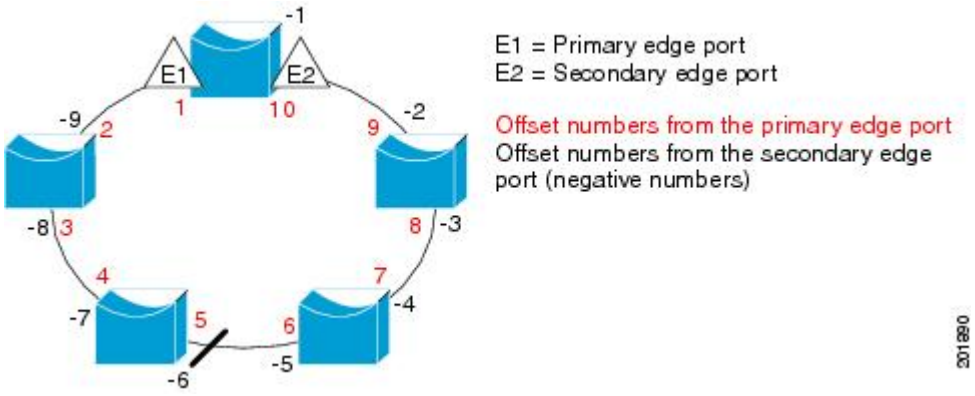
REP セグメント内の 1 つのエッジ ポートがプライマリ エッジ ポートとして機能し、もう一方がセカンダリ エッジ ポートとなります。セグメント内の VLAN ロード バランシングに常に参加しているのがプライマリ エッジ ポートです。REP VLAN バランシングは、設定された代替ポートでいくつかの VLAN をブロックし、プライマリ エッジ ポートでその他の全 VLAN をブロックすることで実行されます。VLAN ロード バランシングを設定する際に、次の 3 種類の方法のいずれかを使用して代替ポートを指定できます。

- インターフェイスにポート ID を入力します。セグメント内のポート ID を識別するには、ポートの **show interface rep detail** インターフェイス コンフィギュレーション コマンドを入力します。
- **preferred** キーワードを入力します。これにより、**rep segment** *segment-id* **preferred** インターフェイス コンフィギュレーション コマンドで優先代替ポートとしてすでに設定されているポートを選択します。
- セグメント内のポートのネイバー オフセット番号を入力します。これは、エッジ ポートのダウンストリーム ネイバー ポートを識別するものです。ネイバー オフセット番号の範囲は、-256 ～ +256 で、0 値は無効です。プライマリ エッジ ポートはオフセット番号 1 です。1 を超える正数はプライマリ エッジ ポートのダウンストリーム ネイバーを識別します。負数は、セカンダリ エッジ ポート（オフセット番号 -1）とそのダウンストリーム ネイバーを示します。

（注） プライマリ（またはセカンダリ）エッジポートからポートのダウンストリーム位置を識別することで、プライマリ エッジ ポートのオフセット番号を設定します。番号1はプライマリ エッジポートのオフセット番号なので、オフセット番号 1 は入力しないでください。

次の図に、E1 がプライマリ エッジ ポートで E2 がセカンダリ エッジ ポートの場合の、セグメントのネイバーオフセット番号を示します。リングの内側にある赤い番号は、プライマリ エッジ ポートからのオフセット番号で、リングの外側にある黒い番号がセカンダリ エッジ ポートからのオフセット番号です。正のオフセット番号（プライマリ エッジ ポートからのダウンストリーム位置）または負のオフセット番号（セカンダリ エッジ ポートからのダウンストリーム位置）のいずれかにより、（プライマリ エッジ ポートを除く）全ポートを識別できます。E2 がプライマリ エッジ ポートになるとオフセット番号 1 となり、E1 のオフセット番号が -1 になります。

図 *9*: セグメント内のネイバー オフセット番号



REP セグメントが完了すると、すべての VLAN がブロックされます。VLAN ロード バランシングを設定する際には、次の 2 種類の方法のいずれかを使用してトリガーを設定する必要もあります。

- プライマリ エッジ ポートのあるスイッチ上で **rep preempt segment** *segment-id* 特権 EXEC コマンドを入力することで、いつでも手動で VLAN ロード バランシングをトリガーすることができます。
- **rep preempt delay** *seconds* インターフェイス コンフィギュレーション コマンドを入力すると、プリエンプション遅延時間を設定できます。リンク障害が発生して回復すると、設定されたプリエンプション期間の経過後に VLAN ロード バランシングが開始されます。設定時間が経過する前に別のポートで障害が発生した場合、遅延タイマーが再開されることに注意してください。

