



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

最終更新：2025年5月30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

- 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](#) [英語] 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](#) [英語] 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るには、[Cisco Warranty Finder](#) にアクセスしてください。

シスコバグ検索ツール

[シスコのバグ検索ツール](#) (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

シスコの技術マニュアル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。



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

第 1 章

Parallel Redundancy Protocol 1

PRP について 1

スイッチの役割 3

PRP チャンネル 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

PRP インターフェイスの TrustSec 5

PRP インターフェイスでの TrustSec の設定 6

CTS および PRP の show コマンド 7

TrustSec デバッグコマンド 10

前提条件 11

注意事項と制約事項 11

デフォルト設定 14

PRP チャンネルおよびグループの作成 14

例 16

監視フレームの VLAN タギングを使用した PRP チャンネルの設定 17

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 20

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 21

PRP チャンネルおよびグループの無効化	22
Syslog のエラーおよび警告メッセージ	23
PRP ログ間隔の設定	23
設定例	24
設定の確認	36
関連資料	38
機能の履歴	38

第 2 章

PRP を介した PTP	41
PRP を介した PTP	41
サポートされる PTP のプロファイルとクロックモード	44
PRP RedBox のタイプ	45
LAN-A および LAN-B の障害検出と処理	51
PRP を介した PTP の CLI コマンド	51
show ptp clock running	52
show prp channel detail	52
show prp statistics ptpPacketStatistics	52
show ptp lan port int	53
ptp clock boundary domain	53
PRP を介した PTP 機能の履歴	54

第 3 章

Resilient Ethernet Protocol	55
Resilient Ethernet Protocol	55
リンク完全性	57
高速コンバージェンス	58
VLAN 負荷分散	58
スパニングツリーとの相互作用	60
Resilient Ethernet Protocol (REP) ネゴシエート (廃止)	60
REP ポート	61
Resilient Ethernet Protocol Fast	62
高速 REP の設定	63
REP ゼロタッチプロビジョニング	64

REP およびデイゼロ	64
REP ZTP の概要	67
Resilient Ethernet Protocol の設定	68
REP のデフォルト設定	68
REP の設定ガイドラインと制限事項	69
REP ZTP 設定時の注意事項	71
REP 管理 VLAN の設定	72
REP インターフェイスの設定	73
VLAN 負荷分散の手動によるプリエンプションの設定	77
REP の SNMP トラップ設定	78
REP ZTP の設定	79
Resilient Ethernet Protocol 設定の監視	80
REP ZTP ステータスの表示	82
Resilient Ethernet Protocol の機能履歴	85

 第 4 章

Media Redundancy Protocol	87
Media Redundancy Protocol	87
MRP モード	88
プロトコルの動作	88
Media Redundancy Automanager	90
ライセンス	91
IE9300 スタック上の MRP	91
MRP-STP の相互運用性	92
前提条件	92
注意事項と制約事項	92
デフォルト設定	94
TIA 15 または STEP7 を使用した Profinet MRP モードの設定	94
PROFINET GSD ファイルのインストール	94
PROFINET MRP の起動	95
Simatic Step 7 または TIA 15 ポータルを使用した Profinet の管理	96
MRP CLI モードの設定	100

MRP マネージャの設定 101

設定例 105

設定の確認 107

機能の履歴 107

第 5 章

高可用性シームレス冗長性 109

高可用性シームレス冗長性 109

ループ回避 111

HSR RedBox の動作モード 111

HSR SAN モード 111

HSR の CDP と LLDP 112

HSR アップリンクの冗長性に関する機能拡張 112

注意事項と制約事項 115

デフォルト設定 117

HSR リングの設定 119

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 120

設定の確認 121

設定例 121

関連資料 125

機能の履歴 125



第 1 章

Parallel Redundancy Protocol

- PRP について (1 ページ)
- PRP インターフェイスの TrustSec (5 ページ)
- 前提条件 (11 ページ)
- 注意事項と制約事項 (11 ページ)
- デフォルト設定 (14 ページ)
- PRP チャンネルおよびグループの作成 (14 ページ)
- 監視フレームの VLAN タギングを使用した PRP チャンネルの設定 (17 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 (20 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 (21 ページ)
- PRP チャンネルおよびグループの無効化 (22 ページ)
- Syslog のエラーおよび警告メッセージ (23 ページ)
- 設定例 (24 ページ)
- 設定の確認 (36 ページ)
- 関連資料 (38 ページ)
- 機能の履歴 (38 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-E 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。

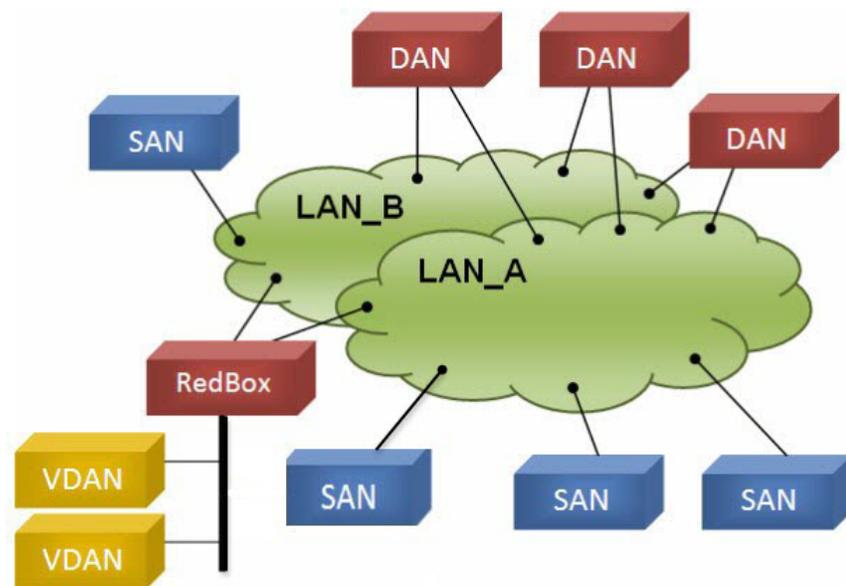
PRPは異なる方式を使用します。この方式では、2つのネットワーク インターフェイスを2つの独立した分離された並列ネットワーク（LAN-AとLAN-B）に接続することで、（ネットワーク要素ではなく）エンドノードが冗長性を実装します。これらのデュアル接続ノード（DAN）のそれぞれには、ネットワーク内の他のすべてのDANへの冗長経路があります。

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。経路の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経路に流れ続け、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。

スイッチの役割

IE-9320-26S2C-A、IE-9320-26S2C-E、IE-9320-22S2C4X-A、および IE-9320-22S2C4X-E 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 チャンネル

PRP チャンネルまたはチャンネルグループは、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。チャンネルグループでは、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 チャン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、チャンネルもダウンします。サポートされる PRP チャン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 チャンネル番号	IE9300 シリーズ
PRP チャンネル 1	Gi1/0/21 (LAN-A) および Gi1/0/22 (LAN-B)
PRP チャンネル 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 チャン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 エントリのスーパー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 チャンネルから 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。

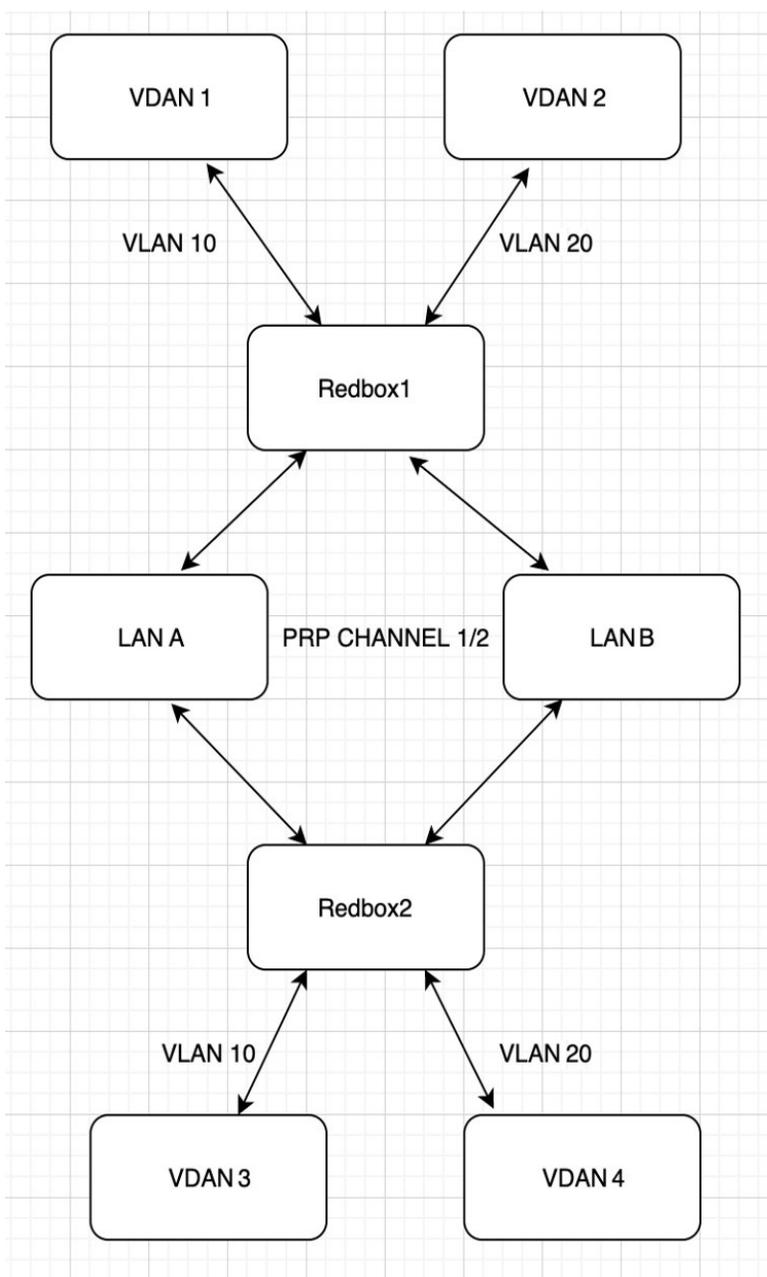
VDAN の接続された RedBox は、これらの VDAN の代理で監視フレームを送信する必要があります。他のすべてのポートに着信し、PRP チャンネルポートから送信されるトラフィックの場合、スイッチは、送信元 MAC アドレスを学習して VDAN テーブルに追加し、それらのアドレスに対応する監視フレームの送信を開始します。学習された VDAN エントリにはエージングが適用されます。

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 チャン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 チャンネル 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 チャンネルを通過します。



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 チャンネルの設定 \(17 ページ\)](#) を参照してください。

PRP インターフェイスの TrustSec

PRP チャンネルのメンバーインターフェイスで Cisco TrustSec (CTS) を設定できます。この機能は、IE-9320-26S2C-A、IE-9320-26S2C-E、IE-9320-22S2C4X-A、および IE-9320-22S2C4X-E スイッチでのみサポートされます。

TrustSec は物理インターフェイスでのみサポートされるため、論理 PRP チャネルインターフェイスで TrustSec を設定することはできません。PRP チャネルには 2 つのインターフェイスが含まれます (Gi1/0/21 と Gi1/0/22 など)。PRP チャネルのメンバーであるインターフェイスで TrustSec を設定するには、次の条件が満たされていることを確認します。

- TrustSec を使用するには、Network Advantage ライセンスが必要です。
- PRP チャネルに含める前に、まず各インターフェイスで TrustSec を設定します。
- LAN-A と LAN-B でインラインタギングと伝播を想定どおりに行えるようにするには、両方の PRP チャネルインターフェイスの TrustSec 設定を同じにする必要があります。



(注) CTS + Security Association Protocol (SAP) および CTS + MACsec Key Agreement (MKA) 方式は、PRP インターフェイスではサポートされていません。

PRP インターフェイスでの TrustSec の設定

ここでは、PRP インターフェイスでの TrustSec の設定例を示します。PRP チャネルインターフェイスを設定するには、個々のインターフェイスを設定するか、または **interface range <>** を使用します。

有効な設定

次に、各インターフェイスで TrustSec を一度に 1 つずつ設定し、その個々のインターフェイスを PRP チャネルの一部にする例を示します。

```
switch#configure terminal
switch(config)#int gi1/0/21
switch(config-if)#switchport mode access
switch(config-if)#switchport access vlan 30
switch(config-if)#cts manual
switch(config-if-cts-manual)#policy static sgt 1000 trusted
switch(config-if-cts-manual)#exit
switch(config-if)#prp-channel-group 1
Creating a PRP-channel interface PRP-channel 1
```

```
switch(config-if)#
switch(config-if)#int gi1/0/22
switch(config-if)#switchport mode access
switch(config-if)#switchport access vlan 30
switch(config-if)#cts manual
switch(config-if-cts-manual)#policy static sgt 1000 trusted
switch(config-if-cts-manual)#exit
switch(config-if)#prp-channel-group 1
switch(config-if)#end
```

次に、インターフェイスの範囲で TrustSec を設定し、インターフェイスを PRP チャネルの一部にする例を示します。

```
switch#configure terminal
switch(config-if)#int range gi1/0/21-1/0/22
```

```
switch(config-if)#switchport mode access switch
switch(config-if)#switchport access vlan 30
switch(config-if)#cts manual
switch(config-if-cts-manual)#policy static sgt 1000 trusted
switch(config-if-cts-manual)#exit
switch(config-if)#prp-channel-group 1
Creating a PRP-channel interface PRP-channel 1
```

無効な設定

次の例の設定は、TrustSec の設定を試みる前にインターフェイスが PRP チャンネルのメンバーとして設定されているため、無効です。

```
switch#configure terminal
switch(config)#int gi1/0/21
switch(config-if)#prp-channel-group 1
Creating a PRP-channel interface PRP-channel 1

switch(config-if)#switchport mode access
switch(config-if)#switchport access vlan 30
switch(config-if)#cts manual
Interface is a member of a port channel. To change CTS first remove from port channel.
switch(config-if)#
```

CTS および PRP の show コマンド

ここでは、PRP メンバーインターフェイスで TrustSec を設定するときには使用できる **show** コマンドと、いくつかのコマンド出力の例を示します。

- **show cts interface summary**
- **show cts pacs**
- **show cts interface <>**
- **show cts role-based counters**
- **show prp channel detail**
- **show prp statistics ingressPacketStatistics**
- **show prp statistics egressPacketStatistics**

次に、**show cts interface summary** コマンドの出力例を示します。

```
switch#show cts interface summary
CTS Interfaces
-----
Interface                               Mode    IFC-state dot1x-role peer-id    IFC-cache
Critical-Authentication
-----
Gi1/0/21                                MANUAL  OPEN      unknown   unknown   invalid   Invalid
Gi1/0/22                                MANUAL  OPEN      unknown   unknown   invalid   Invalid

R1#show cts pacs
AID: 51F577DCE176855650F2F5609418AC6
PAC-Info:
  PAC-type = Cisco Trustsec
  AID: 51F577DC7E176855650F2F5609418AC6
```

```

I-ID: petra3400ipv4
A-ID-Info: Identity Services Engine
Credential Lifetime: 09:06:08 UTC Wed Nov 01 2023
PAC-Opaque:
000200B8000300010004001051F577DC7E176855650F2F5609418AC60006009C000301002EBB79441FEE97B0E0B339B9036F9C710000001364C8D
1A000093A8054BC5FA1780A24E23B60A4BFF46AF47A317EB20391BFCA6F0CABA7F66393F05799A3B0EAB602B54749DCF7225A45FDD1349A81977D857B9C3
1959A2B54CFC4505CD903D84394E69E5795DB1543BB575FB8D51A6FA021FB5E6A0C296F8CA21318377688073516714125D38973D9BF2A66792E3AD10CA05C3
E739CA1
Refresh timer is set for 12w4d
R1#show cts interface GigabitEthernet1/0/21
Global Dot1x feature is Disabled
Interface GigabitEthernet1/0/21:
  CTS is enabled, mode:    MANUAL
  IFC state:              OPEN
  Interface Active for 00:03:25.772
  Authentication Status:  NOT APPLICABLE
  Peer identity:          "unknown"
  Peer's advertised capabilities: ""
  Authorization Status:   SUCCEEDED
  Peer SGT:               30
  Peer SGT assignment:   Trusted
  SAP Status:             NOT APPLICABLE
  Propagate SGT:         Enabled
  Cache Info:
    Expiration            : N/A
    Cache applied to link : NONE

  Statistics:
    authc success:        0
    authc reject:         0
    authc failure:        0
    authc no response:    0
    authc logoff:         0
    sap success:          0
    sap fail:             0
    authz success:        0
    authz fail:           0
    port auth fail:       0

L3 IPM:  disabled.

```

次に、**show cts role-based counters** コマンドの出力例を示します。

```

switch# show cts role-based counters
Role-based IPv4 counters
From    To      SW-Denied  HW-Denied  SW-Permitt  HW-Permitt  SW-Monitor
HW-Monitor
*       *       0          0          0           0           0
0
122    0       0          0          0           0           0
0
200    0       0          0          0           2845        0
0
201    130    0          0          0           0           0
0
130    200    0          0          0           2845        0
0

```

次に、**show prp channel detail** コマンドの出力例を示します。

```
switch#show prp channel 1 summary
Flags:  D - down          P - bundled in prp-channel
        R - Layer3       S - Layer2
        U - in use
```

```
Number of channel-groups in use: 1
Group  PRP-channel  Ports
-----+-----+-----
1      PR1(SU)      Gi1/0/21(P), Gi1/0/22(P)
```

```
R1#show prp channel 1 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 = 1/1 Port state = Inuse
     Protocol = Enabled
  2) Port: Gi1/0/22
     Logical slot/port = 1/2 Port state = Inuse
     Protocol = Enabled
```

次に、**show prp statistics ingressPacketStatistics** コマンドの出力例を示します。

```
switch#sh prp statistics ingressPacketStatistics
PRP prp_maxchannel 2 INGRESS STATS:
PRP channel-group 1 INGRESS STATS:
  ingress pkt lan a: 1010
  ingress pkt lan b: 1038
  ingress crc lan a: 0
  ingress crc lan b: 0
  ingress danp pkt acpt: 20
  ingress danp pkt dscrd: 20
  ingress supfrm rcv a: 382
  ingress supfrm rcv b: 390
  ingress over pkt a: 0
  ingress over pkt b: 0
  ingress pri over pkt a: 0
  ingress pri over pkt b: 0
  ingress oversize pkt a: 0
  ingress oversize pkt b: 0
  ingress byte lan a: 85127
  ingress byte lan b: 85289
  ingress wrong lan id a: 402
  ingress wrong lan id b: 402
  ingress warning lan a: 1
  ingress warning lan b: 1
  ingress warning count lan a: 137
  ingress warning count lan b: 137
  ingress unique count a: 0
  ingress unique count b: 0
  ingress duplicate count a: 20
  ingress duplicate count b: 20
  ingress multiple count a: 0
  ingress multiple count b: 0

PRP channel-group 2 INGRESS STATS:
  ingress pkt lan a: 0
  ingress pkt lan b: 0
  ingress crc lan a: 0
```

```

ingress crc lan b: 0
ingress danp pkt acpt: 0
ingress danp pkt dscrd: 0
ingress supfrm rcv a: 0
ingress supfrm rcv b: 0
ingress over pkt a: 0
ingress over pkt b: 0
ingress pri over pkt a: 0
ingress pri over pkt b: 0
ingress oversize pkt a: 0
ingress oversize pkt b: 0
ingress byte lan a: 0
ingress byte lan b: 0
ingress wrong lan id a: 0
ingress wrong lan id b: 0
ingress warning lan a: 0
ingress warning lan b: 0
ingress warning count lan a: 0
ingress warning count lan b: 0
ingress unique count a: 0
ingress unique count b: 0
ingress duplicate count a: 0
ingress duplicate count b: 0
ingress multiple count a: 0
ingress multiple count b: 0

```

次に、**show prp statistics egressPacketStatistics** コマンドの出力例を示します。

```

switch#sh prp statistics egressPacketStatistics
PRP channel-group 1 EGRESS STATS:
  duplicate packet: 20
  supervision frame sent: 427
  packet sent on lan a: 934
  packet sent on lan b: 955
  byte sent on lan a: 96596
  byte sent on lan b: 96306
  egress packet receive from switch: 517
  overrun pkt: 0
  overrun pkt drop: 0
PRP channel-group 2 EGRESS STATS:
  duplicate packet: 0
  supervision frame sent: 0
  packet sent on lan a: 0
  packet sent on lan b: 0
  byte sent on lan a: 0
  byte sent on lan b: 0
  egress packet receive from switch: 0
  overrun pkt: 0
  overrun pkt drop: 0

```

TrustSec デバッグコマンド

ここでは、PRP メンバーインターフェイスで TrustSec をトラブルシューティングするときに見える **debug** コマンドを示します。

- **debug prp errors**
- **debug prp events**
- **debug prp detail**

- `debug cts error`
- `debug cts aaa`
- `debug cts all`

前提条件

- IE-9320-26S2C-A、IE-9320-26S2C-E、IE-9320-22S2C4X-A、または IE-9320-22S2C4X-E 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 パケットが破棄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、**system mtu 1506** と設定して PRP LAN-A と LAN-B ネットワーク内のスイッチの MTU サイズを 1506 に増やします。
- 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、チャンネル内に 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。
- チャン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。

