Parallel Redundancy Protocol

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。

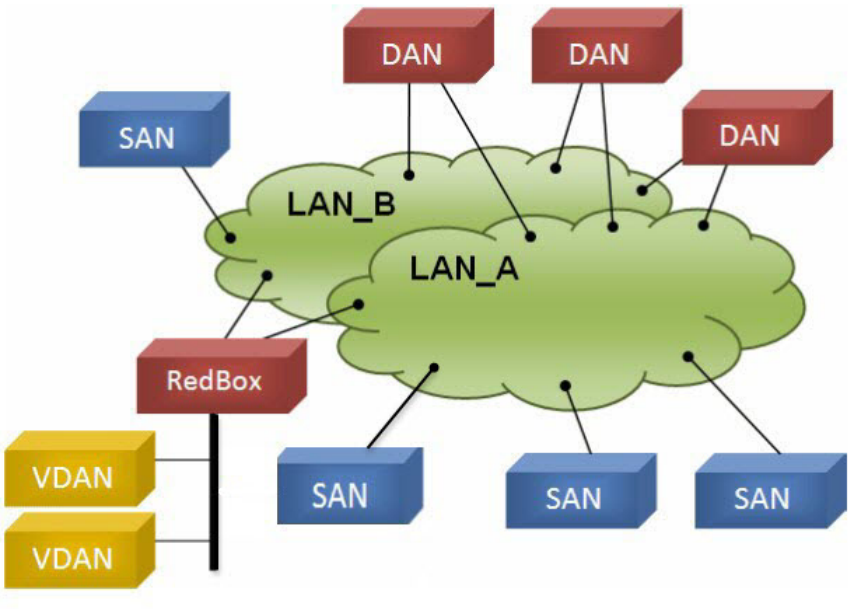
PRP は異なる方式を使用します。この方式では、2 つのネットワーク インターフェイスを 2 つの独立した分離された並列ネットワーク（LAN-A と LAN-B）に接続することで、（ネットワーク要素ではなく）エンドノードが冗長性を実装します。これらのデュアル接続ノード（DAN）のそれぞれには、ネットワーク内の他のすべての DAN への冗長経路があります。

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 チャネル

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

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

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

混合トラフィックと監視フレーム

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

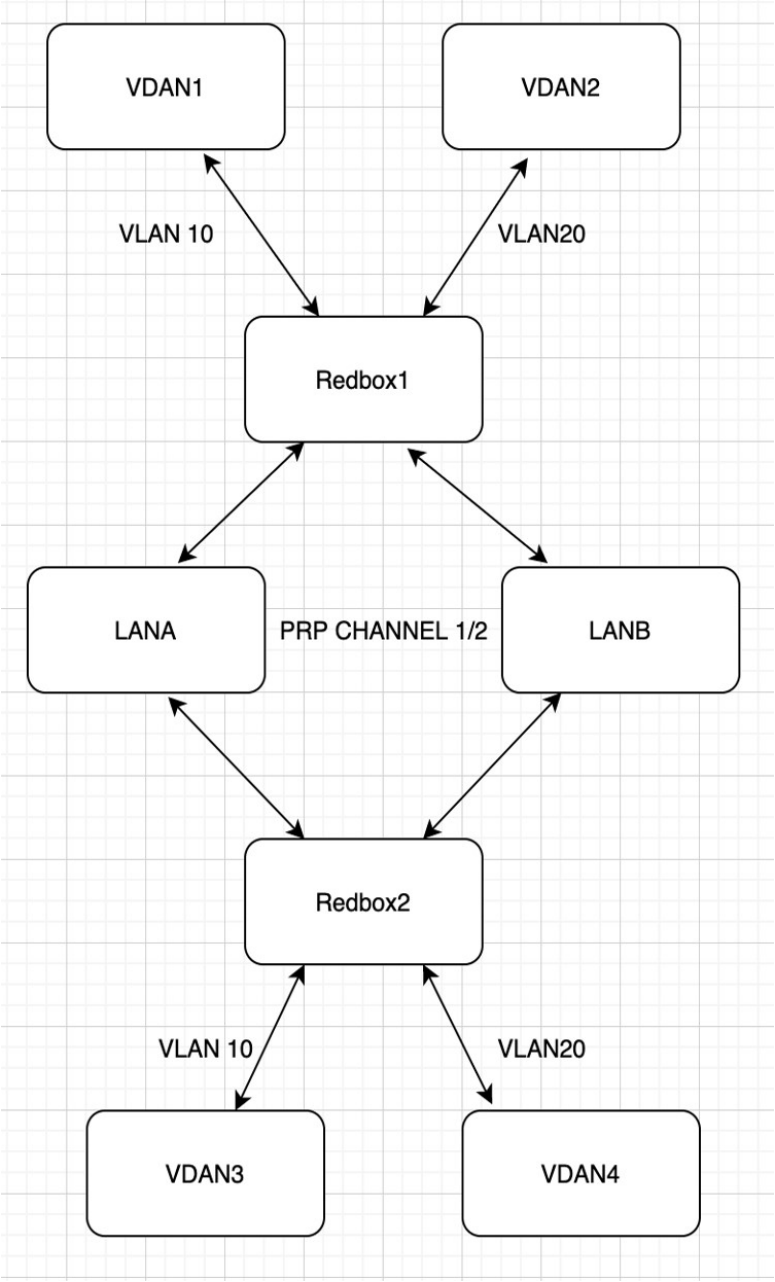
VDAN の接続された RedBox は、これらの VDAN の代理で監視フレームを送信する必要があります。他のすべてのポートに着信し、PRP チャネルポートから送信されるトラフィックの場合、スイッチは、送信元 MAC アドレスを学習して VDAN テーブルに追加し、それらのアドレスに対応する監視フレームの送信を開始します。学習された VDAN エントリにはエージングが適用されます。