（注） VLAN ロード バランシングが設定されている場合、手動での介入またはリンク障害および回復によってトリガーされるまで、動作が開始されません。

VLAN ロード バランシングがトリガーされると、プライマリ エッジ ポートがメッセージを送信して、セグメント内の全インターフェイスにプリエンプションについて警告します。メッセージがセカンダリ ポートで受信されると、メッセージがネットワークに送信され、メッセージ内で指定された VLAN セットをブロックするように代替ポートに通知し、残りの VLAN をブロックするようにプライマリ エッジ ポートに通知します。

またすべての VLAN をブロックするために、セグメント内の特定ポートを設定できます。プライマリ エッジ ポートだけによって VLAN ロード バランシングが開始され、セグメントが各エンドでエッジ ポートによって終端されていない場合開始することができません。プライマリ エッジ ポートは、ローカル VLAN ロードバランシング設定を決定します。

ロード バランシングを再設定するには、プライマリ エッジ ポートを再設定します。ロードバランシング設定を変更すると、プライマリ エッジ ポートでは、**rep preempt segment** コマンドが実行されるか、ポート障害および復旧のあとで設定済みプリエンプト遅延期間が経過してから、新規設定が実行されます。エッジ ポートを通常セグメント ポートに変更しても、既存の VLAN ロードバランシング ステータスは変更されません。新規エッジ ポートを設定すると、新規トポロジ設定になる可能性があります。

スパニングツリー インタラクション

REP は STP とやり取りしませんが、共存はできます。セグメントに属しているポートはスパニングツリーの制御から削除されるため、セグメント ポートでは STP BPDU の送受信は行われません。したがって、STP はセグメント上で実行できません。

STP リング コンフィギュレーションから REP セグメント コンフィギュレーションに移行するには、まずリング内の単一ポートをセグメントの一部として設定し、次にセグメント数を最小限にするように隣接するポートを設定します。各セグメントには、常にブロックされたポートが含まれているので、セグメントが複数になるとブロックされたポートも複数になり、接続が失われる可能性があります。セグメントがエッジ ポートの場所まで両方向に設定されたら、次にエッジ ポートを設定します。

Resilient Ethernet Protocol（REP）ネゴシエート

（注） REP ネゴシエートは、アップリンク ポートでのみ機能します。

REP とスパニングツリープロトコル（STP）は、2 つの異なるループ回避プロトコルです。REP には、コンバージェンス時間の点で STP よりも優れた点があります。REP は、リング内で単一のリンク障害が発生した場合に冗長パスを提供できるように、リングトポロジで動作するよう設定できます。

シスコのスイッチは、デフォルトで STP が有効になっています。STP が有効になっているスイッチが（新しいノードの追加または既存のノードの交換のために）すでに実行中の REP リングに挿入されると、次の条件が適用されます。

- 新しいスイッチにより、REP リングが切断されます。
- 新しいスイッチは、REP リングの一部として設定されるまで、リングを介して通信できません。

REP ネゴシエート機能は、REP ステータスをピアとネゴシエートすることで、これらの問題を解決しようとします。次の表に、REP ネゴシエーションイベントがトリガーされるタイミングと実行するアクションを示します。ここでは、両方のピアがネゴシエート中、いずれのピアもネゴシエートしていないという、2 つのイベントがあります。

SELF REP をネゴシエート	PEERS REP をネゴシエート	トリガーされるイベント	動作
True	True	REPN	REP を設定
True	False	REPNN	STP を設定
False	X	REPNN	STP のまま

この機能は、3 つの異なるプロトコルに依存して必要なデータを取得し、正しい設定を決定します。関連するさまざまなプロトコルとその目的を次に示します。

- **STP**：デフォルトでは、STP はシスコスイッチのすべてのポートで有効になっています。
- **REP**：カスタマーネットワークを設定して、コンバージェンス時間と冗長性改善のために REP リングを形成します。
- **Cisco Discovery Protocol (CDP)**：この機能は、CDP メッセージを介して送信されるユーザー定義の TLV に依存して、インターフェイスの正しい（STP または REP）設定をネゴシエートします。

REP ポート

REP セグメントは、障害ポート、オープン ポート、および代替ポートで構成されます。

- 標準セグメント ポートとして設定されたポートは、障害ポートとして起動します。
- ネイバーとの隣接関係が確立されると、ポートは代替ポート ステートに移行して、インターフェイス内の全 VLAN をブロックします。ブロックされたポートのネゴシエーションが実施され、セグメントが安定すると、1 つのブロックされたポートが代替ロールに留まり、他のすべてのポートがオープン ポートになります。
- リンク内で障害が発生すると、すべてのポートが障害ステートに遷移します。代替ポートは、障害通知を受信すると、すべての VLAN を転送するオープン ステートに遷移します。