- 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 UDL D を無効にする必要があります。
- **spanning-tree bpdudfilter 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 BPD U フィルタは、すべての入出力 BPD U トラフィックを破棄します。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-E 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ンネルの帯域幅の 90% を超えることはできません。
- 負荷分散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 チャンネルは、作成するまでスイッチに存在しません。[PRP チャンネル \(3 ページ\)](#) 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 チャンネルおよびグループの作成

スイッチで PRP チャン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 チャンネル \(3 ページ\)](#) 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 \(11 ページ\)](#) と [注意事項と制約事項 \(11 ページ\)](#) を確認してください。
- PRP チャンネルを作成する前に、PRP チャン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 チャン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。チャンネル 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. 冗長チャンネルのループ検出を無効にします。
8. 冗長チャンネルの 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 チャンネルグループを作成します。
10. PRP チャンネルを起動します。
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 bpdupfilter 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

手順

-
- 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 チャン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。チャンネル 1 の場合は、次のように入力します。
- interface range GigabitEthernet1/1/0/21-22**
- チャンネル 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 チャンネル 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 冗長チャンネルのループ検出を無効にします。

no keepalive

ステップ 8 冗長チャンネルの 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 チャン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ン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 チャンネルを起動します。

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 bpdudfilter を設定します。

spanning-tree bpdudfilter 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 トラフィックを破棄します。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 チャンネルを作成する方法、PRP チャン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 チャン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 チャンネルの設定

VLAN タグ付き監視フレームを使用したスイッチで PRP チャン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 チャンネル \(3 ページ\)](#) 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 \(11 ページ\)](#) と [注意事項と制約事項 \(11 ページ\)](#) を確認してください。
- PRP チャンネルを作成する前に、PRP チャン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 チャン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。チャンネル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. 冗長チャンネルのループ検出を無効にします。
7. 冗長チャンネルの 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 チャンネルグループを作成します。
9. PRP チャンネルを起動します。
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 bpdudfilter 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

手順

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 チャン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。チャンネル1の場合は、次のように入力します。

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

チャンネル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 チャンネル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 冗長チャンネルのループ検出を無効にします。

no keepalive

ステップ 7 冗長チャンネルの 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 チャン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ン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 チャンネルを起動します。

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 bpdupfilter を設定します。

spanning-tree bpdupfilter enable

スパンニングツリー BPDU フィルタは、すべての入出力 BPDU トラフィックを破棄します。このコマンドは、ネットワーク内に独立したスパン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 bpdupfilter 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

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

手順

- 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

手順

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 ]
```

チャンネルグループを指定しない場合は、すべての PRP チャン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 \(20 ページ\)](#) 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 チャン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 チャン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

手順

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 チャン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-E 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 \(23 ページ\)](#) 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

手順

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 \(23 ページ\)](#) 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。


```
!  
!  
!  
!  
!  
!  
!  
!  
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 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
!

```



```

!
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

```



```

!
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 チャン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 e2transparent
!
!
!
!
!
!
!
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
```



```
!  
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
<code>show prp channel {1 2 [detail status summary] detail status summary}</code>	指定した PRP チャンネルに対する設定の詳細を表示します。
<code>show prp control {VdanTableInfo ptpLanOption ptpProfile supervisionFrameLifeCheckInterval supervisionFrameOption supervisionFrameRedboxMacaddress supervisionFrameTime}</code>	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。
<code>show prp node-table [channel-group <group> detail]</code>	PRP ノードテーブルを表示します。
<code>show prp statistics {egressPacketStatistics ingressPacketStatistics nodeTableStatistics pauseFrameStatistics ptpPacketStatistics}</code>	PRP コンポーネントの統計情報を表示します。
<code>show prp vdan-table [channel-group <group> detail]</code>	PRP VDAN テーブルを表示します。
<code>show interface prp-channel {1 2}</code>	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 チャン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 チャン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 チャンネルに 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)#
```

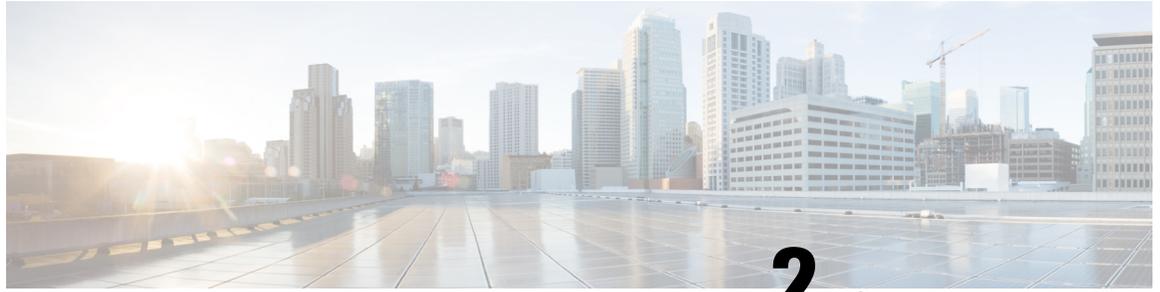
関連資料

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-E 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-E で使用可能になりました。

リリース	機能名	機能情報
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 (41 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 (44 ページ)
- PRP RedBox のタイプ (45 ページ)
- LAN-A および LAN-B の障害検出と処理 (51 ページ)
- PRP を介した PTP の CLI コマンド (51 ページ)
- PRP を介した PTP 機能の履歴 (54 ページ)

PRP を介した PTP

高精度時間プロトコル (PTP) は、並列冗長プロトコル (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-E スイッチでサポートされています。

PRP は、冗長性により高可用性を PTP に提供します。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つの独立した経路を介した並列伝送による冗長性を実現する PRP 方式は、他の通信とは異なり、PTP では機能しません。ひとつのフレームに生じる遅延は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せん。
- 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。

- 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を転送する義務を負いません。

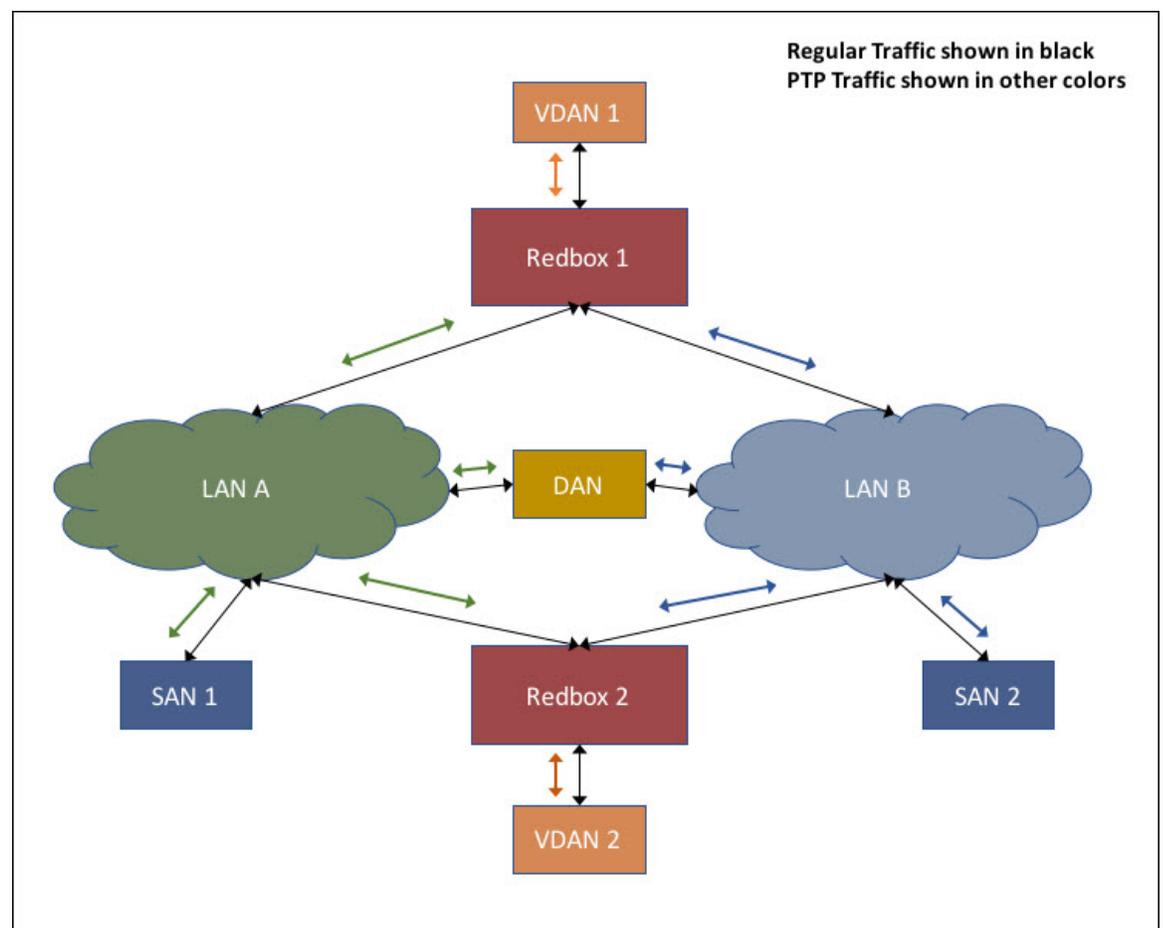
LAN-A および LAN-B を介した PTP をサポートする前は、PTP トラフィックは上記の PTP および並列伝送の問題を回避するために、LAN-A でのみ許可されていました。ただし、LAN-A が停止すると、PTP 同期は失われていました。基礎となる PRP インフラストラクチャによって提供される冗長性の利点を PTP で活用できるようにするため、PRP ネットワーク上の PTP パケットは他のタイプのトラフィックとは異なる方法で処理されます。

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



この図では、VDAN1 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「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 チャン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-E 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 チャンネル 1 に対応。
- Gi1/0/23 および Gi1/0/24 : PRP チャンネル 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 チャンネル」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	あり	E2E を使用するダブル接続 BC (DABC) としての PRP RedBox
	E2E TC	なし	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	あり	P2P を使用するダブル接続 BC (DABC) としての PRP RedBox
	P2P TC	あり	P2P を使用するダブル接続 TC (DATC) としての PRP RedBox

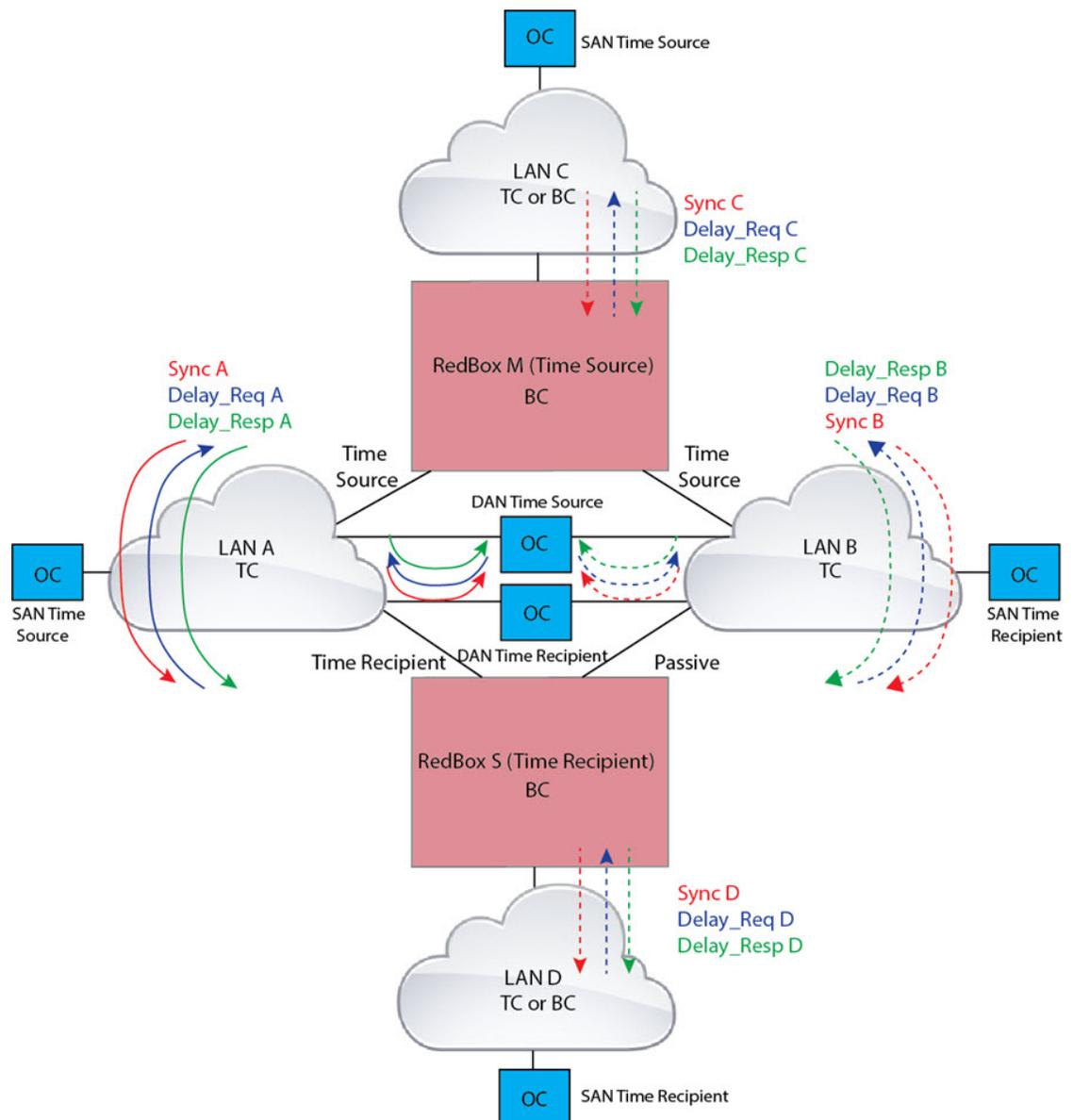
PRP RedBox のタイプ

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 チャン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。

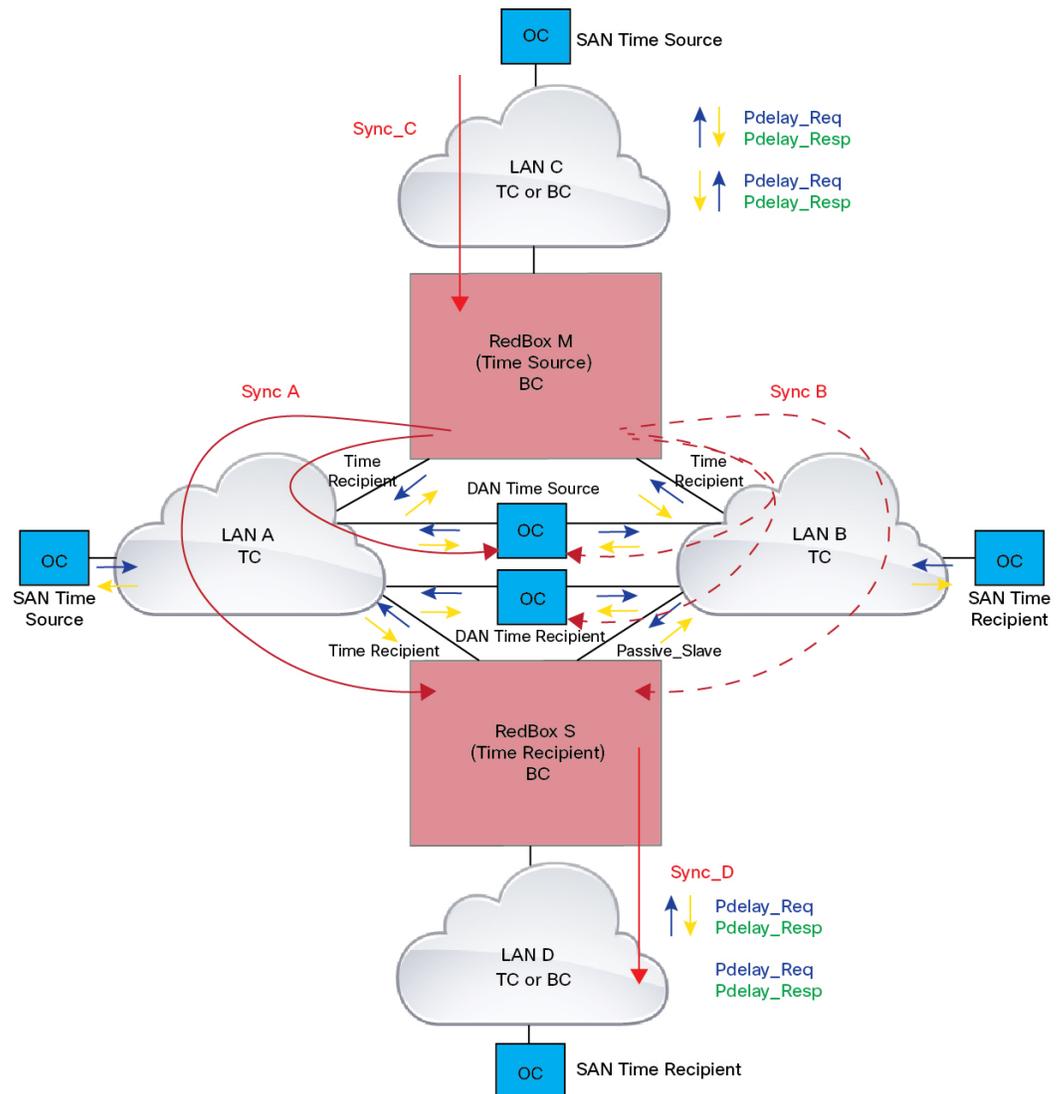
これは、計算された遅延とオフセットを維持しますが、ローカルクロックの操作を実行しないという意味でパッシブです。遅延とオフセットの情報をすぐに利用できるようにすることで、ポート A で時刻源への接続が失われた場合に、その役割を時刻受信者に円滑に変更できます。

PTP 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 LANC 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、通常の実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 経路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）。

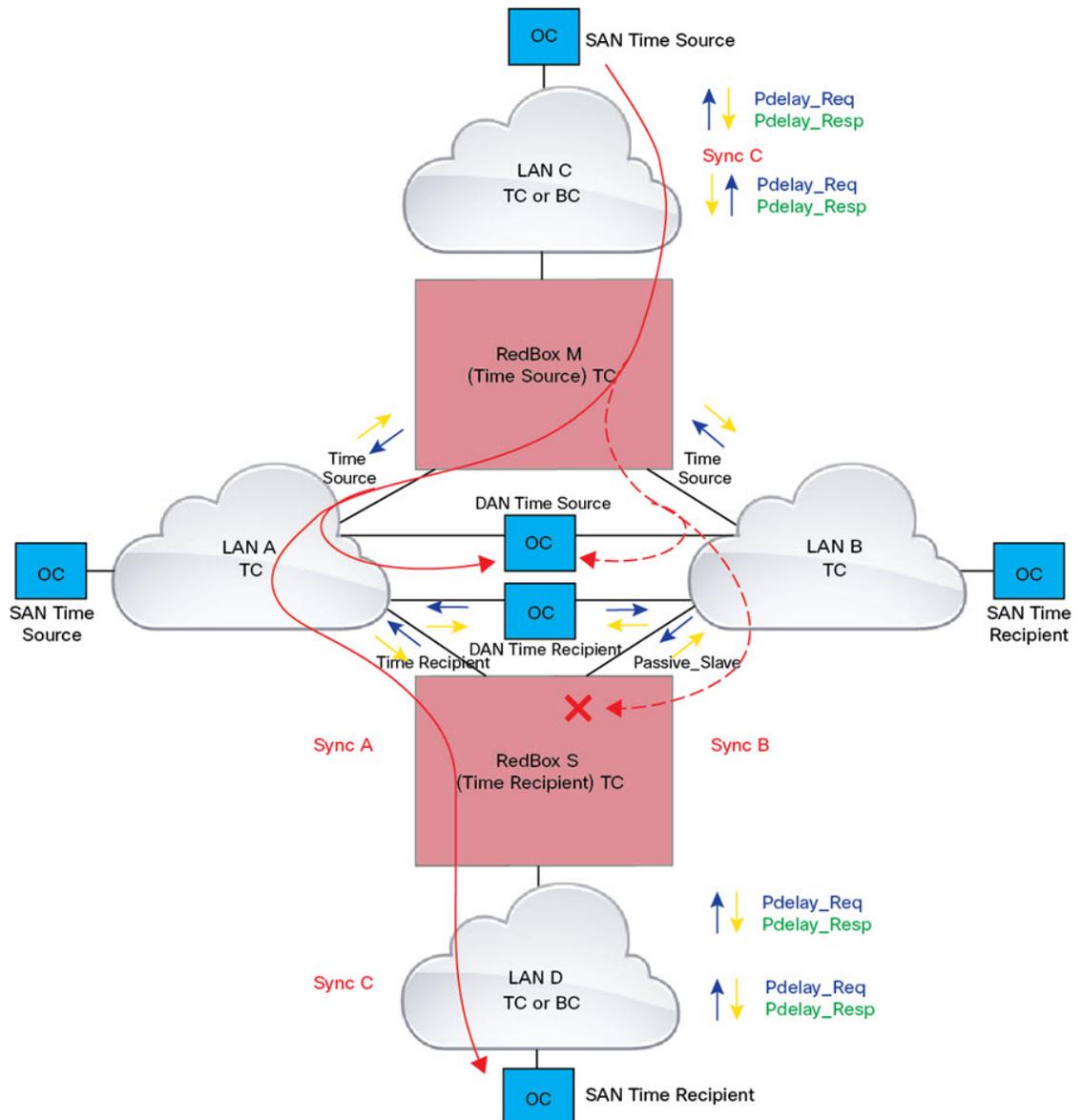
- ポート B は PASSIVE_SLAVE 状態です。ポート A と同様に時刻源からの遅延とオフセットを維持しますが、ローカルクロックに対する操作は実行しません。すべての同期情報を使用できるようにすることで、ポート A が GM との通信を失った場合に、新しい時刻受信者として円滑に引き継ぐことができます。

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 LANC 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 経路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円滑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 内で破棄された。

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 計算が開始されます。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、状態の変更は不可分操作で行われます。

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、迅速かつ円滑に行う必要があります。

LAND の SAN 時刻受信者も、RedBox S でのタイミングの変更を確認し、新しいクロックに収束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、変更は通常円滑に行われます。

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

                Name      Tx Mode  Role      Transport  State      Sessions  PTP Master
                dyn1     mcast   negotiated Ethernet    Slave      1         UNKNOWN
                dyn2     mcast   negotiated Ethernet    Passive Slave 1         UNKNOWN
```