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 チャネルの監視フレームで VLAN ID を指定できます。

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



設定の詳細については、監視フレームの VLAN タギングを使用した PRP チャネルの設定 （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:
000200B800030001000400105 1F577DC7E176855650F2F5609418AC60006009C000301002BBB79441FEE97B0E0B339B9036F9C7100000001364C8D
1A000093A8054BC5FA1780A24E23B60A4BFF46AF47A317EE20391BFCA6F0CAABA7F66393F05799A3B0EAB602B54749DCF7225A45FDDB1349A81977D857B9C3
1959A2B54CFC4505CD903D84394E69E5795D31543BB575FB8D51A6FA021FB5E6A0C296F8CA21318377688073516714125D38973D9BF2A66792E3AD1C0A05C3
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使用できる **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、チャネル内に2つのアクティブポートが設定されている必要があります。
- チャネルグループ内の両方のインターフェイスに、同じ設定が必要です。
- レイヤ 3 の場合は、PRP チャネルインターフェイスで IP アドレスを設定する必要があります。

- PRP が有効になっているインターフェイスでは、LLDP と CDP を無効にする必要があります。
- 特にインターフェイスに media-type sfp がある場合は、PRP が有効になっているインターフェイスで UDLD を無効にする必要があります。
- **spanning-tree bpdufilter enable** コマンドは、prp-channel インターフェイスで必須です。スパニングツリー BPDU フィルタは、すべての入出力 BPDU トラフィックを破棄します。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がわかります。

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

```
show prp channel 2 detail

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

ノードテーブルと VDAN テーブル

- スイッチは、ノードテーブルで最大512（SAN+DANP）件のエントリをサポートします。
- 静的ノード/VDAN の最大数は 16 です。

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

デフォルト設定

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

PRP チャネルおよびグループの作成

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

始める前に

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

手順の概要

1. グローバル コンフィギュレーション モードを開始します。
2. PRP チャネルグループにギガビット イーサネット インターフェイスを 2 つ割り当てます。チャネル 1 の場合は、次のように入力します。
3. （任意）レイヤ 2 トラフィックの場合は、**switchport** と入力します。（デフォルト）：
4. （任意）非トランキングでタグのない、単一の VLAN レイヤ 2（アクセス）インターフェイスを設定します。
5. （任意）ギガビット イーサネット インターフェイスの VLAN を作成します。
6. （任意）スイッチで高精度時間プロトコル（PTP）を無効にします。
7. 冗長チャネルのループ検出を無効にします。
8. 冗長チャネルの UDLD を無効にします。

9. サブインターフェイスモードを開始し、PRP チャネルグループを作成します。
10. PRP チャネルを起動します。
11. PRP インターフェイスを指定し、インターフェイスモードを開始します。
12. prp-channel インターフェイスで bpdufilter を設定します。
13. （任意）LAN-A/B ポートを設定して、FORWARD モードにすばやく移行します。

手順の詳細

ステップ 1 グローバル コンフィギュレーション モードを開始します。

configure terminal

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

interface range GigabitEthernet1/1/0/21-22

チャネル 2 の場合は、次のように入力します。

interface range GigabitEthernet21/0/23-24

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

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

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

switchport

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

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

switchport mode access

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

switchport access vlan <*value*>

（注） この手順は、レイヤ 2 トラフィックにのみ必要です。

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

no ptp enable

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

ステップ 7 冗長チャネルのループ検出を無効にします。

no keepalive

ステップ 8 冗長チャネルの UDLD を無効にします。

udld port disable

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

prp-channel-group *prp-channel group*

prp-channel group：1 または 2 の値

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

このコマンドの **no** 形式はサポートされていません。

ステップ 10 PRP チャネルを起動します。

no shutdown

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

interface prp-channel *prp-channel-number*

prp-channel-number：1 または 2 の値

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

spanning-tree bpdufilter enable

スパニングツリー BPDU フィルタは、すべての入力および出力 BPDU トラフィックを破棄します。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チャネルを作成する方法、PRPチャネルグループを作成する方法、そのグループに 2 つのポートを割り当てる方法の例を示します。

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