通常セグメント ポートをエッジ ポートに変換しても、エッジ ポートを通常セグメント ポートに変換しても、必ずトポロジ変更が発生するわけではありません。エッジポートを通常セグメント ポートに変更する場合、設定されるまで VLAN ロード バランシングは実装されません。VLAN ロード バランシングの場合、セグメント内に 2 つのエッジ ポートを設定する必要があります。

スパニングツリー ポートとして再設定されたセグメント ポートは、スパニングツリー設定に従って再起動します。デフォルトでは、これは指定ブロッキング ポートです。PortFast が設定されていたり、STP が無効の場合、ポートはフォワーディング ステートになります。

Resilient Ethernet Protocol の設定

セグメントは、チェーンで相互接続されているポートの集合で、セグメント ID が設定されています。REP セグメントを設定するには、REP 管理 VLAN を設定し（またはデフォルト VLAN 1 を使用し）、次にインターフェイス コンフィギュレーション モードを使用してセグメントにポートを追加します。2 つのエッジ ポートをセグメント内に設定して、デフォルトで 1 つをプライマリ エッジ ポート、もう 1 つをセカンダリ エッジ ポートにします。1 セグメント内のプライマリ エッジ ポートは 1 つだけです。別のスイッチのポートなど、セグメント内で 2 つのポートをプライマリ エッジ ポートに設定すると、REP がそのうちのいずれかを選択してセグメントのプライマリ エッジ ポートとして機能させます。必要に応じて、STCN および VLAN ロードバランシングが送信される場所を設定できます。

REP のデフォルト設定

- REP はすべてのインターフェイス上で無効です。有効にする際に、エッジ ポートとして設定されていなければインターフェイスは通常セグメント ポートになります。
- REP を有効にする際に、STCN の送信タスクは無効で、すべての VLAN はブロックされ、管理 VLAN は VLAN 1 になります。
- VLAN ロード バランシングが有効の場合、デフォルトは手動でのプリエンプションで、遅延タイマーは無効になっています。VLAN ロード バランシングが設定されていない場合、手動でのプリエンプション後のデフォルト動作は、プライマリ エッジ ポートで全 VLAN がブロックとなります。
- REP Fast はデフォルトで無効になっています。
- REP ゼロタッチプロビジョニングは、グローバルレベルではデフォルトで有効に、インターフェイスレベルでは無効になっています。

REP の設定ガイドラインと制限事項

REP の設定時には、次の注意事項に従ってください。

- まず 1 ポートの設定から始めて、セグメント数とブロックされたポートの数を最小限に抑えるように隣接するポートを設定することを推奨します。

- 外部ネイバーが設定されておらずセグメント内では3つ以上のポートに障害が発生した場合、1ポートがデータ パス用のフォワーディング ステートになり、設定中の接続性の維持に役立ちます。

  show rep interfaceコマンド出力では、このポートのポートロールは「Fail Logical Open」と表示され、他の障害ポートのポートロールは「Fail No Ext Neighbor」と表示されます。障害ポートの外部ネイバーが設定されている場合、ポートは代替ポート ステートに移行して、代替ポート選択メカニズムに基づいて最終的にオープン ステートになるか、代替ポートのままになります。

- REP ポートは、レイヤ 2 IEEE 802.1Q またはトランクポートのいずれかにする必要があります。

- 同じ許可 VLAN のセットでセグメント内のすべてのトランク ポートを設定することを推奨します。

- Telnet接続を通じてREPを設定する際には注意してください。これは、別のREPインターフェイスがブロック解除のメッセージを送信するまで、REP はすべての VLAN をブロックするためです。同じインターフェイス経由でルータにアクセスするTelnetセッションでREP を有効にすると、ルータへの接続が失われることがあります。

- 同じセグメントやインターフェイスで REP と STP を実行することはできません。

- STP ネットワークを REP セグメントに接続する場合、接続はセグメント エッジであることを確認してください。エッジで実行されていないSTP接続は、REPセグメントではSTPが実行されないため、ブリッジング ループが発生する可能性があります。すべての STP BPDU は、REP インターフェイスで廃棄されます。

- REP がスイッチの 2 ポートで有効の場合、両方のポートが通常セグメント ポートまたはエッジ ポートである必要があります。REP ポートは以下の規則に従います。