show prp channel detail

両方のポートチャン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、受信時の破棄も表示されます。

```
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 チャンネル 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 チャンネル 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	並列冗長プロトコル (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-E 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

Resilient Ethernet Protocol

- [Resilient Ethernet Protocol](#) (55 ページ)
- [Resilient Ethernet Protocol Fast](#) (62 ページ)
- [REP ゼロタッチプロビジョニング](#) (64 ページ)
- [Resilient Ethernet Protocol の設定](#) (68 ページ)
- [Resilient Ethernet Protocol 設定の監視](#) (80 ページ)
- [Resilient Ethernet Protocol の機能履歴](#) (85 ページ)

Resilient Ethernet Protocol

Resilient Ethernet Protocol (REP) はシスコ独自のプロトコルで、スパン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 負荷分散をサポートします。



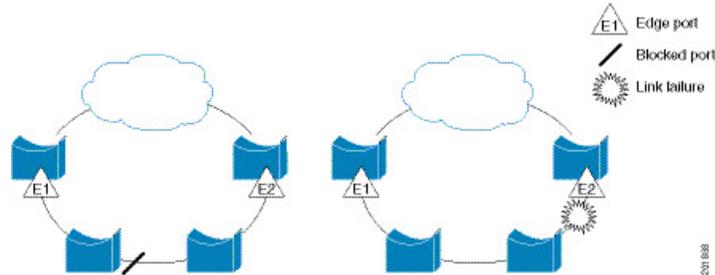
(注) REP は、Network Essentials ライセンスの Cisco Catalyst IE9300 高耐久性シリーズスイッチの Cisco IOS XE Cupertino 17.9.x 以降のリリースでサポートされています。

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な場合、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転送状態に戻り、ネットワークの中断を最小限に抑えます。

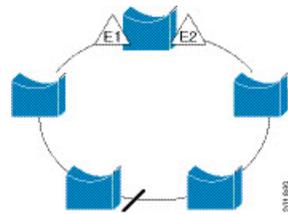
図 6: REP オープンセグメント



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



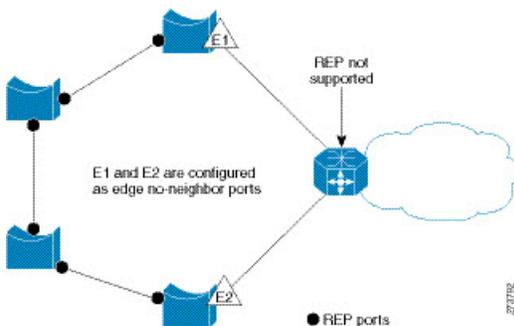
REP セグメントには、次のような特徴があります。

- 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 でブロック状態となります。VLAN 負荷分散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 のブロック状態を制御します。
- 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) を非ネイバリエッジポートとして設定できます。非ネイバリエッジポートは、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: 非ネイバリエッジポート



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、ネットワーク内で転送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 対応ネイバリエッジポートを検出して、セグメント内の接続性を確立します。ネイバリエッジポートが検出されるまで、インターフェイス上ですべての VLAN がブロックされます。ネイバリエッジポートが特定されたあと、REP が代替ポートとなるネイバリエッジポートと、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、スパン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リエッジポート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。

- ネイバリエッジポートに同じセグメント ID がない
- 複数のネイバリエッジポートに同じセグメント 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一貫して 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ドします。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ドされます。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ドを制御することができます。

VLAN 負荷分散

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 負荷分散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 負荷分散を設定する際に、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。

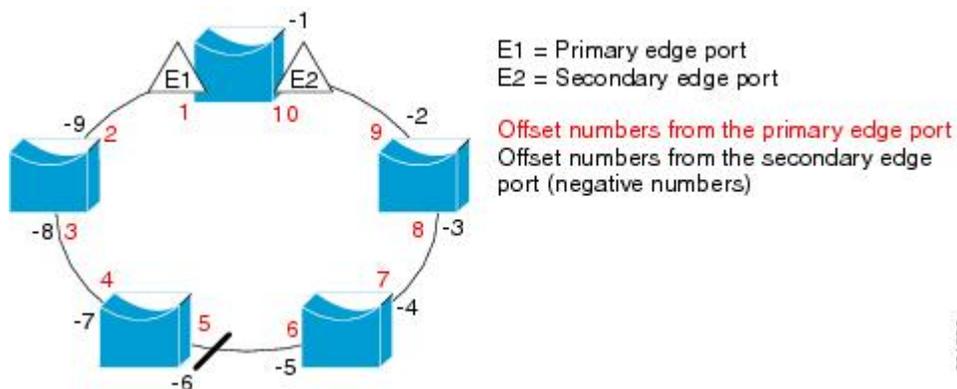
- インターフェイスにポート ID を入力します。セグメント内のポート ID を識別するには、ポートの **show interface rep detail** インターフェイス コンフィギュレーション コマンドを入力します。
- **preferred** キーワードを入力します。これにより、**rep segment segment-id preferred** インターフェイス コンフィギュレーション コマンドで優先代替ポートとしてすでに設定されているポートを選択します。
- セグメント内のポートのネイバー オフセット番号を入力します。これは、エッジポートの下流ネイバー ポートを識別するものです。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 エッジポートの下流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) とその下流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下流の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下流の位置）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下流の位置）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 負荷分散を設定する際には、次の 2 種類の方法のいずれかを使用して発動条件を設定する必要があります。

- 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 負荷分散を発動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、プリエンブ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ブション期間の経過後に VLAN 負荷分散が開始されます。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 負荷分散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発動されるまで、動作が開始されません。

VLAN 負荷分散が発動されると、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 負荷分散が開始され、セグメントが両端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 負荷分散設定を決定します。

負荷分散を再設定するには、プライマリ エッジ ポートを再設定します。負荷分散設定を変更すると、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 負荷分散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。

スパンニングツリーとの相互作用

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ン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 (廃止)



(注) IOS-XE リリース 17.17.1、17.15.3、17.12.5、17.9.7 以降、REP ネゴシエート機能は廃止されました。代わりに REP-ZTP を使用できます。

REP とスパン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経路を提供できるように、リングトポロジで動作するように設定できます。

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ています。次の表に、REP ネゴシエーションイベントが発動す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。



(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。

SELFREP をネゴシエート	PEERS REP をネゴシエート	発動されるイベント	動作
True	True	REPNN	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状態に移行して、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役に留まり、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状態に遷移します。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状態に遷移します。

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 負荷分散は実装されません。VLAN 負荷分散の場合、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、ポートは転送状態になります。

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。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、リンク喪失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高速 REP 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) を発動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 ごとに開始され、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番目のタイマーが開始され、10ms 以内の受信を確認します。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。

高速 REP 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。高速 REP 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。高速 REP 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。高速 REP 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、高速 REP 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。

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

高速 REP 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。

手順

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

```

REP ゼロタッチプロビジョニング

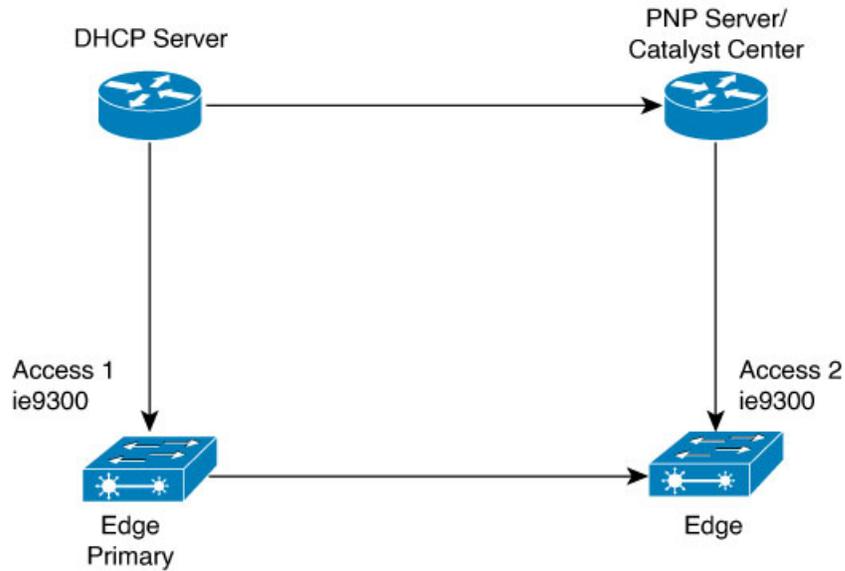
ルータやスイッチなどのネットワークデバイスをオンラインで展開して完全に機能させるには、事前にかかなりの量の手動による設定が必要です。ゼロタッチプロビジョニング (ZTP) テクノロジーによってこれらのプロセスが自動化され、手動による設定を最小限に抑えるか、まったく行うことなくネットワークデバイスを機能する状態へと立ち上げます。Cisco ネットワーク プラグアンドプレイ (PnP) および自動インストール デイゼロ ソリューションは、エンタープライズ ネットワークおよび産業用ネットワークを利用するお客様にシンプルかつセキュアなユニファイド/統合オフリングを提供することで、既存ネットワーク向けの更新のプロビジョニングにおけるデバイスのロールアウトを簡易化します。ただし、Resilient Ethernet Protocol (REP) の設計方法により、PnP は REP をサポートしません。REP ZTP 機能が導入される前は、デイゼロの REP リングプロビジョニングには手動による介入が必要でした。REP ZTP 機能によって REP LSL パケットに新しい Type-Length-Value (TLV) 拡張が導入され、ゼロタッチテクノロジーを使用した REP リングの設定をサポートします。

REP およびデイゼロ

ZTP を使用した一般的なスイッチの展開では、NVRAM にスタートアップ コンフィギュレーションがないスイッチで Cisco Open Plug-n-Play (PnP) エージェントが起動し、DHCP 検出プロセスが開始されます。このプロセスでは、スイッチに必要な IP 設定を DHCP サーバーから取得します。DHCP サーバーは、DHCP メッセージでベンダー固有のオプション 43 を使用して追加情報を挿入するように設定できます。DHCP サーバーは、オプション 60 と文字列「cisco pnp」を含む DHCP DISCOVER メッセージをスイッチから受信すると、要求元のスイッチに PnP サーバーの IP アドレスまたはホスト名を送信します。スイッチが DHCP 応答を受信すると、PnP エージェントは応答からオプション 43 を抽出して、PnP サーバーの IP アドレスまたはホスト名を取得します。次に、スイッチ上の PnP エージェントは、PnP サーバーと通信するためにこの IP アドレスまたはホスト名を使用します。最後に、PnP サーバーは、プロビジョニングを完了するために必要なデイゼロ設定をスイッチにダウンロードします。

次の図は、REP ZTP を導入する前のデイゼロでの REP リングのプロビジョニング例を示しています。

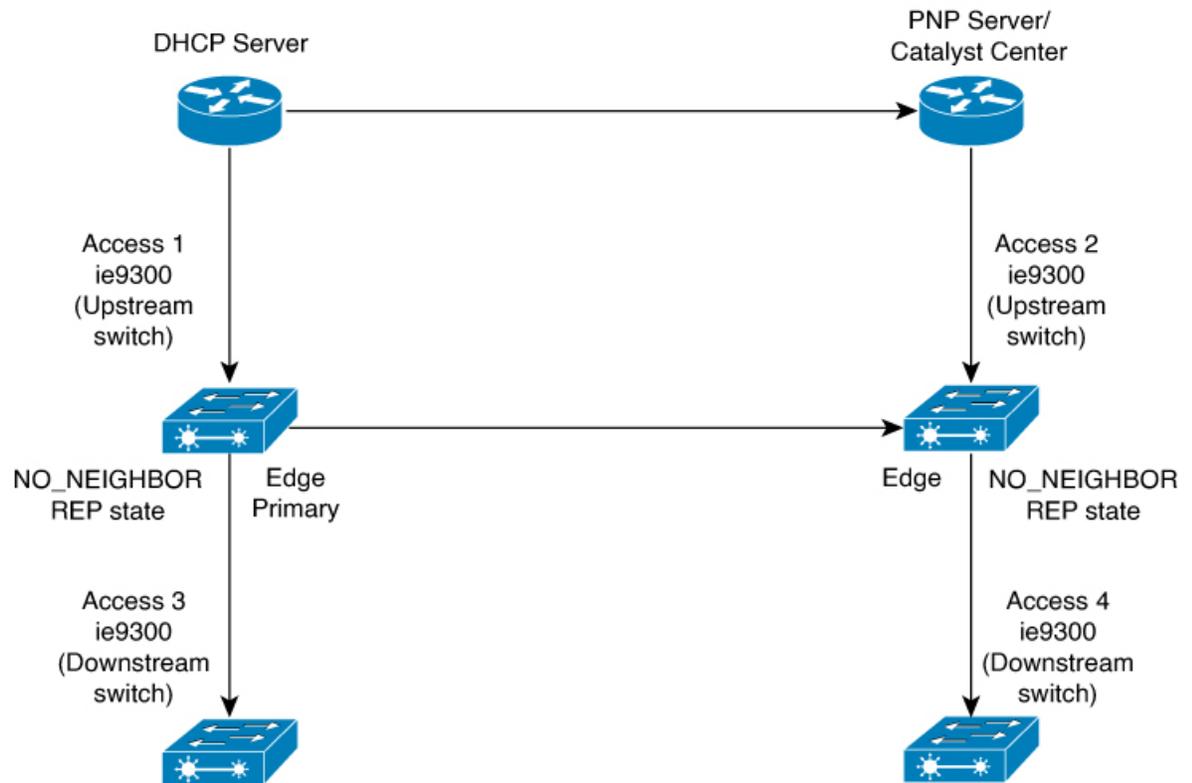
図 10: REP リングへのエッジノードの追加



(注) DHCP サーバーと PnP サーバー/Cisco DNA センターは、REP リングには含まれていません。

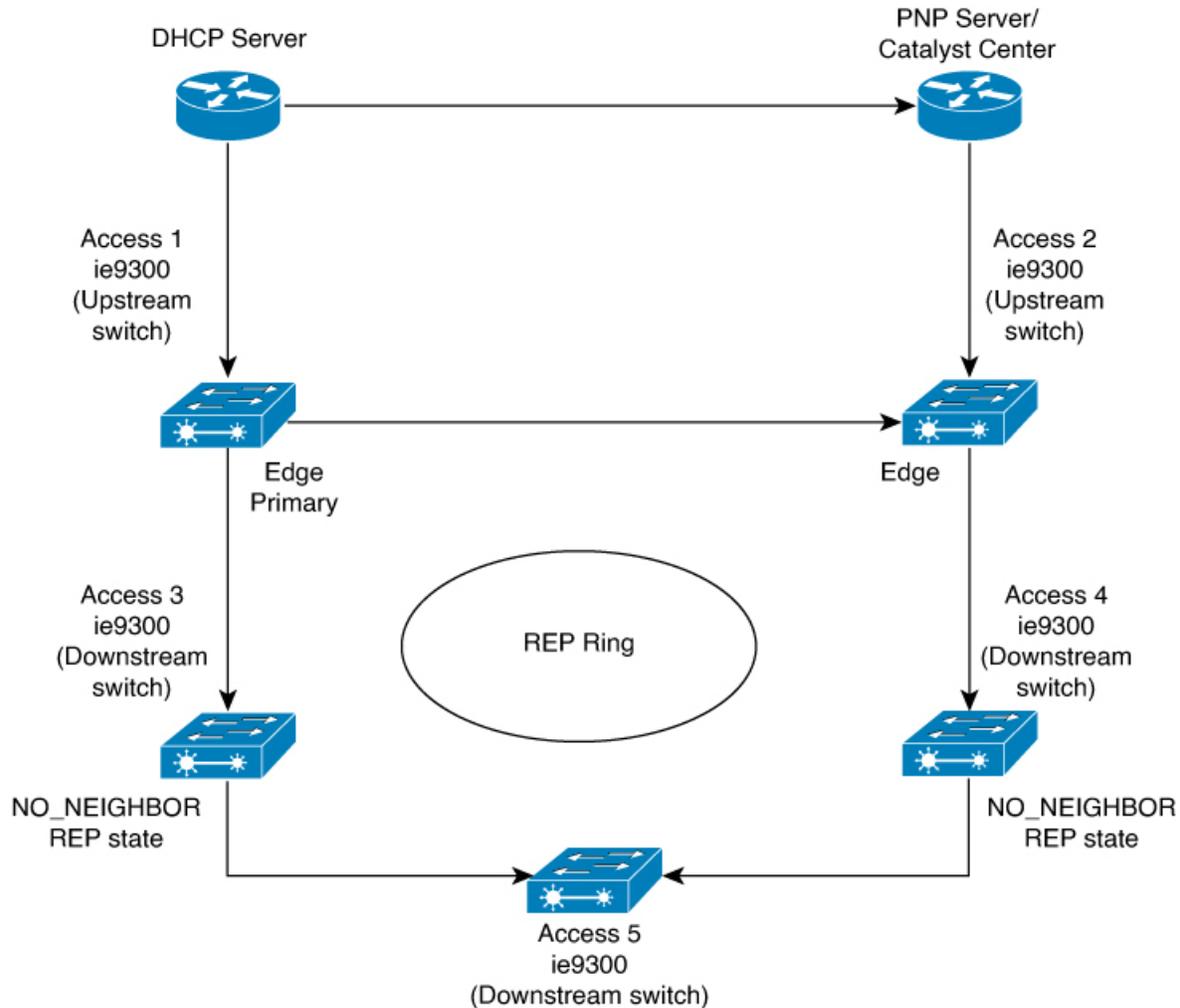
プロビジョニングされるノードの最初のセットは、図内の Access 1 と Access 2 です。これらが REP リングの 2 つのエッジノードとなります。PnP では Access 1 のプライマリエッジおよび Access 2 のセカンダリエッジとしてダウンリンクポートが設定されていることに注意してください。

図 11: 下流ノードの追加



Access 3 または Access 4 のいずれかの電源がオンになると、REP エッジプライマリポートは REP プロトコルのネゴシエーションを開始し、ネイバーポートが REP 対応ポートではないことを検出します（スイッチは PnP のプロビジョニング後にのみ REP リングに追加されます。前述のように、最初に DHCP サーバーに接続する必要があります）。上流スイッチポートに REP が設定され、下流スイッチが PnP でオンボードされると、REP ポートは REP ピアを検出できないため、NO_NEIGHBOR 状態になります。NO_NEIGHBOR 状態では、REP でそのポート上のすべての VLAN がブロックされます。これは、REP 状態が NO_NEIGHBOR であるため、PnP スタートアップ VLAN 上の新しいスイッチから受信した DHCP ディスカバリメッセージが上流スイッチによって破棄されることを意味します。REP リングに追加されたすべての新しいスイッチに対して、ブロックされたポートの同じシーケンスが継続します（次の図の Access 5 を参照）。

図 12: NO_NEIGHBOR の REP 状態



REP ZTP の概要

REP ZTP 拡張機能では、上流スイッチと下流スイッチの両方がこの機能に対応している必要があります。新しい下流スイッチの電源がオンになると、PNP/自動インストールが開始されます。上流スイッチのインターフェイスが REP 用に設定されており、下流スイッチはデフォルトでは REP ではないため、下流スイッチへのインターフェイスはブロックされます（上流スイッチは REP_NO_NEIGHBOR 状態です）。

上流スイッチのインターフェイスがブロックされていても、REPLSL パケットは下流スイッチに送信されます。これは正常です。REP ZTP 機能の拡張により、下流スイッチは新しい TLV を使用して REP LSL パケットの送信を開始し、ネイバーが PNP プロビジョニングを試行していることを上流スイッチに通知します。

上流スイッチが新しい TLV でこの REP LSL を読み取ると、PNP スタートアップ VLAN のインターフェイスのみがブロック解除されます。上流インターフェイスがメンバーになっている他のすべての VLAN は、引き続きブロックされます。上流スイッチはこのインターフェイスの PNP スタートアップ VLAN 上でパケットを転送しているため、下流スイッチは PNP プロセスを完了できます。