```
switch(config-if)# exit
switch(config)# interface prp-channel 1
switch(config)# spanning-tree bpdufilter enable
```

```
switch# configure terminal
switch(config)# interface range GigabitEthernet1/0/21-22
switch(config-if)# switchport
switch(config-if)# switchport mode access
switch(config-if)# switchport access vlan 2
switch(config-if)# no ptp enable
switch(config-if)# no keepalive
switch(config-if)# udld port disable
switch(config-if)# prp-channel-group 1
switch(config-if)# no shutdown
switch(config-if)# exit
switch(config)# interface prp-channel 1
switch(config)# spanning-tree bpdufilter enable
```

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

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

監視フレームの VLAN タギングを使用した PRP チャネルの設定

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

始める前に

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

手順の概要

1. グローバル コンフィギュレーション モードを開始します。

2. PRP チャネルグループにギガビット イーサネット インターフェイスを 2 つ割り当てます。チャネル 1 の場合は、次のように入力します。
3. インターフェイスが複数の VLAN のトラフィックを伝送できるように、PRP インターフェイスをトランク管理モードに設定します。
4. トランクインターフェイスの許可 VLAN を設定します。
5. （任意）スイッチで高精度時間プロトコル（PTP）を無効にします。
6. 冗長チャネルのループ検出を無効にします。
7. 冗長チャネルの UDLD を無効にします。
8. サブインターフェイスモードを開始し、PRP チャネルグループを作成します。
9. PRP チャネルを起動します。
10. PRP インターフェイスを指定し、インターフェイスモードを開始します。
11. prp-channel インターフェイスで bpdufilter を設定します。
12. 監視フレームの VLAN タグで使用する VLAN ID を設定します。
13. （任意）監視フレームの VLAN タグに設定するサービスクラス（COS）値を設定します。
14. インターフェイスの VLAN タギングを有効にします。
15. （任意）LAN-A/B ポートを設定して、FORWARD モードにすばやく移行します。

手順の詳細

ステップ 1 グローバル コンフィギュレーション モードを開始します。

configure terminal

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

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

チャネル 2 の場合は、次のように入力します。

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

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

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

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

switchport mode trunk

ステップ 4 トランクインターフェイスの許可 VLAN を設定します。

switchport trunk allowed vlan *value*

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

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

no ptp enable

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

ステップ 6 冗長チャネルのループ検出を無効にします。

no keepalive

ステップ 7 冗長チャネルの UDLD を無効にします。

udld port disable

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

prp-channel-group *prp-channel group*

prp-channel group：1 または 2 の値

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

このコマンドの **no** 形式はサポートされていません。

ステップ 9 PRP チャネルを起動します。

no shutdown

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

interface prp-channel *prp-channel-number*

prp-channel-number：1 または 2 の値

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

spanning-tree bpdufilter enable

スパニングツリー BPDU フィルタは、すべての入出力 BPDU トラフィックを破棄します。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 12 監視フレームの VLAN タグで使用する VLAN ID を設定します。

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

prp-channel-number：1 または 2 の値

value：0 ～ 4095 の VLAN 番号

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

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

value：1 ～ 7 で指定します。デフォルトは 1 です。

ステップ 14 インターフェイスの VLAN タギングを有効にします。

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

prp-channel-number：1 または 2 の値

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

spanning-tree portfast edge trunk

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

例

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

スタティックエントリをノードテーブルと VDAN テーブルに追加

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

手順の概要

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

手順の詳細

ステップ 1 グローバル コンフィギュレーション モードを開始します。

configure terminal

例：

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

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

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

prp-channel group：1 または 2 の値

mac-address：ノードの MAC アドレス

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

ステップ 3 VDAN テーブルに追加する MAC アドレスを指定します。

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

prp-channel group：1 または 2 の値

mac-address：ノードまたは VDAN の MAC アドレス