  - 同じ REP セグメントに属することができるスイッチ上のポートは 2 つだけです。

  - セグメント内にスイッチ上の1ポートだけが設定されている場合、そのポートがエッジ ポートとなります。

  - 同じセグメント内に属するスイッチに2つのポートがある場合、両方のポートがエッジポートであるか、両方のポートが通常セグメントポートであるか、一方が通常ポートでもう一方が非ネイバー エッジ ポートである必要があります。スイッチ上のエッジ ポートと通常セグメント ポートが同じセグメントに属することはできません。

  - スイッチ上の2ポートが同じセグメントに属していて、1つがエッジ ポートとして設定され、もう1つが通常セグメントポートに設定されている場合（設定ミス）、エッジ ポートは通常セグメント ポートとして扱われます。

- REPインターフェイスはブロックされた状態になり、ブロック解除できるようになるまでブロックされた状態のまま残ります。突然の接続切断を避けるために、このステータスを認識しておく必要があります。

- REP はネイティブ VLAN 上においてすべての LSL PDU をタグなしフレームで送信します。シスコ マルチキャスト アドレスに送信された BPA メッセージは、管理 VLAN で送信されます。これはデフォルトで VLAN 1 です。
- ネイバーからの hello が受信されないままどのくらいの時間が経過すると REP インターフェイスがダウンするかを設定できます。**rep lsl-age-timer** インターフェイス コンフィギュレーション コマンドを使用して、120 ～ 10000 ミリ秒の時間を設定します。次に、LSL Hello タイマーはエージング タイマーの値を 3 で割った値に設定されます。通常の動作では、ピア スイッチのエージング タイマーが満了になって hello メッセージが確認されるまでに LSL hello が 3 回送信されます。**rep lsl-age-timer** は、非 REP Fast 銅線ギガビットインターフェイスにのみ使用します。他のすべてのインターフェイスでは、**rep lsl-age-timer** を使用するメリットがありません。
  - EtherChannel ポート チャネル インターフェイスでは、1000 ミリ秒未満の LSL エージング タイマー値はサポートされていません。ポート チャネルで 1000 ミリ秒未満の値を設定しようとすると、エラー メッセージが表示されてコマンドが拒否されます。
  - **lsl-age-timer** は、通常のリンクダウン検出がコンバージェンス時間に対して遅すぎる場合に使用することを目的としています。

    FastEthernet 接続と光ファイバ接続には、**lsl-age-timer** は必要ありません。ギガビット銅線では、**lsl-age-timer** の代わりに REP Fast を使用できます。
- REP ポートは、次のポート タイプのいずれかに設定できません。
  - スイッチド ポート アナライザ（SPAN）宛先ポート
  - トンネル ポート
  - アクセスポート
- REP は EtherChannel でサポートされていますが、EtherChannel に属する個別のポートではサポートされません。
- スイッチごとに最大 64 の REP セグメントを設定できます。
- REP リングのサイズに制限はありません。REP リングサイズが 20 ノードを超えると、50 ミリ秒のサブコンバージェンスに到達できない場合があります。

REP Fast の設定時には、次の注意事項に従ってください。

- この機能を有効にするには、リンクの両端で REP Fast を設定しなければなりません。
- REP Fast によって約束されたコンバージェンス時間に到達するには、REP セグメント内のすべてのインターフェイスが REP Fast に対応し、REP Fast が有効になっている必要があります。混在している場合、リンク障害時のコンバージェンス時間の保証はありません。
- 次の制限事項に注意してください。
  - 最大 3 つの REP セグメントで REP Fast を有効にできます。
  - MAC Sec はサポートされていません。

- オーバースタックはサポートされていません。
- EtherChannel を介した REP Fast はサポートされていません。

REP 管理 VLAN を設定する

リンク障害メッセージ、およびロード バランシング時の VLAN ブロッキング通知によって作成される遅延を回避するため、REP はハードウェア フラッド レイヤ（HFL）で通常のマルチキャスト アドレスにパケットをフラッディングします。これらのメッセージは REP セグメントだけではなくネットワーク全体にフラッディングされます。管理VLANを設定することで、これらのメッセージのフラッディングを制御できます。

REP 管理 VLAN を設定する場合、次の注意事項に従ってください。

- 管理 VLAN を設定しない場合、デフォルトは VLAN 1 です。
- すべてのセグメントに対し 1 つの管理 VLAN をスイッチで設定できます。
- 管理 VLAN は RSPAN VLAN になりません。

REP 管理 VLAN を設定するには、特権 EXEC モードで次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **rep admin vlan** *vlan-id*
4. **end**
5. **show interface** ［*interface-id*］ **rep detail**
6. **copy running-config startup config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**rep admin vlan** *vlan-id* 例： `Device(config)# rep admin vlan 2`	管理 VLAN を指定します。範囲は 2 ～ 4094 です。 管理 VLAN をデフォルトの 1 に設定するには、**no rep admin vlan** グローバル コンフィギュレーション コマンドを入力します。