この機能の目的は、新しいスイッチが手動による介入なしに REP リングに参加できるようにすることです。上流スイッチのインターフェイスは、下流スイッチが自身の設定を受信し、自身のインターフェイスを REP 用に設定するまで、スタートアップ VLAN のブロックを解除したままにします。PNP プロセスに障害が発生した場合、上流スイッチのインターフェイスは PNP スタートアップ VLAN をブロッキング状態に戻します。下流スイッチが受信した設定でインターフェイスが REP 用に設定されると、上流スイッチは PNP スタートアップ VLAN をブロッキング状態に戻します。

PnP スタートアップ VLAN のブロック解除を要求するために、新しい TLV を使用して REP LSL を送信する下流の動作は、スタートアップ コンフィギュレーションのないスイッチのデフォルト動作です。PnP スタートアップ VLAN をブロック解除状態にするうえで、セキュリティ上の理由から、上流スイッチでは下流スイッチへのインターフェイスを明示的に有効にする必要があります。インターフェイスレベルのコマンドは `rep ztp-enable` です。[REP ZTP の設定 \(79 ページ\)](#) を参照してください。



(注) 上流スイッチは、複数の REP リングの一部として、複数の下流ネイバーに接続できます。PnP スタートアップ VLAN は、下流スイッチが接続されているインターフェイスでのみブロック解除されます。

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 負荷分散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い場合は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 負荷分散が有効の場合、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 負荷分散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。
- 高速 REP 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。

- IOS-XE リリース 17.15.2 以降、IE9300 スイッチは最大 8 つの REP セグメントまたは 3 つの高速 REP セグメントをサポートしています。以前のリリースでは、スイッチは最大 4 つの REP セグメントまたは 3 つの高速 REP セグメントをサポートしていました。
- まず 1 つのポートから始めて、セグメント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。
- セグメント内の 3 つ以上のポートに障害が発生し、外部ネイバーが設定されていない場合、設定中にデータ経路の接続性を維持するために 1 つのポートが転送状態に移行します。
show interfaces rep コマンド出力では、このポートのポート役割は「Fail Logical Open」と表示され、他の障害ポートのポート役割は「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。
- SSH または Telnet 接続を介して REP を設定する場合は注意が必要です。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 をブロックします。SSH または Telnet セッションに使用されるものと同じインターフェイスで 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。STP を非エッジロケーションに接続すると、STP が REP セグメ

ントで動作せず、すべての STP BPDUs が REP インターフェイスで破棄されるため、ブリッジンググループが発生する可能性があります。

- 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として設定されている必要があります。REP ポートは次のルールに従います。
 - 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。
 - スイッチ上の 2 ポートが同じセグメントに属している場合、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。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最初はブロック状態で起動し、安全にブロック解除可能になるまでブロックされたままになります。予期しない接続の損失を防ぐために、このステータスに注意してください。
- 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 ~ 10,000 ミリ秒の範囲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、非高速 REP 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 ポートチャン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。ポートチャンネルで 1000 ミリ秒未満の値を設定しようとする、エラーメッセージが表示され、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 ではサポートされますが、EtherChannel 内の個々のポートではサポートされません。
 - REP リングのサイズに制限はありませんが、ノード数が 20 を超えるリングでは、目的のコンバージェンスが達成されない場合があります。

高速 REP 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、リンクの両端で高速 REP を設定しなければなりません。
- REP セグメントには、ギガビット光ファイバとギガビット銅線を混在させることができます。ギガビット銅線インターフェイスに高速 REP がある場合、単一障害からのコンバージェンスに必要な 50 ミリ秒の要件を達成できます。
- 高速 REP は、すべてのインターフェイスが高速 REP をサポートしているわけではない REP セグメント内に展開できます。ただし、このような場合は 50 ミリ秒のコンバージェンスが確保されない場合があります。
- 次の制限事項に注意してください。
 - 同時に最大 3 つの REP セグメントで高速 REP を有効にできます。
 - MACsec は高速 REP とのみ相互運用できます。
 - 高速 REP はスタック環境ではサポートされていません。
 - EtherChannel を介した高速 REP はサポートされていません。

REP ZTP 設定時の注意事項

- REP ZTP では、Cisco Catalyst IE9300 高耐久性シリーズスイッチに PnP 機能が存在する必要があります。
- NO_NEIGHBOR 状態での REP の動作は、Cisco IOS XE 17.14.1 以降で変更されています。NO_NEIGHBOR 状態でのポート転送動作のこの一時的な状態変化により、DHCP 要求メッセージが DHCP サーバーに到達し、新しいスイッチの PnP プロビジョニングがブロック解除されます。PnP の完了後に REP 状態機械に影響が出ることはありません。
- NO_NEIGHBOR 状態での REP の動作の変更は、Cisco IOS XE 17.14.1 以降の REP ゼロタッチプロビジョニング (ZTP) にのみ適用されます。PnP 機能が存在しない場合、通常の REP 機能は期待どおりに動作します。
- REP ZTP 機能は、ファイバアップリンクポートで REP bpduleak/ネゴシエートされた機能と共存します。

- REP ZTP 機能は、EtherChannel が下流のインターフェイスにデフォルトで存在しないため、上流スイッチの EtherChannel インターフェイスではダイゼロ向けに使用できません。REP ZTP は、物理インターフェイスでのみ機能します。
- REP ZTP は、銅線（ダウンリンク）インターフェイスと光ファイバ（アップリンク）インターフェイスの両方でサポートされます。
- REP ZTP は、REP ZTP によるサポートを要求する Cisco IOS XE を実行している他の IE スイッチング製品とのみ相互運用できます。

REP 管理 VLAN の設定

リンク障害メッセージ、および負荷分散時の 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

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	rep admin vlan <i>vlan-id</i> 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。
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 [<i>interface-id</i>] 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

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	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。 <ul style="list-style-type: none"> • （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 負荷分散を設定できるポート）としてポートを設定します。

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> • (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。 <p>(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。</p> <ul style="list-style-type: none"> • (任意) preferred : ポートが優先代替ポートであるか、VLAN 負荷分散の優先ポートであるかを示します。 <p>(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。</p>
ステップ 6	rep stcn { <i>interface interface id</i> <i>segment id-list</i> <i>stp</i> } 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。 <ul style="list-style-type: none"> • interface interface-id : 物理インターフェイスまたはポートチャンネルを指定して、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。 <p>(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。</p>

	コマンドまたはアクション	目的
ステップ 7	<p>rep block port {<i>id port-id</i> <i>neighbor-offset</i> preferred} vlan {<i>vlan-list</i> all}</p> <p>例 :</p> <pre>Device(config-if)# rep block port id 0009001818D68700 vlan 1-100</pre>	<p>(任意) プライマリエッジポートに VLAN 負荷分散を設定して、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、<i>neighbor_offset</i>、preferred)、代替ポートでブロックされるように VLAN を設定します。</p> <ul style="list-style-type: none"> • 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。 • <i>neighbor_offset</i> : エッジポートからの下流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下流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。 <p>(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。</p> <ul style="list-style-type: none"> • preferred : すでに VLAN 負荷分散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。 <p>(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。</p>
ステップ 8	<p>rep preempt delay <i>seconds</i></p> <p>例 :</p> <pre>Device(config-if)# rep preempt delay 100</pre>	<p>(任意) プリエンプション遅延時間を設定します。</p> <ul style="list-style-type: none"> • リンク障害が発生して復旧した後に、VLAN 負荷分散を自動的に発動するには、このコマンドを使用します。

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> 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。 <p>(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。</p>
ステップ 9	rep lsl-age-timer <i>value</i> 例： Device(config-if)# rep lsl-age-timer 2000	<p>(任意) ネイバーからの hello が受信されないままのくらいの時間 (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。</p> <p>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。</p> <p>(注)</p> <ul style="list-style-type: none"> 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 [<i>interface-id</i>] rep [<i>detail</i>] 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 負荷分散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 コマンドを入力してプリエンプション遅延時間を設定しない場合、デフォルトでは手動により当該セグメントの VLAN 負荷分散を発動します。手動で VLAN 負荷分散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	rep preempt segment <i>segment-id</i> 例： Device# 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 負荷分散を発動します。 実行前にコマンドを確認する必要があります。
ステップ 3	show rep topology segment <i>segment-id</i> 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 4	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、Simple Network Management Protocol (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の役割変更を通知するようにスイッチを設定できます。

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）。
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。

	コマンドまたはアクション	目的
ステップ 3	snmp mib rep trap-rate <i>value</i> 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。 <ul style="list-style-type: none"> 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。

REP ZTP の設定

REP ZTP を設定するには、グローバルレベルおよびインターフェイスレベルで有効または無効にします。デフォルトの状態は、次のとおりです。

- グローバルレベル：有効
- インターフェイスレベル：無効

下流デバイスに接続されている上流デバイスインターフェイスのインターフェイスレベルで、この機能を明示的に有効にする必要があります。有効にすると、そのインターフェイスだけが下流スイッチから通知を受信し、PnP スタートアップ VLAN をブロックまたはブロック解除します。



(注) DNAC または PNP サーバーの設定を適用する場合、ユーザーはこの CLI 設定を設定テンプレートに明示的に追加して、機能を有効にする必要があります。

手順

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。

```
Switch# configure terminal
```

ステップ 2 REP ZTP をグローバルに有効にします。

```
Switch(config)# rep ztp
```

REP ZTP を無効にするには、Switch(config)# **no rep ztp** コマンドの **no** 形式を使用します。

ステップ 3 下流デバイスに接続されている上流デバイスインターフェイスで、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。

```
Switch(config)# interface <interface-name>
```

ステップ 4 インターフェイスで REP ZTP を有効にします。

```
Switch(config-if)# rep ztp-enable
```

インターフェイスで REP ZTP を無効にするには、Switch(config-if)#**no rep ztp-enable** コマンドの **no** 形式を使用します。

例

次に、下流デバイスに接続されている上流デバイスインターフェイスで REP ZTP 機能を有効にするために必要な最小設定の例を示します。

```
Switch#show running-config interface gigabitEthernet 1/0/1
Building configuration...
```

```
Current configuration : 93 bytes
!
interface GigabitEthernet1/0/1
  switchport mode trunk
  rep segment 100
  rep ztp-enable
end
```

Resilient Ethernet Protocol 設定の監視

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      Gi1/0/11      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

```

REP ZTP ステータスの表示

インターフェイスで REP ZTP の状態を確認するには、**show** コマンドを使用します。次の例では、インターフェイス GigabitEthernet 1/0/1 でこの機能を無効にし、インターフェイス GigabitEthernet 1/0/2 で有効にしています。**pnnp_startup_vlan** のステータスは「Blocked」です。

手順

ステップ 1 特権 EXEC モードで、次のように入力します。

show interfaces rep detail

例：

```

GigabitEthernet1/0/1  REP enabled
Segment-id: 100 (Segment)
PortID: 00016C13D5AC4320
Preferred flag: No
Operational Link Status: TWO_WAY
Current Key: 00026C13D5AC43209DAB
Port Role: Open
Blocked VLAN: <empty>
Admin-vlan: 1
REP-ZTP Status: Disabled
REP Segment Id Auto Discovery Status: Enabled
REP Segment Id Type: Manual
Preempt Delay Timer: disabled
LSL Ageout Timer: 5000 ms
LSL Ageout Retries: 5
Configured Load-balancing Block Port: none
Configured Load-balancing Block VLAN: none
STCN Propagate to: none
LSL PDU rx: 382, tx: 297
HFL PDU rx: 0, tx: 0
BPA TLV rx: 1, tx: 19
BPA (STCN, LSL) TLV rx: 0, tx: 0
BPA (STCN, HFL) TLV rx: 0, tx: 0
EPA-ELECTION TLV rx: 95, tx: 0
EPA-COMMAND TLV rx: 0, tx: 0
EPA-INFO TLV rx: 95, tx: 95

GigabitEthernet1/0/2  REP enabled
Segment-id: 100 (Segment)
PortID: 00026C13D5AC4320
Preferred flag: No
Operational Link Status: NO_NEIGHBOR
Current Key: 00026C13D5AC43209DAB
Port Role: Fail No Ext Neighbor
Blocked VLAN: 1-4094

```

```

Admin-vlan: 1
REP-ZTP Status: Enabled
REP-ZTP PnP Status: Unknown
REP-ZTP PnP Vlan: 1
REP-ZTP Port Status: Blocked
REP Segment Id Auto Discovery Status: Enabled
REP Segment Id Type: Manual
Preempt Delay Timer: disabled
LSL Ageout Timer: 5000 ms
LSL Ageout Retries: 5
Configured Load-balancing Block Port: none
Configured Load-balancing Block VLAN: none
STCN Propagate to: none
LSL PDU rx: 11, tx: 11
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

```

ステップ 2 show コマンドを再度使用して、**pnp_startup_vlan** のステータスを表示します。

下流デバイスが起動すると、接続された上流スイッチインターフェイスに通知を送信し、**pnp_startup_vlan** のブロックを解除して DHCP IP アドレスを取得します。さらに、PNP サーバーまたは DNAC との通信も確立します。show コマンドを実行すると、ステータスが「Unblocked」と表示されます。

次に示す上流スイッチの syslog では、ポートの FWD および BLK について通知しています。PnP によってコンソールが制御され、コンソールで syslog を出力できないため、下流スイッチに syslog はありません。

```
REP-6-ZTPPORTFWD: Interface GigabitEthernet1/0/2 moved to forwarding on ZTP notification
```

```
REP-6-ZTPPORTBLK: Interface GigabitEthernet1/0/2 moved to blocking on ZTP notification
```

例 :

```

Switch#show interfaces rep detail
GigabitEthernet1/0/1  REP enabled
Segment-id: 100 (Segment)
PortID: 00016C13D5AC4320
Preferred flag: No
Operational Link Status: TWO_WAY
Current Key: 00026C13D5AC43209DAB
Port Role: Open
Blocked VLAN: <empty>
Admin-vlan: 1
REP-ZTP Status: Disabled
REP Segment Id Auto Discovery Status: Enabled
REP Segment Id Type: Manual
Preempt Delay Timer: disabled
LSL Ageout Timer: 5000 ms
LSL Ageout Retries: 5
Configured Load-balancing Block Port: none
Configured Load-balancing Block VLAN: none
STCN Propagate to: none
LSL PDU rx: 430, tx: 358
HFL PDU rx: 0, tx: 0
BPA TLV rx: 1, tx: 67
BPA (STCN, LSL) TLV rx: 0, tx: 0

```

```

BPA (STCN, HFL) TLV rx: 0, tx: 0
EPA-ELECTION TLV rx: 107, tx: 0
EPA-COMMAND TLV rx: 0, tx: 0
EPA-INFO TLV rx: 107, tx: 108

GigabitEthernet1/0/2   REP enabled
Segment-id: 100 (Segment)
PortID: 00026C13D5AC4320
Preferred flag: No
Operational Link Status: NO_NEIGHBOR
Current Key: 00026C13D5AC43209DAB
Port Role: Fail No Ext Neighbor
Blocked VLAN: 1-4094
Admin-vlan: 1
REP-ZTP Status: Enabled
REP-ZTP PnP Status: In-Progress
REP-ZTP PnP Vlan: 69
REP-ZTP Port Status: Unblocked
REP Segment Id Auto Discovery Status: Enabled
REP Segment Id Type: Manual
Preempt Delay Timer: disabled
LSL Ageout Timer: 5000 ms
LSL Ageout Retries: 5
Configured Load-balancing Block Port: none
Configured Load-balancing Block VLAN: none
STCN Propagate to: none
LSL PDU rx: 32, tx: 40
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

```

ステップ 3 PnP スタートアップ VLAN のインターフェイス状態を確認するには、**show platform hardware l2 stp** コマンドを使用します。

例：