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

すべてのノードテーブルと VDAN テーブルのダイナミックエントリのクリア

手順の概要

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

手順の詳細

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

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

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

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

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

（注） **clear prp node-table** コマンドと **clear prp vdan-table** コマンドは、ダイナミックエントリのみをクリアします。スタティックエントリをクリアするには、スタティックエントリをノードテーブルとVDAN テーブルに追加 （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 チャネルおよびグループの無効化

手順の概要

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

手順の詳細

ステップ 1 グローバル コンフィギュレーション モードを開始します。

configure terminal

ステップ 2 PRP チャネルを無効にします。

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

prp-channel-number：1 または 2 の値

ステップ 3 インターフェイス モードを終了します。

exit

Syslog のエラーおよび警告メッセージ

エラーと警告が syslog になるように IE-9320-26S2C-A、IE-9320-26S2C-E、IE-9320-22S2C4X-A、および IE-9320-22S2C4X-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

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 （22 ページ）セクションに記載されている PRP エラーと警告から syslog を生成します。

例

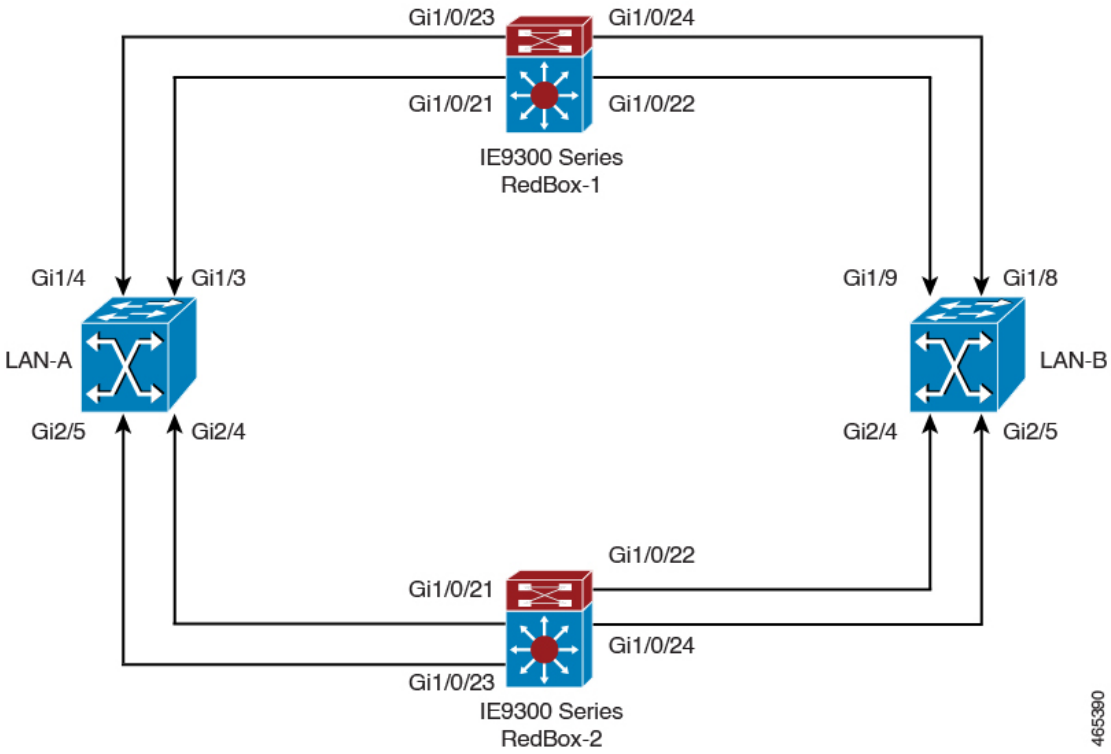
次のテキストは、ロギング間隔を設定した結果の出力例を示しています。

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

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

設定例

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



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

次に、LAN-A の設定を示します。

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

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

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

LAN-B の設定を次に示します。

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

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

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

RedBox-1 の設定は次のとおりです。

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

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

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

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

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

RedBox-2 の設定は次のとおりです。

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

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

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

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

VLAN タギングの例

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

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

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

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

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

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

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

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

PRP_IE9300#
```

設定の確認

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

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

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

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

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

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

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

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

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

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

REDBOX1#
```

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

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

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

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

次に、ロギング間隔を 600 秒に設定するコマンドの例を示します。

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

switch(config)#
```

関連資料

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

機能の履歴

リリース	機能名	機能情報
Cisco IOS XE Dublin 17.12.1	Parallel Redundancy Protocol	この機能は、Cisco Catalyst IE9300 高耐久性シリーズ スイッチ の IE-9320-22S2C4X-A および IE-9320-22S2C4X-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。
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。

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。