	コマンドまたはアクション	目的
ステップ 4	**end** 例： `Device(config)# end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 5	**show interface**［*interface-id*］**rep detail** 例： `Device# show interface gigabitethernet1/0/1 rep detail`	（任意）REP インターフェイスの設定を検証します。
ステップ 6	**copy running-config startup config** 例： `Device# copy running-config startup config`	（任意）スイッチ スタートアップ コンフィギュレーション ファイルに設定を保存します。

REP インターフェイスの設定

REP を設定する場合、各セグメントインターフェイスで REP を有効にして、セグメント ID を指定します。このタスクは必須で、他の REP 設定の前に実行する必要があります。また、各セグメントにプライマリおよびセカンダリ エッジ ポートを設定する必要があります。それ以外の手順はすべてオプションです。

インターフェイスで REP を有効にし、設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *interface-id*
4. **switchport mode trunk**
5. **rep segment** *segment-id* [**edge**［**no-neighbor**］[**primary**]] [**preferred**]
6. **rep stcn** {**interface** *interface id* | **segment** *id-list* | **stp**}
7. **rep block port** {**id** *port-id* | *neighbor-offset* | **preferred**} **vlan** {*vlan-list* | **all**}
8. **rep preempt delay** *seconds*
9. **rep lsl-age-timer** *value*
10. **end**
11. **show interface**［*interface-id*］**rep** [**detail**]
12. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet1/0/1`	インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。インターフェイスは物理レイヤ2インターフェイスまたはポート チャネル（論理インターフェイス）に設定できます。
ステップ 4	**switchport mode trunk** 例： `Device(config-if)# switchport mode trunk`	インターフェイスをレイヤ 2 トランク ポートとして設定します。
ステップ 5	**rep segment** *segment-id* [**edge** [**no-neighbor**] [**primary**]] [**preferred**] 例： `Device(config-if)# rep segment 1 edge no-neighbor primary`	インターフェイス上で REP を有効にして、セグメント番号を特定します。指定できるセグメント ID の範囲は 1 ～ 1024 です。 （注） 各セグメントに 1 つのプライマリ エッジ ポートを含めて、2 つのエッジ ポートを設定する必要があります。 これらの任意のキーワードは利用可能です。 • （任意）**edge**：エッジポートとしてポートを設定します。各セグメントにあるエッジ ポートは 2 つだけです。**primary** キーワードなしで **edge** キーワードを入力すると、ポートがセカンダリエッジポートとして設定されます。 • （任意）**primary**：プライマリエッジポート（VLANロードバランシングを設定できるポート）としてポートを設定します。 • （任意）**no-neighbor**：外部 REP ネイバーを持たないエッジポートとしてポートを設定します。ポートはエッジポートのすべてのプロパティを継承し、エッジポートの場合と同様にプロパティを設定できます。

	コマンドまたはアクション	目的
		（注） 各セグメントにあるプライマリエッジポートは 1 つだけですが、2 つの異なるスイッチにエッジポートを設定して **primary** キーワードを両方のスイッチに入力しても、その設定は有効です。ただし、REP ではセグメント プライマリ エッジ ポートとして 1 つのポートだけが選択されます。特権 EXEC モードで **show rep topology** コマンドを入力すると、セグメントのプライマリエッジポートを特定できます。 • （任意）**preferred**：ポートが優先代替ポートであるか、VLAN ロードバランシングの優先ポートであるかを示します。 （注） ポートを優先に設定しても、代替ポートになるとは限りません。同等に可能性のあるポートよりやや可能性が高くなるだけです。通常、前に障害が発生したポートが、代替ポートとなります。
ステップ 6	**rep stcn** {**interface** *interface id* | **segment** *id-list* | **stp**} 例： `Device(config-if)# rep stcn segment 25-50`	（任意）STCN を送信するようにエッジ ポートを設定します。 • **interface** *interface-id*：物理インターフェイスまたはポートチャネルを指定して、STCN を受け取ります。 • **segment** *id-list*：STCN を受け取る 1 つ以上のセグメントを特定します。有効な範囲は 1 ～ 1024 です。 • **stp**：STCN を STP ネットワークに送信します。 （注） STCN を STP ネットワークに送信するために **rep stcn stp** コマンドを設定する場合は、スパニング ツリー（MST）モードがネイバーなしのエッジ ノード上に必要です。
ステップ 7	**rep block port** {**id** *port-id* | *neighbor-offset* | **preferred**} **vlan** {*vlan-list* | **all**} 例：	（任意）プライマリエッジポートに VLAN ロードバランシングを設定して、3 つの方法のいずれかを使用して REP 代替ポートを特定し（**id** *port-id*、