```

Switch#show platform hardware l2 stp ASIC-num 0 vlan-id 69 □[PnP Vlan]
-----STP TABLE START-----
-----
VlanId:1 StpId:0 MemberPort:3 StpState:FORWARDING
VlanId:1 StpId:0 MemberPort:7 StpState:FORWARDING
VlanId:1 StpId:0 MemberPort:25 StpState:FORWARDING
-----
-----STP TABLE END-----

```

ステップ 4 (任意) REP ZTP のトラブルシューティングには、次のデバッグコマンドを使用できます。

- **debug rep lsism** : このコマンドは、NO_NEIGHBOR 状態の LSL 状態機械イベントについて理解するのに役立ちます。
- **debug rep packet** : REP ZTP LSL TLV で LSL パケットをダンプし、ピアクライアントノードの PnP ステータスを確認するには、このコマンドを使用します。

次のタスク

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 17.15.2	Resilient Ethernet Protocol	このリリースから、IE9300 スイッチは最大 8 つの REP セグメントまたは 3 つの高速 REP セグメントをサポートするようになり、以前の 4 つの REP セグメントまたは 3 つの高速 REP セグメントの制限から増加しています。
Cisco IOS XE 17.14.x	Resilient Ethernet Protocol のゼロタッチプロビジョニング	この機能は Cisco Catalyst IE9300 高耐久性シリーズスイッチのこのリリースで導入されました。
Cisco IOS XE Cupertino 17.9.x	Resilient Ethernet Protocol Fast	この機能は Cisco Catalyst IE9300 高耐久性シリーズスイッチのこのリリースで導入されました。



第 4 章

Media Redundancy Protocol

- [Media Redundancy Protocol \(87 ページ\)](#)
- [MRP モード \(88 ページ\)](#)
- [プロトコルの動作 \(88 ページ\)](#)
- [Media Redundancy Automanager \(90 ページ\)](#)
- [ライセンス \(91 ページ\)](#)
- [IE9300 スタック上の MRP \(91 ページ\)](#)
- [MRP-STP の相互運用性 \(92 ページ\)](#)
- [前提条件 \(92 ページ\)](#)
- [注意事項と制約事項 \(92 ページ\)](#)
- [デフォルト設定 \(94 ページ\)](#)
- [TIA 15 または STEP7 を使用した Profinet MRP モードの設定 \(94 ページ\)](#)
- [MRP CLI モードの設定 \(100 ページ\)](#)
- [設定例 \(105 ページ\)](#)
- [設定の確認 \(107 ページ\)](#)
- [機能の履歴 \(107 ページ\)](#)

Media Redundancy Protocol

国際電気標準会議 (IEC) 規格 62439-2 で定義されている Media Redundancy Protocol (MRP) は、産業オートメーションネットワーク向けのリングネットワークトポロジで高速コンバージェンスを実現します。MRP Media Redundancy Manager (MRM) は、リングの最大リカバリ時間を 200 ミリ秒と 500 ミリ秒の範囲で定義します。



- (注) 最大 50 ノードで構成されるリングの場合、Cisco IE スイッチのデフォルトの最大リカバリ時間は 200 ミリ秒です。[MRP マネージャの設定 \(101 ページ\)](#) に説明されているように、500 ミリ秒のリカバリ時間プロファイルを使用するよう、スイッチを設定できます。10 ミリ秒と 30 ミリ秒のリカバリ時間プロファイルはサポートされていません。

MRP はすべての 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。

- IE-9310-26S2C-EおよびIE-9310-26S2C-A
- IE-9320-26S2C-EおよびIE-9320-26S2C-A
- IE-9320-22S2C4X-EおよびIE-9320-22S2C4X-A
- IE-9320-24T4X-EおよびIE-9320-24T4X-A
- IE-9320-24P4X-EおよびIE-9320-24P4X-A
- IE-9320-16P8U4X-EおよびIE-9320-16P8U4X-A
- IE-9320-24P4S-EおよびIE-9320-24P4S-A

MRP モード

MRP は Cisco Catalyst IE9300 高耐久性シリーズ スイッチの MRP コマンドライン インターフェイス (CLI) モードでサポートされています。

MRP CLI モードは、Cisco IOS XE CLI および WebUI (Web ベースのユーザーインターフェイス (UI)) によって管理されます。



(注) MRP CLI モードでスイッチを管理する場合、Siemens STEP7/TIA から MRP 設定をダウンロードすることはできません。

プロトコルの動作

MRP リングでは、MRM はリング マネージャとして機能し、一方 Media Redundancy Clients (MRC) はリングのメンバーノードとして機能します。各ノード (MRM または MRC) には、リングに参加するための 1 対のポートがあります。MRM は、1 つのリングポートの制御フレームをリングを介して送信し、リングからの制御フレームを他のリングポートを介して受信し、反対方向のものも受信することによって、ネットワーク障害に対応するリング トポロジを開始、制御します。MRC は MRM から受信した再構成フレームに応答し、そのリングポート上のリンクの変化を検出して通知することができます。

Cisco Catalyst IE9300 高耐久性シリーズ スイッチのデフォルトでは、リング内のすべてのノードが MRA として起動するように設定されますが、特定のノードを個別に設定して MRA として動作させることもできます。MRA では、投票プロトコルと設定された優先順位値を使用して、MRM が互いに 1 つ選択されます。残りの MRA は MRC 役に遷移します。

すべての MRM および MRC リングポートは、次の状態をサポートします。

- 無効：リングポートで受信したすべてのフレームが破棄されます。
- ブロック：リングポートで MRP 制御フレームと一部の標準フレーム (LLDP など) を除くすべての受信フレームが破棄されます。

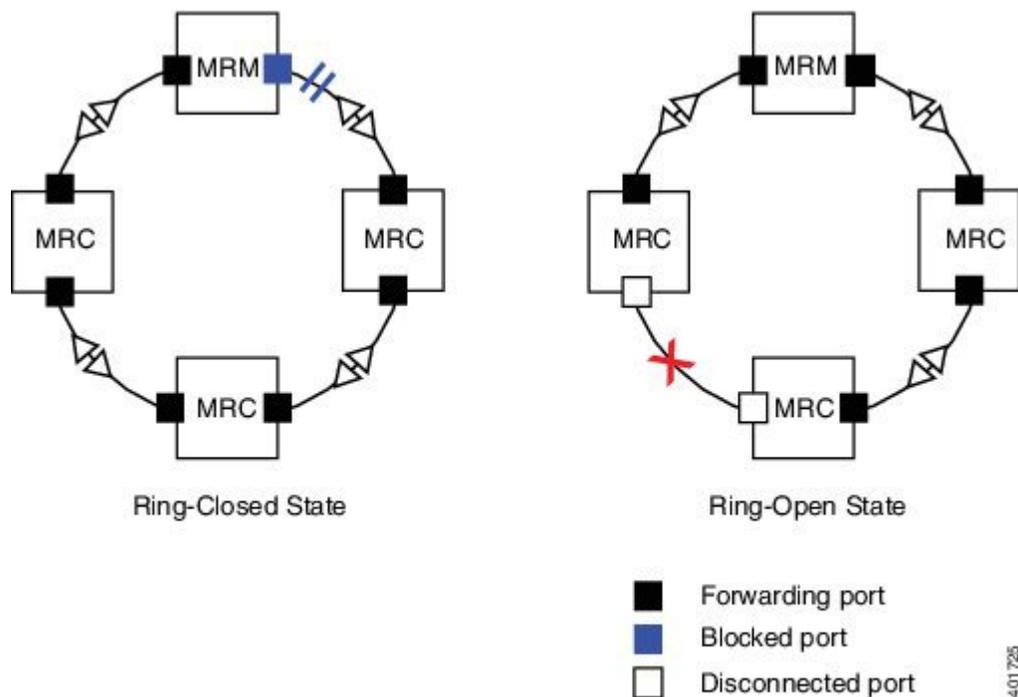
- 転送：リングポートですべての受信フレームが転送されます。
- 未接続：リンクが物理的にダウンしているか切断されています。（この状態は、MRPポートがソフトウェアによって手動で無効にされている「無効効態」とは異なります）。

通常動作中、ネットワークは Ring-Closed 状態で動作します（以下の図を参照）。ループを防止するため、一方のMRMリングポートはブロックで、もう一方のポートは転送になります。ほとんどの場合、すべてのMRCの両方のリングポートは転送状態になります。このループ回避により、物理リングトポロジは論理スタブトポロジになります。

図では、左と右の2つのリングについて、次の点に注意してください。

- 左側のリング：どのポートも切断されていないため、MRMの接続（上部の小さな青い四角）はブロック状態（2本の平行線で示す）です。
- 右側のリング：2つのMRCの接続（左と中央の小さな白い四角）は、赤い「x」で示すように、それらの間のリンクが壊れているため、無効状態です。

図 13: MRP リングの状態



401725

ネットワーク障害が発生した場合：

- ネットワークは Ring-Open 状態に移行します。
- 2つのMRCを接続するリンクに障害が発生した場合、MRMの両方のリングポートは転送状態に変わり、障害に隣接するMRCは無効リングポートと転送リングポートになり、他のMRCは両方のリングポートが転送になります。

Ring-Open 状態では、ネットワーク論理トポロジはスタブになります。

レイヤ2イーサネットフレームは、これら2つのリング状態間の移行に必要な時間中に失われます。MRPプロトコルでは、スイッチオーバー時間を最小限に抑えるためにスイッチオーバーを自動的に管理する手順を定義します。さまざまなパラメータで構成されるリカバリ時間プロファイルは、MRP トポロジ コンバージェンス性能を促進します。200 ミリ秒のプロファイルは、200 ミリ秒の最大リカバリ時間をサポートします。

MRP は 3 種類の制御フレームを使用します。

- リングステータスを監視するため、MRMは定期的に両方のリングポートでテストフレームを送信します。
- MRM が障害またはリカバリを検出すると、両方のリングポートで TopoChange フレームを送信します。
- MRC がローカルポート上で障害またはリカバリを検出すると、LinkChange サブタイプフレーム、Linkdown および Linkup を MRM に送信します。

Media Redundancy Automanager

Media Redundancy Automanager (MRA) として開始するように設定されている場合、ノードでは投票プロトコルと設定された優先順位値を使用して MRM が選択されます。残りの MRA は MRC 役に遷移します。すべての IE9300 ノードを MRA として設定する必要があります。同じリング内に手動で MRM および MRA を設定することはサポートされていません。



- (注)
- CLIを使用してMRAをアクティブ化できます。このガイドの[MRP CLIモードの設定 \(100 ページ\)](#) セクションを参照してください。
 - MRM が選択されると MRA は MRC 役に移行しますが、MRC を明示的に設定することはできません。

MRA 役は、MRM や MRC のような実稼働可能な MRP 役ではありません。MRA 役は、デバイス起動時の一時的な管理上の役割に過ぎません。起動後はノードを MRM 役または MRC 役に遷移する必要があり、マネージャ投票プロセスを通じて MRM が選択されます。

MRA は、次のように機能します。

1. 電源投入時に、すべての MRA がマネージャ投票プロセスを開始します。各 MRA では、両方のリングポートで MRP_Test フレームの送信が開始します。MRP_Test フレームには MRA の優先順位値が含まれています。受信した MRP_Test フレームに含まれるリモートマネージャの優先順位値は、MRA 自身の優先度と比較されます。MRA は自身の優先順位が受信した優先順位よりも高い場合、リモートマネージャの MAC アドレスとともに、テストマネージャの否定応答 (MRP_TestMgrNAck) フレームを送信します。

2. 受信側 MRA が、自身の MAC アドレスを含む MRP_TestMgrNAck を受信すると、受信側 MRA はクライアント（MRC）役への遷移を開始します。
3. MRP_TestPropagate フレームは、クライアント役の他の MRA デバイスに、役割の変更と、より優先順位が高い新規のマネージャについて通知します。このフレームを受信するクライアントは、その情報に応じて、より優先順位が高いマネージャの情報を更新します。これにより、監視しているより優先順位の高いマネージャ役が変更された場合でも、クライアントがクライアント役にとどまることになります。

ライセンス

Cisco Catalyst IE9300 高耐久性シリーズスイッチで MRP を使用するために機能ライセンスは必要ありません。MRP では、Network Essentials または Network Advantage のいずれかの基本ライセンスを使用します。

プラットフォームサポートに関する情報を検出し、機能を使用できるライセンスレベルを確認するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、<https://www.cisco.com/go/cfn> からアクセスします。cisco.com のアカウントは必要ありません。

IE9300 スタック上の MRP

Cisco IOS-XE 17.17.1a 以降では、スタック構成のスイッチ間でのシステムの安定性とシームレスな統合を確保する手段として、Media Redundancy Protocol (MRP) のスタックサポートが導入されています。

MRP の機能と動作は、スタンドアロンとスタックの両方の構成で一貫しています。MRP のスタックセットアップでは、最大 4 メンバーのスタックがサポートされています。

スイッチスタックの詳細については、「[Managing Switch Stacks](#)」を参照してください。

IE9300 スタック上の MRP の利点

スタックセットアップで MRP を展開すると、ネットワーク内にノードレベルの冗長性が導入され、次のような利点が得られます。

- IE9300 スタックセットアップで、200 ミリ秒および 500 ミリ秒のコンバージェンス プロファイルを使用した最大 16 のリングがサポートされます。
- スタックメンバーまたはアクティブスイッチに障害が発生した場合でも、システムの動作が維持されて、シングルポイント障害のリスクが軽減されます。
- ネットワーク全体でのシームレスな統合と信頼性を実現できます。
- ポート密度が向上します。これは、パフォーマンスを犠牲にすることなく、より多くのデバイスに対応するために重要です。

MRP-STP の相互運用性

MRP はスパニングツリープロトコル (STP) と連携して動作し、ユーザが誤って MRP リングに参加していないデバイスを接続した場合に、不要なブロードキャストループを防ぎます。MRP と STP で動作するネットワークでは、スパニングツリーブリッジプロトコルデータユニット (BPDU) は MRP 対応ポートには送信されません。ポートの MRP 設定が解除されリングから離脱すると、そのポートはスパニングツリーに追加されます。MRP 制御フレームは STP ポートを通りません。デフォルトでは、MRP リングのメンバーとして明示的に設定されていないすべてのポートが STP に参加します。

MRP-STP 相互運用性は MRP CLI モードでサポートされ、追加の CLI 設定なしで動作します。

前提条件

MRP は物理リングトポロジに配置されているため、ネットワークストームを回避するためには、MRP 機能を設定または設定解除する前に接続インターフェイスで **shut** コマンドを発行するか、ケーブルを物理的に取り外して、各リングの 2 つのノード間の物理的な接続を 1 つ開けておくことが推奨されます。すべての MRP を正しく設定した後に、ポートで **no shut** コマンドを発行するか、ノード間のケーブルを再接続します。

注意事項と制約事項

一般的なガイドラインと制限事項

- MRP は、IOS XE 17.13.1 リリース以降の 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。
- スタンドアロン IE9300 スイッチで、200 ミリ秒または 500 ミリ秒のコンバージェンスプロファイルを使用した最大 12 のリングがサポートされます。
- 複数の MRP リングのサポートは、CLI または WebUI を介してのみ可能です。
- スイッチは 1 リングあたり最大 50 の MRC をサポートします。
- MRP を Resilient Ethernet Protocol (REP)、スパニングツリープロトコル (STP)、Flex Link、MACsec、または Dot1x と同じインターフェイス (ポート) で実行することはできません。
- アクセスポートでは、MRP インターフェイスで具体的に **switchport mode access** および **switchport access vlan x** コマンドを設定する必要があります。
- MRP インターフェイスは転送状態で起動し、安全にブロック可能と通知されるまで転送状態のままになります。MRP リングの状態は Ring-Closed に変わります。

- MRP ポートは、SPAN 宛先ポート、プライベート VLAN ポート、またはトンネル ポートのいずれのポート タイプとしても設定できません。
- MRP は EtherChannel または EtherChannel に属する個別のポートではサポートされません。
- 各 MRP リングは 1 つの MRP 管理 VLAN のみを持つことができます。トラフィックフラグディングを回避するため、VLAN はデバイスのリングごとに異なる必要があります。VLAN には、単一の MRP リングからのインターフェイスのみをメンバーとして含めることができます。
- 各 IE9300 ノードには、MRP リングのメンバーとして 2 つのインターフェイスを含める必要があります。部分的なリングまたは断片的なリングの使用はサポートされていません。

MRP CLI モードの注意事項と制限事項

- CLI を使用して MRP リングを設定したら、MRP リングを、MRP をサポートするポートペアに接続する必要があります。
- どちらの MRP ポートも同じインターフェイス モード（アクセスまたはトランク）である必要があります。
- 既存の MRP リングの設定（モード）を変更する、またはアクセスとトランク間のリングポートのインターフェイスモードを変更するには、まずリングを削除してから、新しい設定のリングを再作成する必要があります。
- 両方の MRP ポートがアクセスモードの場合、アクセス VLAN はこれに合わせる必要があります。設定済みの MRP VLAN がポートのアクセス VLAN と一致しない場合、MRP VLAN は自動的に MRP ポートのアクセス VLAN に変更されます。
- 2 つのアクセス ポートを持つ MRP リングで、MRP リング作成時にポートが同じアクセス VLAN に属していない場合、または MRP リング作成後にポートの 1 つだけアクセス VLAN を変更した場合、MRP リング動作は中断され、次のようなメッセージが表示されます。