	コマンドまたはアクション	目的
	`Device(config-if)# rep block port id 0009001818D68700 vlan 1-100`	*neighbor_offset*、**preferred**）、代替ポートでブロックされるように VLAN を設定します。 • **id** *port-id*：ポート ID で代替ポートを特定します。セグメント内の各ポートにポート ID が自動的に生成されます。**show interface** *type number* **rep** [**detail**] 特権 EXEC コマンドを入力し、インターフェイスポート ID を表示できます。 • *neighbor_offset*：エッジポートからのダウンストリームネイバーとして代替ポートを特定するための番号。有効範囲は -256 ～ 256 で、負数はセカンダリ エッジ ポートからのダウンストリーム ネイバーを示します。**0** の値は無効です。**-1** を入力すると、セカンダリエッジポートを代替ポートとして識別します。 （注） プライマリエッジポート（オフセット番号 1）に **rep block port** コマンドを入力するので、代替ポートを特定するのにオフセット値 1 は入力できません。 • **preferred**：すでに VLAN ロードバランシングの優先代替ポートとして指定されている通常セグメントポートを選択します。 • **vlan** *vlan-list*：1 つの VLAN または VLAN の範囲をブロックします。 • **vlan all**：すべての VLAN をブロックします。 （注） REP プライマリ エッジ ポート上にだけこのコマンドを入力します。
ステップ 8	**rep preempt delay** *seconds* 例： `Device(config-if)# rep preempt delay 100`	（任意）プリエンプション遅延時間を設定します。 • リンク障害が発生して復旧した後に、VLAN ロード バランシングを自動的にトリガーするには、このコマンドを使用します。 • 遅延時間の範囲は 15 ～ 300 秒です。デフォルトは、遅延時間のない手動によるプリエンプションです。 （注） REP プライマリ エッジ ポート上にだけこのコマンドを入力します。

	コマンドまたはアクション	目的
ステップ 9	**rep lsl-age-timer** *value* 例： `Device(config-if)# rep lsl-age-timer 2000`	（任意）ネイバーからの hello が受信されないままどのくらいの時間（ミリ秒）が経過すると REP インターフェイスがダウンするかを設定します。 指定できる範囲は 120 ～ 10000 ミリ秒（40 ミリ秒単位）です。デフォルト値は 5000 ミリ秒（5 秒）です。 （注） • EtherChannel ポート チャネル インターフェイスでは、1000 ミリ秒未満の LSL エージング タイマー値はサポートされていません。 • リンクのフラップを避けるため、リンクの両方のポートに同じ LSL エージが設定されていることを確認します。
ステップ 10	**end** 例： `Device(config-if)# end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 11	**show interface** ［*interface-id*］**rep** [**detail**] 例： `Device# show interface gigabitethernet1/0/1 rep detail`	（任意）REP インターフェイスの設定を表示します。
ステップ 12	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）スイッチ スタートアップ コンフィギュレーション ファイルに設定を保存します。

VLAN ロード バランシングの手動によるプリエンプションの設定

プライマリエッジポートで **rep preempt delay** *seconds* インターフェイス コンフィギュレーション コマンドを入力しないで、プリエンプション時間遅延を設定する場合、デフォルトではセグメントで VLAN ロードバランシングを手動でトリガーします。手動で VLAN ロード バランシングをプリエンプトする前に、他のすべてのセグメント設定が完了しているかどうか確認してください。**rep preempt delay segment** *segment-id* コマンドを入力すると、プリエンプションによってネットワークが中断する可能性があるため、コマンド実行前に確認メッセージが表示されます。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

ステップ 3	**rep preempt segment** *segment-id*
	例：
	`Device(config)# rep preempt segment 100`
	`The command will cause a momentary traffic disruption.`
	`Do you still want to continue? [confirm]`
		手動により、セグメント上の VLAN ロード バランシングをトリガーします。
		実行前にコマンドを確認する必要があります。

ステップ 4	**end** 例： `Device# end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 5	**show rep topology segment** *segment-id* 例： `Device# show rep topology segment 100`	（任意）REP トポロジの情報を表示します。
ステップ 6	**end** 例： `Device# end`	特権 EXEC モードを終了します。

REP の SNMP トラップ設定

REP 固有のトラップを送信して、簡易ネットワーク管理プロトコル（SNMP）サーバーにリンクの動作状態の変更およびすべてのポート役割の変更を通知するようにルータを設定できます。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**snmp mib rep trap-rate** *value* 例： `Device(config)# snmp mib rep trap-rate 500`	スイッチで REP トラップの送信を有効にして、1 秒あたりのトラップの送信数を設定します。 • 1 秒あたりのトラップの送信数を入力します。範囲は 0 ～ 1000 です。デフォルトは 0（制限なし、発生するたびにトラップが送信される）です。
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show running-config** 例： `Device# show running-config`	（任意）実行コンフィギュレーションを表示します。これを使用して REP トラップ コンフィギュレーションを検証できます。
ステップ 6	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）スイッチ スタートアップ コンフィギュレーション ファイルに設定を保存します。

Resilient Ethernet Protocol Fast

Resilient Ethernet Protocol（REP）Fast を使用すると、スイッチの銅線ギガビットイーサネット（GE）ポートでのリンク障害の検出とコンバージェンスを高速化できます。

REP は当初、ファストイーサネット（FE 10/100）ポート用に設計されました。FE ポートのリンクダウン検出時間は 10 ミリ秒（ms）で、コンバージェンス時間は約 50 ms です。ファイバ GE ポートでもリンクダウン検出時間は 10 ms ですが、GE 銅線インターフェイスでは、リンクドロップ検出時間および回復時間が 750 ～ 350 ms となります。その結果、GE 光ファイバインターフェイスでは、対応する銅線インターフェイスよりもはるかに迅速にリンク損失と回復を検出できます。つまり、GE 銅線インターフェイスを使用すると、REP のコンバージェンス時間が大幅に長くなります。

リンクダウン検出時間を改善するため、REP インターフェイスが REP Fast モードに設定されている場合は、より高速なリンク障害検出（5 ～ 10 ms 以内）をトリガーするビーコンメカニズムが実装されています。スイッチには、REP インターフェイスごとに 2 つのタイマーがあります。最初のタイマーは 3 ms ごとにトリガーされ、ビーコンフレームをネイバーノードに送信します。フレームの送受信が成功すると、両方のタイマーがリセットされます。送信後にパケットが受信されない場合は、2 番目のタイマーがトリガーされ、10 ms 以内に受信を確認し

ます。パケットが受信されない場合、タイマーの期限が切れたときにリンクダウンメッセージがスイッチに送信されます。

REP Fast は、個々のリンク単位で動作します。REP プロトコルには影響しません。REP Fast が機能するには、リンクの両端で REP Fast をサポートする必要があります。REP Fast は REP 用に設定された任意のインターフェイスリンクペアで使用できますが、もともとはギガビット銅線リンクの問題を解決するために作成されました。REP Fast によって、ギガビット銅線インターフェイスでのリンク障害検出がより迅速になります。

REP リングには、通常の REP リンクと REP Fast リンクを混在させることができます。REP Fast を使用するインターフェイスは、通常動作の一環として 1 秒間に 3,000 パケットを送信します。REP Fast を有効にしても設定されたインターフェイスのペアでのみ動作するため、REP リングサイズには影響しません。REP Fast はビーコンフレームを生成する必要があるため、1 台の REP ノード上で一度に REP Fast を設定できるインターフェイスは 6 つのみです。

ネイバーが確認応答し、REP Fast モードに設定された場合、50 ms 以内にコンバージェンスが発生します。ネイバースイッチが REP Fast 機能をサポートしていない場合は、通常の REP モードを使用してリンクのアップ/ダウンを検出する必要があります。この場合、リンクの両端で Fast モードを無効にする必要があります。

REP Fast の設定について詳しくは、このガイドの「REP Fast の設定」を参照してください。

REP Fast の設定

REP Fast を設定するには、次の手順を実行します。

始める前に

「REP の設定」の説明に従って、スイッチで REP を有効にし、REP トポロジを設定します。

ステップ 1 グローバル コンフィギュレーション モードを開始します。

configure terminal

ステップ 2 インターフェイスを指定してインターフェイス設定モードを開始します。

interface *interface-id*

ステップ 3 REP Fast を有効にします。

REP fastmode

ステップ 4 特権 EXEC モードに戻ります。

end

例

```
gabitEthernet 1/0/1
switch-RJ(config-if)#rep seg
```

```
switch-RJ(config-if)#rep segment ?
<1-1024> Between 1 and 1024

switch-RJ(config-if)#rep segment 10
switch-RJ(config-if)#rep fastmode
switch(config)#int <interface number>
switch(config-if)#
switch(config-if)#rep ?
  fastmode       REP fastmode
switch (config-if)#rep fastmode ?
  <cr>  <cr>

switch#sh run int <interface number>
Building configuration...

Current configuration : 89 bytes
!
interface <interface number>
 switchport mode trunk
 rep segment <segment id>
 rep fastmode
end
switch#

switch#sh run int <interface number>
Building configuration...

Current configuration : 89 bytes
!
interface <interface number>
 switchport mode trunk
 rep segment <segment id>
 rep fastmode
end
```