```
ERROR% The ring 1 ports don't belong to the same access VLAN. The MRP ring will not function until the issue has been fixed
```

この問題を解決するには、2 つのリングポートのアクセス VLAN の設定を同じにします。

- 200 ミリ秒の標準プロファイルと 500 ミリ秒のプロファイルがサポートされています。10 ミリ秒と 30 ミリ秒のプロファイルはサポートされていません。
- CLI を使用して MRA をアクティブ化できます。
- MRM が選択されると MRA は MRC 役に移行しますが、MRC を明示的に設定することはできません。

デフォルト設定

- MRP はデフォルトで無効になっています。MRP CLI は、MRP が有効になっている場合のデフォルトモードです。
- デフォルトの VLAN は 1 です。



(注) デフォルト以外の VLAN を、MRP リング 1 に割り当てる前に作成します。

TIA 15 または STEP7 を使用した Profinet MRP モードの設定

ライセンス (Cisco IOS XE 17.6.x 以前) をアクティブ化した後、Siemens TIA または STEP7 を使用して、PROFINET MRP 設定をシスコスイッチにプッシュすることができます。IOS XE バージョン 17.6.x 以前では、PROFINET で MRP を設定する前に、MRP 機能ライセンスをインストールする必要があります。IOS XE 17.7.1 以降では、機能ライセンスなしで PROFINET で MRP を設定できます。



(注) PROFINET および TIA を使用している場合、CLI を使用してスイッチの設定を実行または変更しないでください。これには MRC または MRM 権限を設定することが含まれます。MRP CLI モードと PROFINET MRP モードは相互に排他的です。



(注) シスコスイッチが PROFINET PLC に接続されている場合、**show profinet status | include Connected** の出力は **Yes** になります。**show profinet status | include Connected** の出力が **No** の場合、スイッチは PROFINET PLC に接続されていません。

PROFINET GSD ファイルのインストール

PROFINET MRP GSD ファイルは、Cisco IOS XE ソフトウェアリリースにバンドルされています。スイッチが少なくとも 1 回起動した後、スイッチの GSD ファイルは「ProfinetGSD」というディレクトリに配置されます。このディレクトリには、全スイッチ SKU のすべての GSD を含む zip ファイルがあります。リリースにバンドルされ、ProfinetGSD ディレクトリに含められる GSD ファイルを使用することを推奨します。



注意 Cisco IOS ソフトウェアにバンドルされているバージョンより古い TIA 15 または STEP 7 にインストールされた GSD XML ファイルがある場合、非互換性により起こり得る問題を回避するため、古いファイルを削除することを推奨します。

PROFINET MRP の起動

前提条件

LLDP プロトコルを使用してすべての近接デバイスを検出するため、PROFINET MRP をネットワークにプッシュする前に、MRP イーサネットポートを承認し、リング（オープンリング）から切断することを推奨します。このアプローチにより、何か問題があった場合に、不必要なフラッドングを回避できます。

手順の概要

1. （オプション）**show lldp neighbor** と入力し、LLDP プロトコルがすべてのネイバーを正しく検出することを確認します。
2. （Cisco IOS XE 17.6 以前）すべての MRP ライセンスがスイッチ上でアクティブであることを確認します。
3. PROFINET ステータスに「接続済み」と表示されていることを確認します。
4. **profinet mrp ring 1** の出力を調べることで、MRP ポートが正しく接続されていることを確認でき、次の報告が得られます。

手順の詳細

手順

ステップ 1 （オプション）**show lldp neighbor** と入力し、LLDP プロトコルがすべてのネイバーを正しく検出することを確認します。

ステップ 2 （Cisco IOS XE 17.6 以前）すべての MRP ライセンスがスイッチ上でアクティブであることを確認します。

ステップ 3 PROFINET ステータスに「接続済み」と表示されていることを確認します。

ステップ 4 **profinet mrp ring 1** の出力を調べることで、MRP ポートが正しく接続されていることを確認でき、次の報告が得られます。

- ブロック済みモードの 1 つの MRM ポート
- フォワーディングモードの他のすべての MRM ポート（のバランス）

（注）

MRP デバイスのロールを変更する（MRP クライアントから MRP マネージャ、または MRP マネージャから MRP クライアントなど）前に、MRP リングが開いていることを確認します。

Simatic Step 7 または TIA 15 ポータルを使用した Profinet の管理

このセクションでは、TIA ポータル内の主要画面の概要について説明します。ここでは設定の詳細については説明しません。TIA ポータルの詳細な使用方法については、Siemens Simatic STEP7 のユーザ マニュアルを参照してください。



(注) PROFINET モードの MRP 自動マネージャは、TIA V15 でのみサポートされます。

図 14: MRP を設定する前の PROFINET デバイス検出 (DCP) ウィンドウ

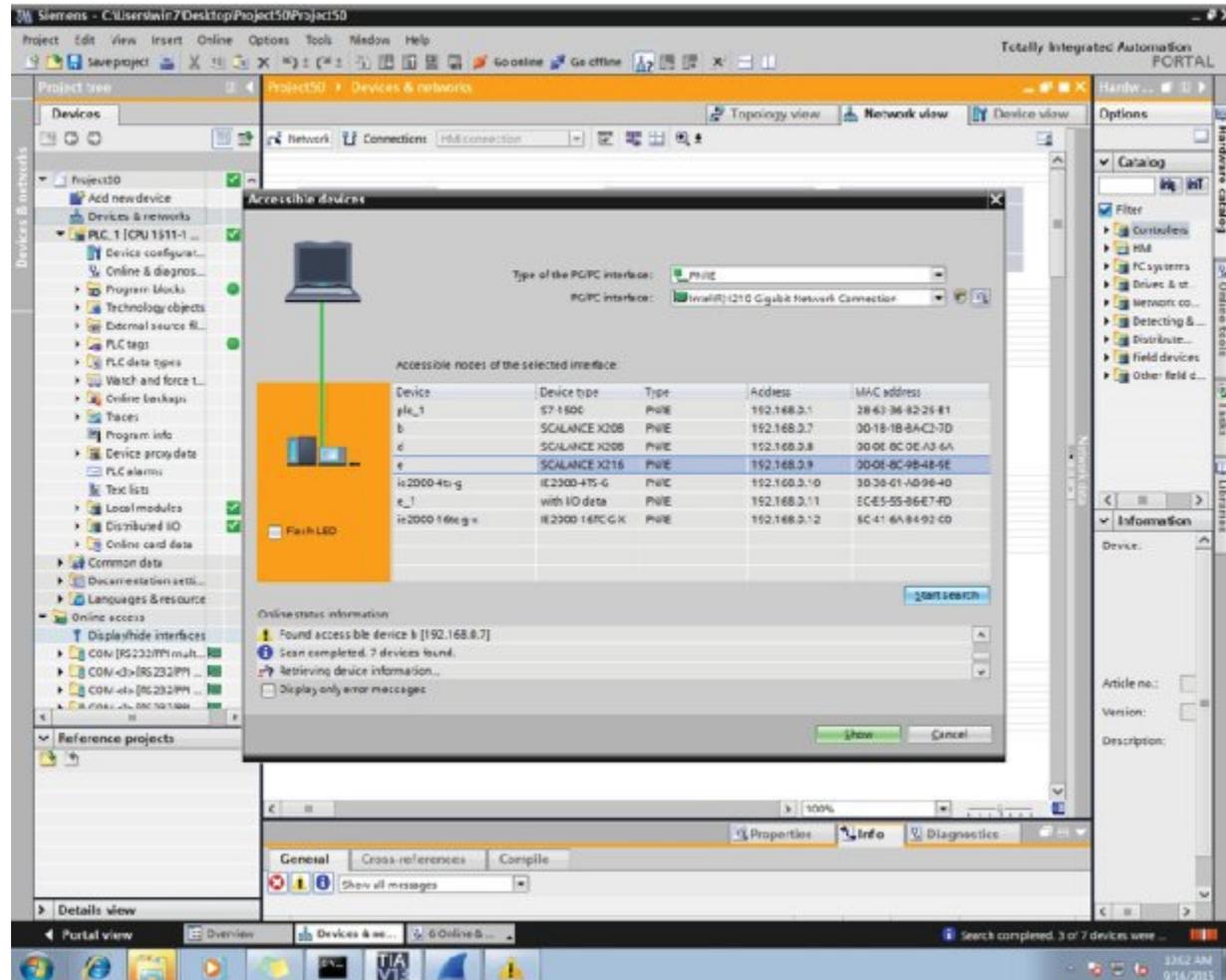


図 15: PROFINET MRP マネージャと MRP ドメインの定義

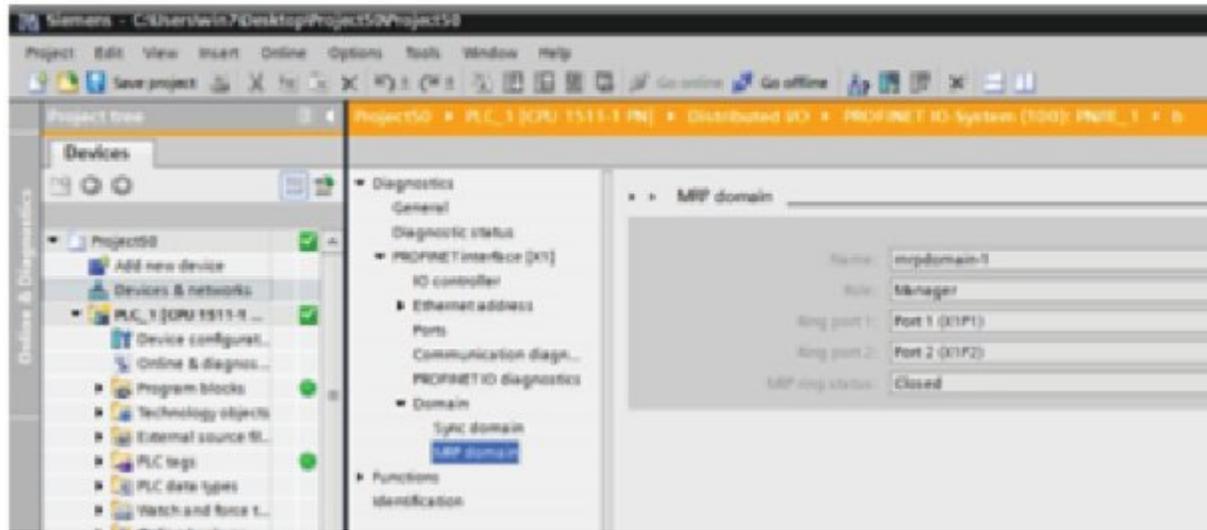


図 16: PROFINET MRP クライアントと MRP ドメインの定義

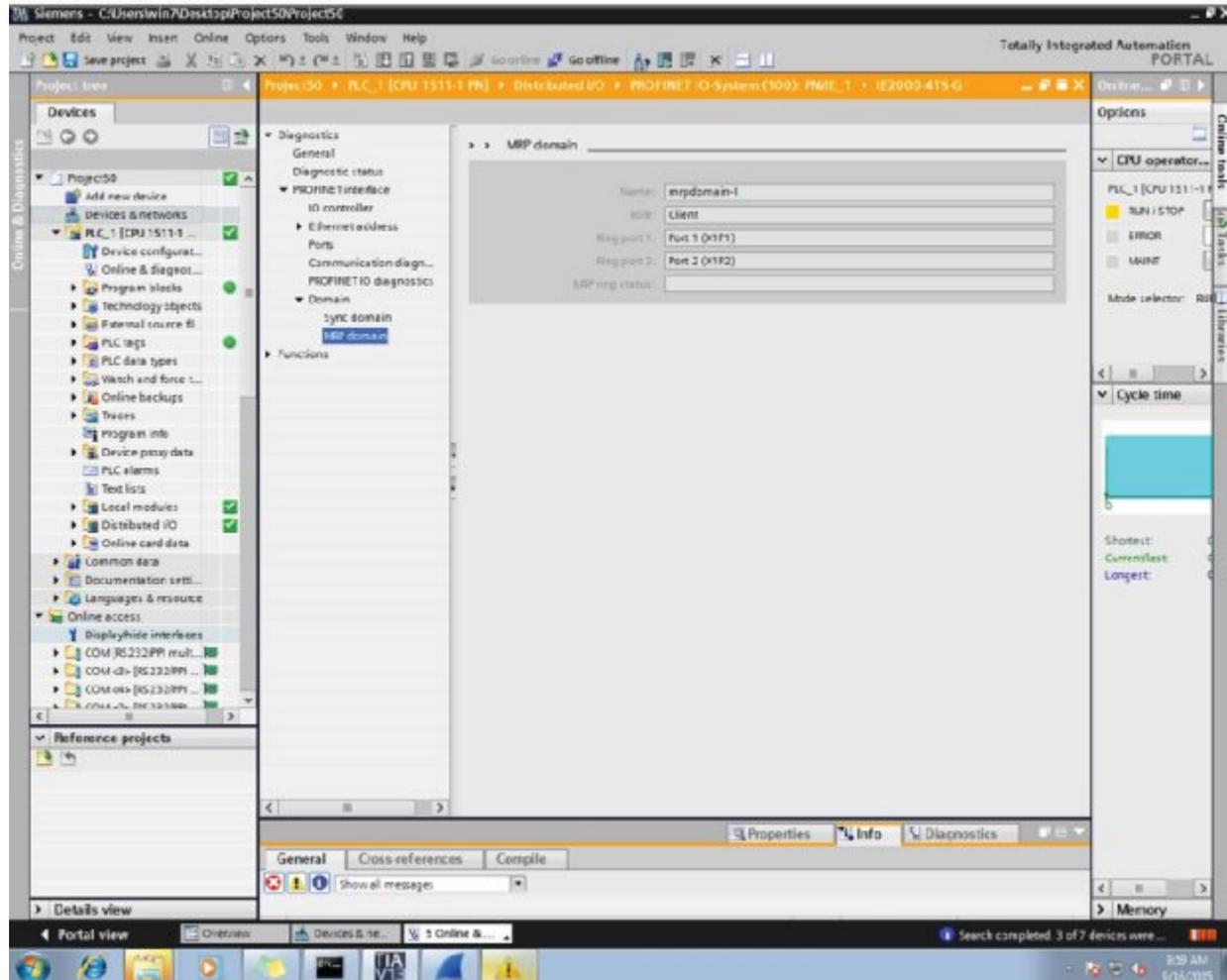


図 17: PROFINET MRP インターフェイスの定義

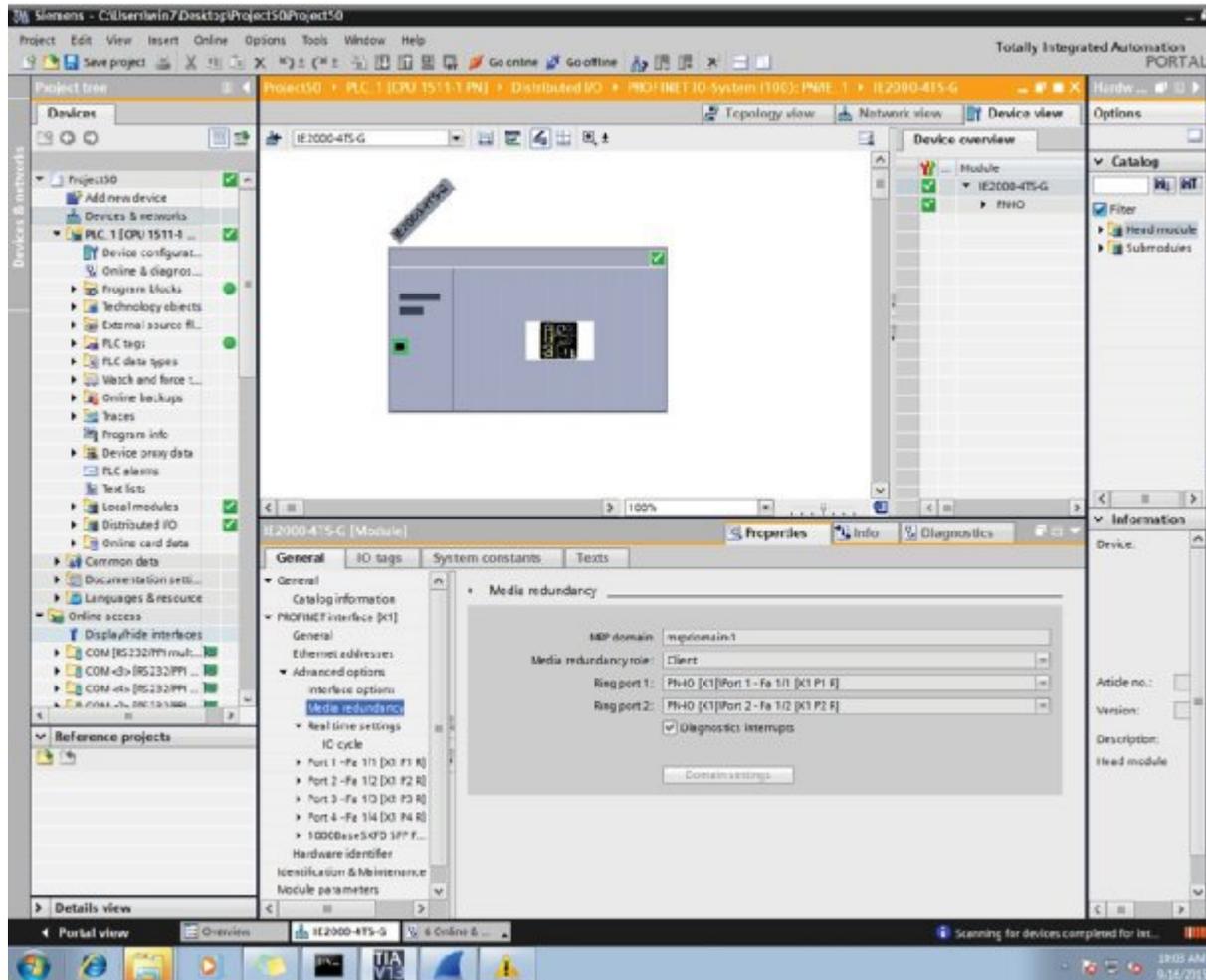
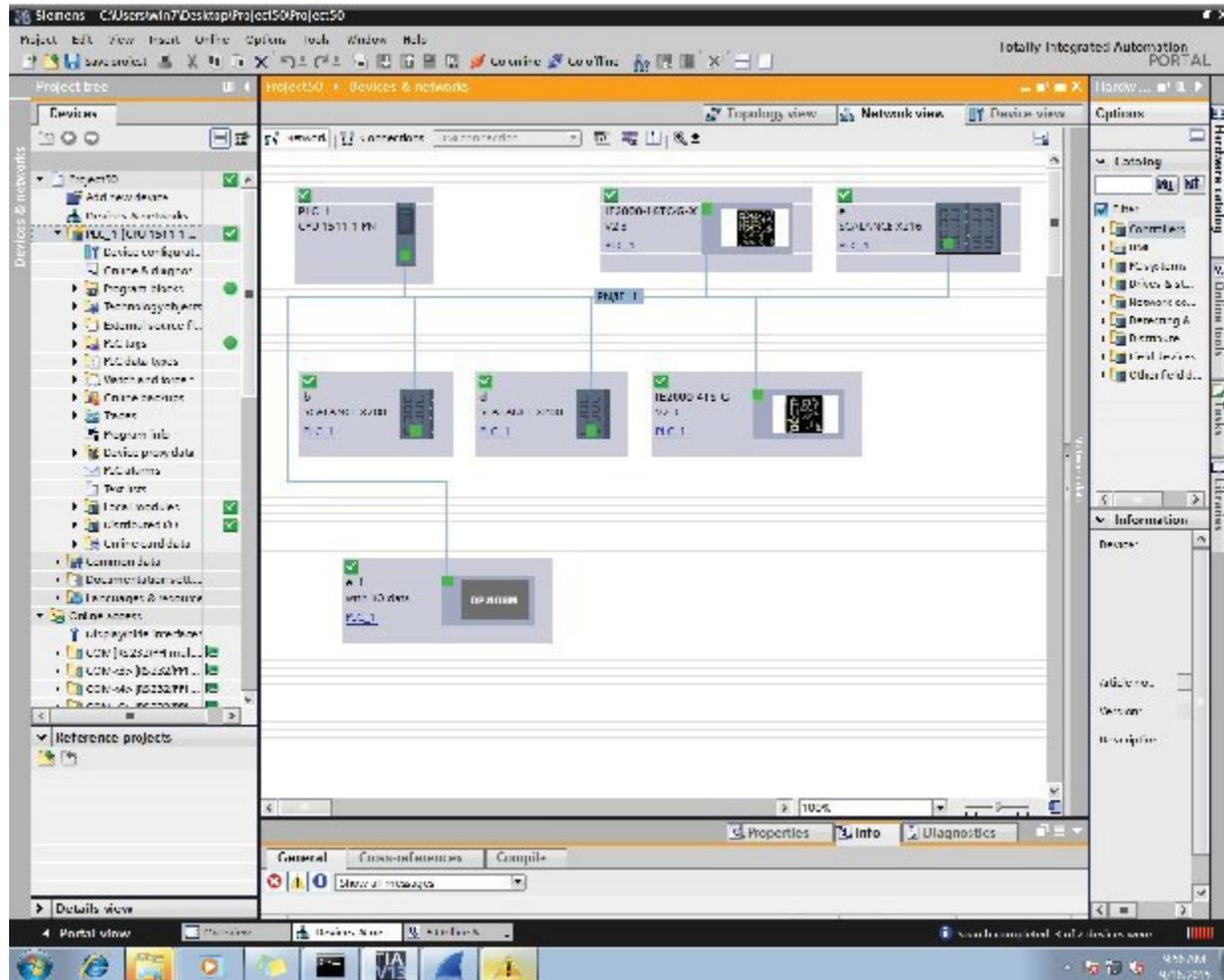


図 18: PROFINET MRP のネットワーク構成図



MRP CLI モードの設定

MRP を設定するには、ノードを MRA として設定し、2つの MRP ポートを指定します。

スタックセットアップでは最大 16 のリングを設定でき、スタンドアロンノードでは最大 12 のリングを設定できます。

次の MRP 設定パラメータはオプションです。

- domain-id : MRP リングを表す一意の ID。
- domain-name : 設定した MRP ドメイン ID の論理名。
- profile : 200 ミリ秒 (デフォルト)
- vlan-id : MRP フレームを送信するための VLAN。

MRP マネージャの設定

スイッチをデフォルトである MRP CLI モードの MRA として設定するには、次の手順に従います。



(注) デバイスが PLC モジュールに接続されている場合、MRP に対して「no device in the ring」が選択されていることを確認します。

手順の概要

1. MRP を有効化します。
2. スイッチで MRP マネージャモードを設定します。
3. (単一の MRP リングの場合はオプション) ドメイン ID を設定します。
4. (単一の MRP リングの場合はオプション) ドメイン名を設定します。
5. (任意) VLAN ID を設定します。
6. (任意) リカバリ プロファイルを設定します。
7. MRA の優先順位を設定します。
8. 間隔を設定します。
9. 最初のリング ポートとして動作するポートの ID を指定します。
10. インターフェイス モードを設定します。
11. MRP リングにインターフェイスを関連付けます。
12. グローバル コンフィギュレーション モードに戻ります。
13. 2 番目のリング ポートとして動作するポートの ID を指定します。
14. インターフェイス モードを設定します。
15. MRP リングにインターフェイスを関連付けます。
16. 特権 EXEC モードに戻ります。
17. (複数のリングの場合) リングを追加するごとに、ステップ 1 ~ 14 を繰り返します。

手順の詳細

手順

ステップ 1 MRP を有効化します。

```
mrp ring mrp_id
```

指定されたリング ID で MRP リングを設定します。

ステップ 2 スイッチで MRP マネージャモードを設定します。

```
mode auto-manager
```

ステップ 3 (単一の MRP リングの場合はオプション) ドメイン ID を設定します。

domain-id *value*

value : ハイフンによって 5 つのグループに分けられた 32 桁の 16 進数の UUID 文字列

例 : 550e8400-e29b-41d4-a716-446655440000

リング 1 のデフォルト ドメイン ID は FFFFFFFF-FFFF-FFFF-FFFF-FFFFFFFFFFFFE です。

(注)

ドメイン ID は、必要な場合にのみデフォルトから変更します。

ステップ 4 (単一の MRP リングの場合はオプション) ドメイン名を設定します。

domain-name *name*

name : 最大 32 文字の文字列

ステップ 5 (任意) VLAN ID を設定します。

vlan-id *vlan*

ステップ 6 (任意) リカバリ プロファイルを設定します。

profile { **200** | **500** }

- 200 : 最大リカバリ時間 200 ミリ秒
- 500 : 最大リカバリ時間 500 ミリ秒

ステップ 7 MRA の優先順位を設定します。

priority *value*

value : 範囲は <36864 ~ 61440> で、最低値は 65535。

デフォルトの優先順位は 40960 です。

ステップ 8 間隔を設定します。

interval *interval*

(注)

[Interval] フィールドは、MRP の WebUI には表示されません。

- 20 : 200 ミリ秒プロファイルに対する MRP_Test のデフォルト間隔 20 ミリ秒
- 50 : 500 ミリ秒プロファイルに対する MRP_Test のデフォルト間隔 50 ミリ秒

ステップ 9 最初のリング ポートとして動作するポートの ID を指定します。

interface *port*

ステップ 10 インターフェイス モードを設定します。

switchport mode { **access** | **trunk** }

(注)

MRP をアクセスモードで設定するには **switchport mode access** を指定する必要があります。

ステップ 11 MRP リングにインターフェイスを関連付けます。

```
mrp ring 1
```

ステップ 12 グローバル コンフィギュレーション モードに戻ります。

```
exit
```

ステップ 13 2 番目のリング ポートとして動作するポートの ID を指定します。

```
interface port
```

ステップ 14 インターフェイス モードを設定します。

```
switchport mode { access | trunk }
```

(注)

MRP をアクセスモードで設定するには、この手順で **switchport mode access** を指定する必要があります。

ステップ 15 MRP リングにインターフェイスを関連付けます。

```
mrp ring 1
```

ステップ 16 特権 EXEC モードに戻ります。

```
end
```

ステップ 17 (複数のリングの場合) リングを追加するごとに、ステップ 1 ~ 14 を繰り返します。

- 2 番目のリングにリング番号 2 を割り当てます。
- リング 2 に一意のドメイン ID を割り当てます。リング 2 のデフォルト ドメイン ID は FFFFFFFF-FFFF-FFFF-FFFF-FFFFFFFFFFFFD です。
- 3 番目のリングにリング番号 3 を割り当てます。
- リング 3 に一意のドメイン ID を割り当てます。リング 3 のデフォルトドメイン ID は FFFFFFFF-FFFF-FFFF-FFFF-FFFFFFFFFFFFC です。

(注)

各リングには固有のドメイン ID が必要です。2 つのリングで同じドメイン ID を共有することはありません。

例

次に、MRP 自動マネージャを設定する例を示します。

```
Switch#configure terminal
Switch# no profinet mrp
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#mrp ring 1
Switch(config-mrp)#mode manager
Switch(config-mrp-manager)#domain-id FFFFFFFF-FFFF-FFFF-FFFF-FFFFFFFFFFFFE
Switch(config-mrp-manager)#priority 40960
```

```

Switch(config-mrp-manager) #end
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config) #GigabitEthernet1/0/22
Switch(config-if) #switchport mode trunk
Switch(config-if) #mrp ring 1
WARNING% Enabling MRP automatically set STP FORWARDING. It is recommended to shutdown
all interfaces which are not currently in use to prevent potential bridging loops.
Switch(config-if) #exit
Switch(config) #GigabitEthernet1/0/21
Switch(config-if) #switchport mode trunk
Switch(config-if) #mrp ring 1
WARNING% Enabling MRP automatically set STP FORWARDING. It is recommended to shutdown
all interfaces which are not currently in use to prevent potential bridging loops.
Switch(config-if) #exit
Switch(config-if) #end

Switch# show mrp ring 1
MRP ring 1

Profile : 200 ms
Mode : Auto-Manager
Priority : 40960
Operational Mode: Client
From : CLI
License : Active
Best Manager :
MAC Address : 00:78:88:5E:03:81
Priority : 36864

Network Topology: Ring
Network Status : OPEN
Port1: Port2:
MAC Address :84:B8:02:ED:E8:02 MAC Address :84:B8:02:ED:E8:01
Interface :GigabitEthernet1/0/22 Interface :GigabitEthernet1/0/21
Status :Forwarding Status :Forwarding

VLAN ID : 1
Domain Name : Cisco MRP Ring 1
Domain ID : FFFFFFFF-FFFF-FFFF-FFFF-FFFFFFFFFFFFFFE

Topology Change Request Interval : 10ms
Topology Change Repeat Count : 3
Short Test Frame Interval : 10ms
Default Test Frame Interval : 20ms
Test Monitoring Interval Count : 3
Test Monitoring Extended Interval Count : N/A
Switch#show mrp ports

Ring ID : 1
PortName                Status
-----
GigabitEthernet1/0/22   Forwarding
GigabitEthernet1/0/21   Forwarding

```



(注) **show mrp ring** の出力には、Cisco IOS XE リリース 17.7.1 以降の CLI および Profinet モードでは「License: Not Applicable」と表示されます。

設定例

次に、マネージャとして設定された MRP スイッチの例を示します。

```
Switch#configure terminal
Switch# no profinet mrp
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#mrp ring 1
Switch(config-mrp)#mode manager
Switch(config-mrp-manager)#end
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#interface g1/0/21-28
Switch(config-if)#switchport mode trunk
Switch(config-if)#mrp ring 1
WARNING% Enabling MRP automatically set STP FORWARDING. It is recommended to shutdown
all interfaces which are not currently in use to prevent potential bridging loops.
Switch(config-if)#exit
Switch(config)#interface g1/0/27
Switch(config-if)#switchport mode trunk
Switch(config-if)#mrp ring 1
WARNING% Enabling MRP automatically set STP FORWARDING. It is recommended to shutdown
all interfaces which are not currently in use to prevent potential bridging loops.
Switch(config-if)#end

Switch#show mrp ring
MRP ring 1

Profile      : 200 ms
Mode        : Master
From        : CLI

Network Topology: Ring
Port1:
MAC Address  :2C:54:2D:2C:3E:0A
Interface    :gigabitEthernet1/0/28
Status       :Forwarding
Port2:
MAC Address  :2C:54:2D:2C:3E:09
Interface    :gigabitEthernet1/0/27
Status       :Forwarding

VLAN ID      : 1
Domain Name  : Cisco MRP
Domain ID    : FFFFFFFF-FFFF-FFFF-FFFF-FFFFFFFFFFFFE