Resilient Ethernet Protocol 設定のモニタリング

次の例では、**show interface**［*interface-id*］**rep**［**detail**］コマンドの出力を示します。この表示では、アップリンクポートの REP 設定とステータスを示します。

```
Device# show interfaces GigabitEthernet1/0/4 rep detail

GigabitEthernet1/0/4 REP enabled
Segment-id: 3 (Primary Edge)
PortID: 03010015FA66FF80
Preferred flag: No
Operational Link Status: TWO_WAY
Current Key: 02040015FA66FF804050
Port Role: Open
Blocked VLAN: <empty>
Admin-vlan: 1
REP-ZTP Status: Disabled
Preempt Delay Timer: disabled
Configured Load-balancing Block Port: none
Configured Load-balancing Block VLAN: none
STCN Propagate to: none
LSL PDU rx: 999, tx: 652
HFL PDU rx: 0, tx: 0
BPA TLV rx: 500, tx: 4
```

```
BPA (STCN, LSL) TLV rx: 0, tx: 0
BPA (STCN, HFL) TLV rx: 0, tx: 0
EPA-ELECTION TLV rx: 6, tx: 5
EPA-COMMAND TLV rx: 0, tx: 0
EPA-INFO TLV rx: 135, tx: 136
```

次の例では、**show interface** [*interface-id*] **rep** [**detail**] コマンドの出力を示します。この表示では、ダウンリンクポートの REP 設定とステータスを示します。

```
Device#show interface GigabitEthernet1/0/5 rep detail
GigabitEthernet1/0/5   REP enabled
Segment-id: 1 (Segment)
PortID: 019B380E4D9ACAC0
Preferred flag: No
Operational Link Status: NO_NEIGHBOR
Current Key: 019B380E4D9ACAC0696B
Port Role: Fail No Ext Neighbor
Blocked VLAN: 1-4094
Admin-vlan: 1
REP-ZTP Status: Disabled
Preempt Delay Timer: 100 sec
LSL Ageout Timer: 2000 ms
LSL Ageout Retries: 5
Configured Load-balancing Block Port: 09E9380E4D9ACAC0
Configured Load-balancing Block VLAN: 1-100
STCN Propagate to: segment 25
LSL PDU rx: 292, tx: 340
HFL PDU rx: 0, tx: 0
BPA TLV rx: 0, tx: 0
BPA (STCN, LSL) TLV rx: 0, tx: 0
BPA (STCN, HFL) TLV rx: 0, tx: 0
EPA-ELECTION TLV rx: 0, tx: 0
EPA-COMMAND TLV rx: 0, tx: 0
EPA-INFO TLV rx: 0, tx: 0
```

次の例では、**show rep topology** [**segment** *segment-id*] [**archive**] [**detail**] コマンドを示します。この表示では、すべてのセグメントの REP トポロジ情報を示します。

```
Device# show rep topology

REP Segment 1
BridgeName       PortName     Edge Role
---------------- ----------   ---- ----
10.64.106.63     Gi1/0/4      Pri  Open
10.64.106.228    Gi1/0/4           Open
10.64.106.228    Gi1/0/3           Open
10.64.106.67     Gi1/0/3           Open
10.64.106.67     Gi1/0/4           Alt
10.64.106.63     Gi1/0/4      Sec  Open

REP Segment 3
BridgeName       PortName     Edge Role
---------------- ----------   ---- ----
10.64.106.63     Gi1/011     Pri  Open
SVT_3400_2       Gi1/0/3           Open
SVT_3400_2       Gi1/0/4           Open
10.64.106.68     Gi1/0/2           Open
10.64.106.68     Gi1/0/1           Open
10.64.106.63     Gi1/0/2      Sec  Alt
```

Resilient Ethernet Protocol の機能履歴

以下の表に、このガイドに記載されている機能のリリースおよび関連情報を示します。この機能は、特に明記されていない限り、最初のリリース以降のすべてのリリースで使用できます。

リリース	機能	機能情報
Cisco IOS XE Cupertino 17.9.x	Resilient Ethernet Protocol Fast	この機能は、このリリースより Cisco Catalyst IE9300 高耐久性シリーズ スイッチで使用できるようになりました。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。