Topology Change Request Interval      : 10ms
Topology Change Repeat Count          : 3
Short Test Frame Interval              : 10ms
Default Test Frame Interval           : 20ms
Test Monitoring Interval Count         : 3
Test Monitoring Extended Interval Count : N/A
Switch#show mrp ports

Ring ID : 1
PortName          Status
-----
gigabitEthernet1/0/27    Forwarding
gigabitEthernet1/0/28    Forwarding
```

次に、自動マネージャとして設定された MRP スイッチの例を示します。

```
Switch#configure terminal
```

```

Switch# no profinet mrp
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#mrp ring 1
Switch(config-mrp)#mode auto-manager
Switch(config-mrp-auto-manager)#priority 36864
Switch(config-mrp-auto-manager)#end
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#interface gil/0/22
Switch(config-if)#switchport mode trunk
Switch(config-if)#mrp ring 1
WARNING% Enabling MRP automatically set STP FORWARDING. It is recommended to shutdown
all interfaces which are not currently in use to prevent potential bridging loops.
Switch(config-if)#exit
Switch(config)#interface gil/0/21
Switch(config-if)#switchport mode trunk
Switch(config-if)#mrp ring 1
WARNING% Enabling MRP automatically set STP FORWARDING. It is recommended to shutdown
all interfaces which are not currently in use to prevent potential bridging loops.
Switch(config-if)#end

```

```

Switch#show mrp ring
MRP ring 1

Profile      : 200 ms
Mode         : Auto-Manager
Priority      : 36864
Operational Mode: Manager
From         : CLI
License      : Active
Best Manager MAC Address :84:B8:02:ED:E8:01      priority 36864

```

```

Network Topology: Ring
Network Status  : OPEN

Port1:
MAC Address     :84:B8:02:ED:E8:02      MAC Address     :84:B8:02:ED:E8:01
Interface       :GigabitEthernet1/0/22  Interface       :GigabitEthernet1/0/21
Status          :Forwarding              Status          :Forwarding

```

```

VLAN ID        : 1
Domain Name    : Cisco MRP Ring 1
Domain ID      : FFFFFFFF-FFFF-FFFF-FFFF-FFFFFFFFFFFFE

```

```

Topology Change Request Interval      : 10ms
Topology Change Repeat Count          : 3
Short Test Frame Interval             : 10ms
Default Test Frame Interval           : 20ms
Test Monitoring Interval Count        : 3
Test Monitoring Extended Interval Count : N/A

```

```

Topology Change Request Interval      : 10ms
Topology Change Repeat Count          : 3
Short Test Frame Interval             : 10ms
Default Test Frame Interval           : 20ms
Test Monitoring Interval Count        : 3
Test Monitoring Extended Interval Count : N/A

```

次に、設定済みの MRP スイッチの例を示します。

```

Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#mrp ring 1

```

```

Switch(config-mrp)#mode client
Switch(config-mrp-client)#end
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#interface gi1/0/23
Switch(config-if)#switchport mode trunk
Switch(config-if)#mrp ring 1
Switch(config-if)#exit
Switch(config)#interface gi1/0/24
Switch(config-if)#switchport mode trunk
Switch(config-if)#mrp ring 1
Switch(config-if)#end

```

設定の確認

次のコマンドを使用して、MRP 設定を確認します。

コマンド	説明
<code>show mrp ring? {1 - 22}</code>	MRP リングの設定の詳細を表示します。
<code>show mrp ports</code>	MRP ポート状態の詳細を表示します。いずれのポートでも MRP が設定されていない場合、「N/A」と表示されます。
<code>show mrp ring {1 - 22} statistics [all event hardware packet platform]</code>	MRP リングの動作の詳細を表示します。
<code>debug mrp-ring [alarm cli client license manager packet platform]</code>	MRP イベントをトレースします。 (注) manager は、スイッチがマネージャまたは自動マネージャとして設定されている場合にのみ使用可能です。 license は、Cisco IOS XE 17.6.x 以前でのみ使用できません。
<code>show tech-support mrp</code>	すべての MRP の詳細を表示します。

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 17.17.1	IE9300 スタック上の MRP	Cisco IOS-XE 17.17.1 以降では、Media Redundancy Protocol (MRP) のスタックサポートが導入されています。
Cisco IOS XE 17.13.1	Media Redundancy Protocol (MRP)	Cisco IOS-XE 17.13.1 以降では、スタンドアロン IE9300 スイッチで 200 ミリ秒または 500 ミリ秒のコンバージェンス プロファイルを使用した 12 のリングがサポートされます。



第 5 章

高可用性シームレス冗長性

- [高可用性シームレス冗長性 \(109 ページ\)](#)
- [注意事項と制約事項 \(115 ページ\)](#)
- [デフォルト設定 \(117 ページ\)](#)
- [HSR リングの設定 \(119 ページ\)](#)
- [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 \(120 ページ\)](#)
- [設定の確認 \(121 ページ\)](#)
- [設定例 \(121 ページ\)](#)
- [関連資料 \(125 ページ\)](#)
- [機能の履歴 \(125 ページ\)](#)

高可用性シームレス冗長性

高可用性シームレス冗長性 (HSR) は、国際標準規格 IEC 62439-3-2016 第 5 条で定義されています。HSR は Parallel Redundancy Protocol (PRP) に似ていますが、リングトポロジで動作するように設計されています。任意のトポロジの並列独立ネットワーク 2 系統 (LAN-A と LAN-B) の代わりに、HSR は反対方向のトラフィックを持つリングを定義します。このリングで、ポート A はトラフィックを反時計回りに送信し、ポート B はトラフィックを時計回りに送信します。

HSR は、パケット形式も PRP と異なります。スイッチが重複パケットを判別して廃棄できるように、追加のプロトコル固有情報がデータフレームとともに送信されます。PRP の場合、これは冗長制御トレーラ (RCT) と呼ばれるトレーラの一部として送信されますが、HSR の場合は HSR ヘッダーと呼ばれるヘッダーの一部として送信されます。RCT と HSR ヘッダーの両方にシーケンス番号が含まれています。これは、受信したフレームが最初のインスタンスか重複したインスタンスかを判断するために使用されるプライマリデータです。



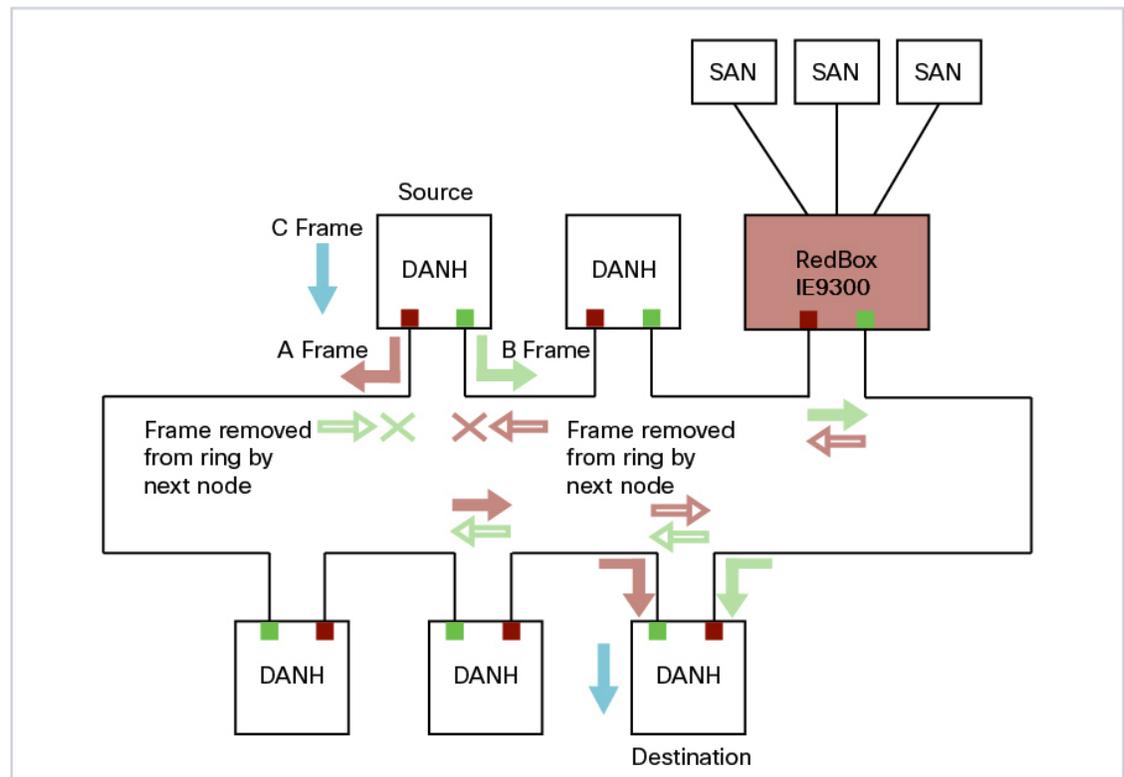
- (注) HSR は Cisco Catalyst IE9300 高耐久性シリーズ スイッチの特定の SKU でサポートされています (サポートされている SKU については、このガイドの「ガイドラインと制限事項」の項を参照してください)。このドキュメントでは、特に明記されていない限り、「スイッチ」という用語は Cisco Catalyst IE9300 高耐久性シリーズ スイッチを指します。

このリリースでは、スイッチは HSR 単一接続ノード (SAN) と 1 つの HSR インスタンスのみをサポートします。また、1 つの HSR または 1 つの PRP インスタンスのみ作成できます。PRP インスタンスを作成した場合、HSR インスタンスは作成できません。

HSR リングに接続された 2 つのインターフェイスを持つ非スイッチングノードは、「HSR 実装ダブル接続ノード (DANH)」と呼ばれます。PRP と同様に、単一接続ノード (SAN) は、RedBox (冗長ボックス) と呼ばれるデバイスを介して HSR リングに接続されます。RedBox は、RedBox が送信元または接続先となるすべてのトラフィックに対して DANH として機能します。スイッチは、HSR リング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。

次の図は、IEC 62439-3 に記載されている HSR リングの例を示します。この例では、RedBox は Cisco Catalyst IE9300 高耐久性シリーズ スイッチです。

図 19: ユニキャストトラフィックを伝送する HSR リングの例



追加設定なしで HSR をサポートしないデバイス (ラップトップやプリンタなど) を HSR リングに直接接続することはできません。これは、すべての HSR 対応デバイスが、リングから受

信するパケットの HSR ヘッダーを処理でき、リングに送信するすべてのパケットに HSR ヘッダーを追加できる必要があるためです。これらのノードは、RedBox を介して HSR リングに接続されます。上の図に示されているように、RedBox には DANH 側に 2 つのポートがあります。非 HSR SAN デバイスは、上流に位置するスイッチポートに接続されます。RedBox は、これらのデバイス向けに監視フレームを生成し、これらのデバイスがリング上で DANH デバイスとみなされるようにします。RedBox が DANH としてエミュレートするため、これらのデバイスは仮想ダブル接続ノード (VDAN) と呼ばれます。

ループ回避

HSR リング内の各ノードは、一方のポートから受信したフレームを HSR ペアの他方のポートに転送します。ループを避け、ネットワーク帯域を有効に使用するため、RedBox では、すでに同じ方向に転送されたフレームは送信されません。ノードがパケットをリングに入れると、そのパケットはループを避けるために次のように処理されます。

- 宛先がリング内のユニキャストパケット：ユニキャストパケットが宛先ノードに到達すると、パケットはそれぞれのノードによって消費され、転送されません。
- 宛先がリング内がないユニキャストパケット：このパケットはリング内に宛先ノードがないため、送信元ノードに到達するまでリング内のすべてのノードによって転送されます。各ノードは、送信したパケットの記録を、それが送信された方向とともに保持するため、送信元ノードは、パケットがループを 1 周したことを検出し、パケットを破棄します。
- マルチキャストパケット：マルチキャストパケットには、このパケットのコンシューマが複数存在する可能性があるため、各ノードによって転送されます。このため、マルチキャストパケットは常に送信元ノードに到達します。ただし、すべてのノードは、受信したパケットをすでに送信インターフェイスを介して転送したかどうかを確認します。パケットが送信元ノードに到達すると、送信元ノードは、このパケットをすでに転送したことを確認し、再度転送せずにパケットを破棄します。

HSR RedBox の動作モード

最も基本的な動作モードは、HSR-SAN モード (シングル RedBox モード) です。このモードでは、RedBox を使用して SAN デバイスが HSR リングに接続されます。このモードでの Redbox の役割は、SAN デバイスをリングの VDAN として表すことです。



(注) このリリースでは、スイッチは HSR-SAN モードのみをサポートします。

HSR SAN モード

HSR-SAN モードでは、RedBox がホストに代わって HSR タグを挿入し、ノード自体から送信されたフレーム、重複フレーム、およびノードが一意的宛先であるフレームを除き、リングトラフィックを転送します。このモードでは、パケットが次のように処理されます。

- 送信元 DANH は上位レイヤから渡されたフレーム（C フレーム）を送信し、フレームの重複を識別するために HSR タグをプレフィックスとして付記してから、各ポートを介してフレーム（A フレームと B フレーム）を送信します。
- 宛先 DANH は、一定の間隔内に各ポートから 2 つの同一フレームを受信します。宛先 DANH は、最初のフレームの HSR タグを削除してから上位レイヤに渡し、重複フレームを破棄します。
- HSR リング内の各ノードは、一方のポートから受信したフレームを HSR ペアの他方のポートに転送します。次の条件を満たした場合、ノードが一方のポートで受信したフレームを他方のポートに転送することはありません。
 - 受信したフレームが、リングを回って発信元ノードに戻ってきたものである。
 - フレームが、受信ノードの上流のノードを宛先 MAC アドレスとするユニキャストフレームである。
 - ノードが同じフレームを同じ方向に送信したことがある。このルールによって、無限ループでフレームがリング内で回転し続けるのを回避する。

HSR の CDP と LLDP

HSR は Cisco Discovery Protocol (CDP) および Link Layer Discovery Protocol (LLDP) に対応しています。CDP および LLDP は、レイヤ 2 ネイバー探索プロトコルです。CDP と LLDP ではどちらも、デバイスに直接接続されているノードに関する情報が提供されます。また、ローカルおよびリモートインターフェイスやデバイス名などの追加情報も提供されます。

CDP または LLDP が有効になっている場合、その CDP または LLDP の情報を使用して HSR リング上の隣接ノードとそのステータスを検索できます。次に、各ノードのネイバー情報を使用して完全な HSR ネットワークトポロジを特定し、リング障害をデバッグおよび特定できます。

CDP と LLDP は、物理インターフェイスでのみ設定されます。

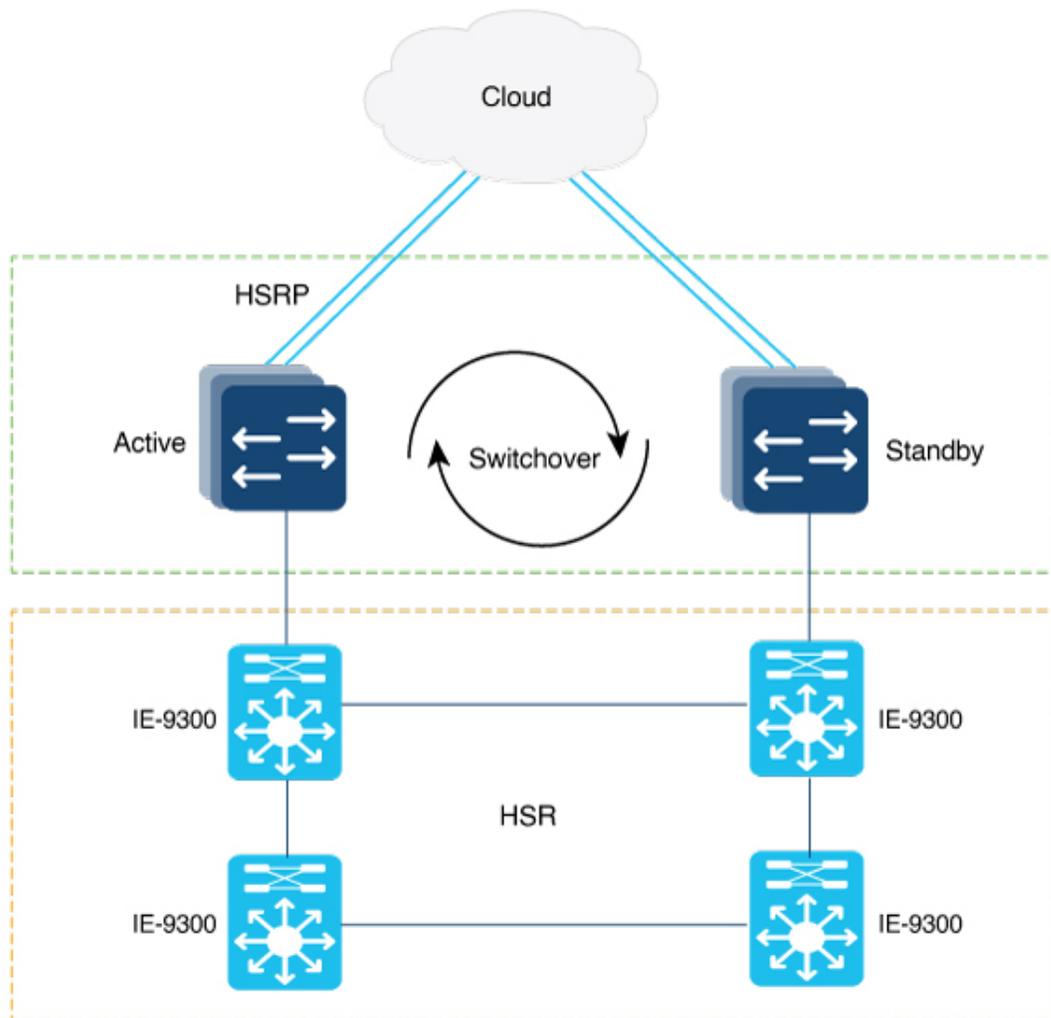
詳細については、「HSR リングの設定」および「設定の確認」を参照してください。

HSR アップリンクの冗長性に関する機能拡張

HSR アップリンクの冗長性に関する機能拡張により、2 つの個別のインターフェイスを 2 つの個別の HSR RedBox を介して HSR リングから上流に接続できるといった、柔軟な設計が可能になります。これにより、HSR リングの出口における単一障害点がなくなります。この機能を利用して高可用性を改善できるプロトコルの例には、HSRP、VRRP、REP などがあります。この機能拡張が行われる以前は、これらのプロトコルが冗長アップリンクで使用されていると、ネクストホップ スプリットブレイン状態や REP フェールオーバー時間の遅延など、望ましくない結果が発生することがありました。

次の図は、HSR リングからのアップリンク ネクストホップゲートウェイの冗長性を実現する、HSR と HSRP を使用したネットワークの例を示しています。

図 20: HSRP を使用したネットワーク冗長性の例



HSR のアップリンク冗長性を実装するには、**fpgamode-DualUplinkEnhancement** 機能が無効になっていないことを確認します。この機能は、ディストリビューションレイヤのデュアルルータ（この場合は HSRP）への接続をサポートするために必要です。

```
Switch#show hsr ring 1 detail | include fpgamode
fpgamode-DualUplinkEnhancement: Enabled
```

出力に「*fpgamode-DualUplinkEnhancement,;Disabled*」と表示される場合は、次のコマンドを発行します。

```
Switch# conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# hsr-ring 1 fpgamode-DualUplinkEnhancement
Switch(config)# end
```

HSRP の設定

次の HSRP 設定の例は、上図の2つのディストリビューションスイッチ（アクティブとスタンバイ）に適用されます。次の設定では、HSRP がスイッチ仮想インターフェイス（SVI）で設定されています。

```
Active# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Active(config)# interface vlan 10
Active(config-if)# ip address 30.30.30.2 255.255.255.0
Active(config-if)# standby 1 ip 30.30.30.1
Active(config-if)# standby 1 priority 120
Active(config-if)# end

Standby# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Standby(config)# interface Vlan10
Standby(config-if)# ip address 30.30.30.4 255.255.255.0
Standby(config-if)# standby 1 ip 30.30.30.1
Standby(config-if)# end

Active# show standby
Vlan10 - Group 1
  State is Active
    8 state changes, last state change 00:03:55
    Track object 1 (unknown)
  Virtual IP address is 30.30.30.1
  Active virtual MAC address is 0000.0c07.ac01 (MAC In Use)
    Local virtual MAC address is 0000.0c07.ac01 (v1 default)
  Hello time 200 msec, hold time 750 msec
    Next hello sent in 0.176 secs
  Preemption enabled, delay min 5 secs, reload 5 secs, sync 5 secs
  Active router is local
  Standby router is 30.30.30.4, priority 100 (expires in 0.656 sec)
  Priority 120 (configured 120)
  Group name is "hsrp-Vl10-1" (default)
  FLAGS: 0/1
Active# show standby brief
          P indicates configured to preempt.
          |
Interface   Grp  Pri P State   Active           Standby           Virtual IP
Vl10         1    120 P Active  local            30.30.30.4       30.30.30.1

Standby# show standby
Vlan10 - Group 1
  State is Standby
    13 state changes, last state change 00:04:17
    Track object 1 (unknown)
  Virtual IP address is 30.30.30.1
  Active virtual MAC address is 0000.0c07.ac01 (MAC Not In Use)
    Local virtual MAC address is 0000.0c07.ac01 (v1 default)
  Hello time 200 msec, hold time 750 msec
    Next hello sent in 0.064 secs
  Preemption enabled, delay min 5 secs, reload 5 secs, sync 5 secs
  Active router is 30.30.30.2, priority 120 (expires in 0.816 sec)
  Standby router is local
  Priority 100 (default 100)
  Group name is "hsrp-Vl10-1" (default)
  FLAGS: 0/1
Standby# show standby brief
          P indicates configured to preempt.
          |
```

Interface	Grp	Pri	P	State	Active	Standby	Virtual IP
Vl10	1	100	P	Standby	30.30.30.2	local	30.30.30.1

注意事項と制約事項

- HSR-SANは、次の Cisco Catalyst IE9300 高耐久性シリーズ スイッチでのみサポートされています。
 - IE-9320-26S2C-EおよびIE-9320-26S2C-A
 - IE-9320-22S2C4X-EおよびIE-9320-22S2C4X-A
- HSR-SAN（シングル RedBox モード）は、このリリースでサポートされる唯一の HSR モードです。
- HSR は、スタンドアロン展開でのみサポートされます。スタック構成のスイッチでは HSR はサポートされません。
- サポートされる HSR インスタンスは 1 つだけです。スイッチでは 1 つの HSR または 1 つの PRP インスタンスのみがサポートされるため、PRP インスタンスが作成されている場合は HSR インスタンスを作成できないことに注意してください。
- HSR リング 1 は、ポートのペア（Gi1/0/21 と Gi1/0/22、または Gi1/0/23 と Gi1/0/24）としてのみ設定できます。これらのポートペアを使用して、HSR リングを 1 つ設定できます。
- HSR 機能には、Network Essentials ライセンスが必要です。
- HSR 機能はデフォルトでは有効になっていないため、HSR リングを明示的に設定する必要があります。
- 必要なファームウェアイメージがシステムで使用できない場合、HSR は自動的に無効になります。
- ポートがリングの一部になると、ポートのメディアタイプ、速度、およびデュプレックス設定を変更することはできません。リングのメンバーシップを設定する前に、これらの設定を適用することを推奨します。
- リングの設定後に HSR インターフェイスのモードがアクセスモードからトランクモードに、またはその逆に変更された場合は、HSR リングをフラップすることを推奨します。
- 推奨されるノードテーブル内のノードの最大数は 512 です。ノードは、同時にリングに接続できるすべての DANH および VDAN デバイスです。この数は絶対的な制限ではありませんが、エン트리数が多いほど、エンドデバイスが受信する重複パケットの数が増える可能性があります。
- HSR リング内の最大ノード数は 50 です。
- HSR リングポートは、L2 モードでのみ設定できます。
- HSR は、次のポートタイプでサポートされます。

- 100 Mbps、全二重。半二重はサポートされません。
 - 1000 Mbps、全二重。半二重はサポートされません。
 - HSR は、アップリンクポートではサポートされません。
- 1 つのリングの両方のポートを同じ速度とタイプにする必要があります（つまり、両方が SFP または銅線になります）。
 - 次のプロトコルと機能は、同じポート上の HSR と相互に排他的です。
 - PRP
 - EtherChannel
 - リンク集約制御プロトコル (LACP)
 - ポート集約プロトコル (PAgP)
 - Resilient Ethernet Protocol (REP)
 - MACsec、HSR、および PRP を同時に使用することはできません。
 - HSR を介した PTP はサポートされていません。
 - HSR では、MTU サイズが最大 1998 バイトのイーサネットペイロードがサポートされません。
 - STP は HSR リングではサポートされていません。デフォルトでは、スパンニングツリープロトコル (STP) のすべてのモードがリングポートで無効になります。
 - スイッチドポートアナライザ (SPAN) およびリモート SPAN (RSPAN) は、HSR ではサポートされていません。つまり、SPAN と RSPAN を使用して HSR リングのトラフィックを監視することはできません。また、RSPAN を使用して監視されているトラフィックは、HSR リングを介して転送しないでください。
 - HSR リング内のすべてのインターフェイスの速度とデュプレックスを同じ設定にすることが重要です。リングのメンバーシップを設定する前に、これらの設定を適用することを推奨します。
 - ポートがリングの一部になると、そのポートをシャットダウンすることはできません。
- たとえば、Gi1/0/23 と Gi1/0/24 が HSR リングの一部である場合、Gi1/0/23 または Gi1/0/24 をシャットダウンしようとしても、操作は許可されません。

```
Switch(config)# interface range gi1/0/23-24
Switch(config-if-range)#shutdown
%Interface GigabitEthernet1/0/23 is configured in a HSR ring shutdown not permitted!
Switch(config-if-range)#
```

HSR リングのシャットダウンを実行できます。次に例を示します。

```
Switch# conf t
Switch(config)#int hs1
Switch(config-if-range)#shut
```

- トランクモードやアクセスモードなどのVLAN設定は、リングに参加している両方のポートで同じにする必要があります。たとえば、HSRリング内のGi1/0/24とGi1/0/23がトランクモードである場合、いずれか1つのポートをアクセスモードに変更すると、リング内の両ポートがバンドルされなくなります。

```
Switch(config)# interface range gi1/0/23-24
Switch(config-if-range)# switchport mode access
Jul 27 22:00:27.809 IST: %EC-5-CANNOT_BUNDLE2: Gi1/0/23 is not compatible with
Gi1/0/24 and will be suspended (trunk mode of Gi1/0/23 is access, Gi1/0/24 is dynamic)
```

- インターフェイスがHSRリングに追加されると、プライマリインターフェイスカウンタのみが更新されます。物理インターフェイスがHSRリングに追加された後は、個々の物理インターフェイスを設定したり状態をチェックしたりする必要はありません。
- スイッチの2つのポートでHSRリングを設定するとすぐに、HSR設定がまだ適用されていない他のスイッチでMACフラップが観察されます。すべてのスイッチでリングを設定する前に、スイッチで新しく作成したHSRリングをシャットダウンし、以下に示すように1つずつ再度有効にすることを推奨します。たとえば、リング内に4つのスイッチがある場合は、各スイッチでHSRリングインターフェイスを無効にします。

```
Switch1(config)# interface range gi1/0/21-22
Switch1(config-if-range)# shutdown
Switch1(config-if-range)# hsr-ring 1
Creating a HSR-ring interface hs1
Switch1(config-if-range)# int hs1
Switch1(config-if-range)# shutdown
Switch1(config-if-range)# end
```

4つのスイッチすべてにリングを設定したら、各スイッチのHSRポートを再度有効にします。

```
Switch1# conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch1(config)# interface range gi1/0/21-22
Switch1(config-if-range)# int hs1
Switch1(config-if-range)# no shutdown
Switch1(config-if-range)# end
Switch1#
```

これにより、メンバースイッチでHSRリングを設定する際に暫定的なMACフラッピングが発生しないようにします。

デフォルト設定

表 1: HSRリングのパラメータ

パラメータ	説明	範囲	デフォルト値
entryForgetTime	重複する廃棄テーブルから非アクティブなエントリをクリアする時間。	0 ~ 65535	400 ミリ秒

パラメータ	説明	範囲	デフォルト値
fpgamode-DualUplinkEnhancement	送信元 MAC のフィルタリング用 FPGA レジスタを設定します。	有効または無効	有効
nodeForgetTime	ノードテーブルから非アクティブなエントリをクリアする時間。	0 ~ 65535	6000 ミリ秒
nodeRebootInterval	起動後に RedBox が監視フレームの送信を開始しなければならない時間。	0 ~ 65535	500 ミリ秒
pauseFrameTime	HSR ポーズフレーム間の時間間隔。	0 ~ 65535	25 ミリ秒
proxyNodeTableForgetTime	プロキシノードテーブルまたはVDANテーブルから非アクティブなエントリをクリアする時間。	0 ~ 65535	6000 ミリ秒
supervisionFrameLifeCheckInterval	監視フレームのライフチェック間隔値。	0 ~ 65535	2000 ミリ秒
supervisionFrameOption			
mac-da	監視フレームの宛先 MAC アドレスに含まれる最後のバイト (01:15:4E:00:01:00)。末尾の 00 は、このパラメータの値に置き換えられます。	MACDA の最後の 8 ビットオプション値 (1 ~ 255)。	デフォルトなし
vlan-cfi	VLAN タグ付きフレームの Canonical Format Indicator (CFI) を有効にします。	有効または無効	無効
vlan-cos	監視フレームの VLAN タグに設定するサービスクラス (COS) 値。	0 ~ 7	0
vlan-id	監視フレームの VLAN タグ。	0 ~ 4095	0

パラメータ	説明	範囲	デフォルト値
vlan-tagged	VLAN タギングオプションを設定します。	有効または無効	無効
supervisionFrameRedboxMacaddress	監視フレーム内の RedBox MAC アドレス。	48 ビット RedBox MAC アドレス	インターフェイス HSR リング MAC アドレス
supervisionFrameTime	監視フレーム間の時間間隔。	0 ~ 65535	3 ミリ秒

HSR リングの設定

HSR リングを設定するには、次の手順に従います。

始める前に

- この章の[注意事項と制約事項 \(115 ページ\)](#) セクションを読み、理解します。
- HSR リングを設定する前に、HSR リング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

-
- 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。
- ```
Switch# configure terminal
```
- ステップ 2** (任意) CDP をグローバルに有効にして、HSR リングノードに関する情報を提供します。
- ```
Switch(config)# cdp run
```
- ステップ 3** (任意) LLDP をグローバルに有効にして、HSR リングノードに関する情報を提供します。
- ```
Switch(config)# lldp run
```
- ステップ 4** インターフェイス コンフィギュレーション モードに入り、HSR リングに割り当てるポートで PTP を無効にします。
- ```
Switch(config)# interface range gi1/0/21-22  
Switch(config-if-range)# no ptp enable
```
- ステップ 5** (任意) HSR リングに割り当てるポートで CDP を有効にします。
- ```
Switch(config-if-range)#cdp enable
```
- ステップ 6** (任意) HSR リングに割り当てるポートで LLDP を有効にします。

## 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

```
Switch(config-if-range)#lldp transmit
Switch(config-if-range)#lldp receive
```

**ステップ7** HSR リングを設定する前に、ポートをシャットダウンします。

```
Switch(config-if-range)# shutdown
```

**ステップ8** HSR リングインターフェイスを作成して、ポートを HSR リングに割り当てます。

```
Switch(config)# interface range gigabitEthernet 1/0/21-22
Switch(config-if-range)# hsr-ring 1
```

**ステップ9** (任意) 必要に応じて、HSR リングのオプションパラメータを設定します。パラメータの説明、範囲、およびデフォルト値については、「デフォルト設定」セクションを参照してください。

```
Switch(config-range)# hsr 1 supervisionFrameLifeCheckInterval 10000
```

**ステップ10** HSR インターフェイスをオンにします。

```
Switch(config-if-range)# no shutdown
Switch(config-if-range)# end
```

### 例

```
Switch# conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface range gigabitEthernet 1/0/21-22
Switch(config-if-range)# no ptp enable
Switch(config-if-range)# shutdown
Switch(config-if-range)# hsr-ring 1
Switch(config-if-range)# hsr-ring 1 supervisionFrameLifeCheckInterval 10000
Switch(config-if-range)# no shutdown
Switch(config-if-range)# end
```

## 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

**ステップ1** 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するには、**clear hsr node-table** コマンドを入力します。

**ステップ2** VDAN テーブル内のダイナミックエントリをすべてクリアするには、**clear hsr vdan-table** コマンドを入力します。

## 設定の確認

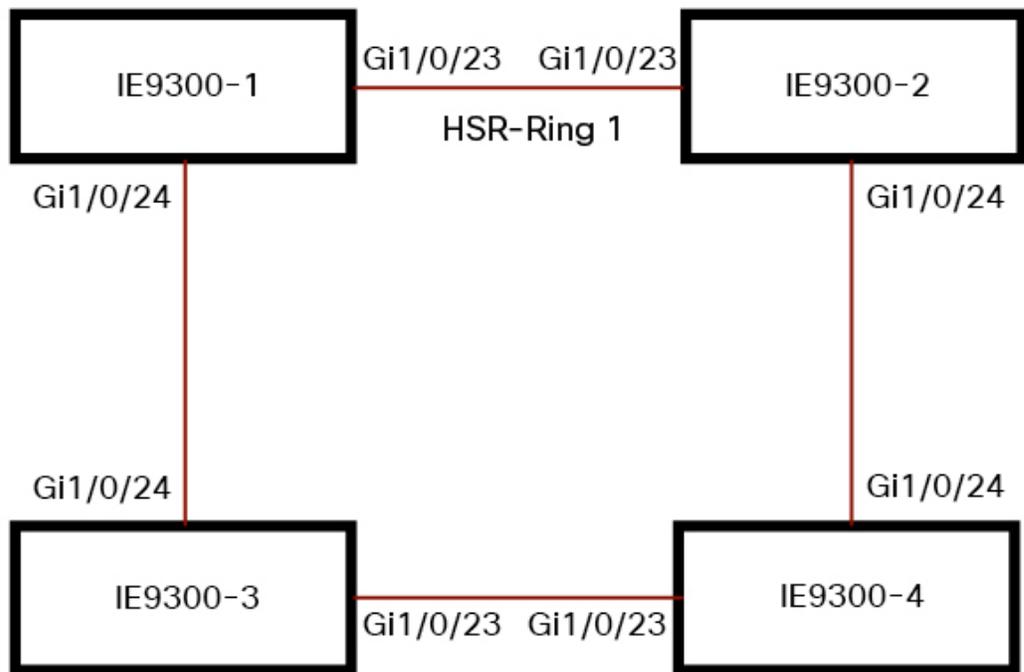
| コマンド                                                                                                                             | 目的                                                                                               |
|----------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------|
| <code>show hsr ring 1 [detail]</code>                                                                                            | 指定された HSR リングの設定の詳細が表示されます。                                                                      |
| <code>show hsr statistics {egressPacketStatistics   ingressPacketStatistics   nodeTableStatistics   pauseFrameStatistics}</code> | HSR コンポーネントの統計情報が表示されます。<br><br>(注)<br>HSR 統計情報をクリアするには、 <b>clear hsr statistics</b> コマンドを入力します。 |
| <code>show hsr node-table</code>                                                                                                 | HSR ノードテーブルが表示されます。                                                                              |
| <code>show hsr vdan-table</code>                                                                                                 | HSR 仮想ダブル接続ノード (VDAN) テーブルが表示されます。<br><br>(注)<br>VDAN テーブルとプロキシノードテーブルは同じです。                     |
| <code>show cdp neighbors</code>                                                                                                  | HSR リングの CDP ネイバー情報が表示されます。                                                                      |
| <code>show lldp neighbors</code>                                                                                                 | HSR リングの LLDP ネイバー情報が表示されます。                                                                     |

## 設定例

### HSR-SAN

次に、4 台のデバイス間で Gi1/0/23 および Gi1/0/24 ポートを使用した HSR リング (リング 1) の設定例を示します。

図 21: 4 台のデバイスを使用した HSR リングの設定



```

IE9300-1# conf t
Enter configuration commands, one per line. End with CNTL/Z.
IE9300-1(config)# interface range gi1/0/23-24
IE9300-1(config-if-range)# shutdown
IE9300-1(config-if-range)# hsr-ring 1
IE9300-1(config-if-range)# no shutdown
IE9300-1(config-if-range)# end
IE9300-1#
IE9300-2# conf t
Enter configuration commands, one per line. End with CNTL/Z.
IE9300-2(config)# interface range gi1/0/23-24
IE9300-2(config-if-range)# shutdown
IE9300-2(config-if-range)# hsr-ring 1
IE9300-2(config-if-range)# no shutdown
IE9300-2(config-if-range)# end
IE9300-2#
IE9300-3# conf t
Enter configuration commands, one per line. End with CNTL/Z.
IE9300-3(config)# interface range gi1/0/23-24
IE9300-3(config-if-range)# shutdown
IE9300-3(config-if-range)# hsr-ring 1
IE9300-3(config-if-range)# no shutdown
IE9300-3(config-if-range)# end
IE9300-3#
IE9300-4# conf t
Enter configuration commands, one per line. End with CNTL/Z.
IE9300-4(config)# interface range gi1/0/23-24
IE9300-4(config-if-range)# shutdown
IE9300-4(config-if-range)# hsr-ring 1
IE9300-4(config-if-range)# no shutdown
IE9300-4(config-if-range)# end

```

```
IE9300-4#
IE9300-1# sh hsr ring 1 detail
HSR-ring: HS1

Layer type = L2
Operation Mode = mode-H
Ports: 2 Maxports = 2
Port state = hsr-ring is Inuse
Protocol = Enabled Redbox Mode = hsr-san
Ports in the ring:
 1) Port: Gi1/0/23
 Logical slot/port = 1/3 Port state = Inuse
 Protocol = Enabled
 2) Port: Gi1/0/24
 Logical slot/port = 1/4 Port state = Inuse
 Protocol = Enabled

Ring Parameters:
Redbox MacAddr: f454.3365.8a84
Node Forget Time: 60000 ms
Node Reboot Interval: 500 ms
Entry Forget Time: 400 ms
Proxy Node Forget Time: 60000 ms
Supervision Frame COS option: 0
Supervision Frame CFI option: 0
Supervision Frame VLAN Tag option: Disabled
Supervision Frame MacDa: 0x00
Supervision Frame VLAN id: 0
Supervision Frame Time: 3 ms
Life Check Interval: 2000 ms
Pause Time: 25 ms

IE9300-2# show hsr ring 1 detail
HSR-ring: HS1

Layer type = L2
Operation Mode = mode-H
Ports: 2 Maxports = 2
Port state = hsr-ring is Inuse
Protocol = Enabled Redbox Mode = hsr-san
Ports in the ring:
 1) Port: Gi1/0/23
 Logical slot/port = 1/3 Port state = Inuse
 Protocol = Enabled
 2) Port: Gi1/0/24
 Logical slot/port = 1/4 Port state = Inuse
 Protocol = Enabled

Ring Parameters:
Redbox MacAddr: 34c0.f958.ee83
Node Forget Time: 60000 ms
Node Reboot Interval: 500 ms
Entry Forget Time: 400 ms
Proxy Node Forget Time: 60000 ms
Supervision Frame COS option: 0
Supervision Frame CFI option: 0
Supervision Frame VLAN Tag option: Disabled
Supervision Frame MacDa: 0x00
Supervision Frame VLAN id: 0
Supervision Frame Time: 3 ms
Life Check Interval: 2000 ms
Pause Time: 25 ms

IE9300-4# sh hsr ring 1 de
```

```

HSR-ring: HS1

Layer type = L2
Operation Mode = mode-H
Ports: 2 Maxports = 2
Port state = hsr-ring is Inuse
Protocol = Enabled Redbox Mode = hsr-san
Ports in the ring:
 1) Port: Gi1/0/23
 Logical slot/port = 1/3 Port state = Inuse
 Protocol = Enabled
 2) Port: Gi1/0/24
 Logical slot/port = 1/4 Port state = Inuse
 Protocol = Enabled

Ring Parameters:
Redbox MacAddr: f454.3312.5104
Node Forget Time: 60000 ms
Node Reboot Interval: 500 ms
Entry Forget Time: 400 ms
Proxy Node Forget Time: 60000 ms
Supervision Frame COS option: 0
Supervision Frame CFI option: 0
Supervision Frame VLAN Tag option: Disabled
Supervision Frame MacDa: 0x00
Supervision Frame VLAN id: 0
Supervision Frame Time: 3 ms
Life Check Interval: 2000 ms
Pause Time: 25 ms

IE9300-3# sh hsr ring 1 detail
HSR-ring: HS1

Layer type = L2
Operation Mode = mode-H
Ports: 2 Maxports = 2
Port state = hsr-ring is Inuse
Protocol = Enabled Redbox Mode = hsr-san
Ports in the ring:
 1) Port: Gi1/0/23
 Logical slot/port = 1/3 Port state = Inuse
 Protocol = Enabled
 2) Port: Gi1/0/24
 Logical slot/port = 1/4 Port state = Inuse
 Protocol = Enabled

Ring Parameters:
Redbox MacAddr: f454.335c.4684
Node Forget Time: 60000 ms
Node Reboot Interval: 500 ms
Entry Forget Time: 400 ms
Proxy Node Forget Time: 60000 ms
Supervision Frame COS option: 0
Supervision Frame CFI option: 0
Supervision Frame VLAN Tag option: Disabled
Supervision Frame MacDa: 0x00
Supervision Frame VLAN id: 0
Supervision Frame Time: 3 ms
Life Check Interval: 2000 ms
Pause Time: 25 ms

```

## 関連資料

- [Cisco Catalyst IE9300 高耐久性シリーズ スイッチのドキュメント](#)。
- IEC 62439-3 『Industrial communication networks - High availability automation networks - Part 3: Parallel Redundancy Protocol (PRP) and High-availability Seamless Redundancy (HSR)』

## 機能の履歴

| 機能名                                            | リリース                 | 機能情報                                       |
|------------------------------------------------|----------------------|--------------------------------------------|
| 高可用性シームレス冗長性 (HSR) - HSR-SAN (シングル RedBox モード) | Cisco IOS XE 17.13.1 | Cisco Catalyst IE9300 高耐久性シリーズ スイッチの初期サポート |



## 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。