4G CUPS の 1:1 ユーザープレーン冗長性

マニュアルの変更履歴

（注） リリース 21.24 よりも前に導入された機能については、詳細な改訂履歴は示していません。

改訂の詳細	リリース
初版	21.24 より前

機能説明

4G CUPS の 1:1 ユーザープレーン冗長性機能は、障害が発生したユーザープレーン（UP）の検出をサポートし、障害が発生した UP の機能をシームレスに処理します。各アクティブ UP には専用のスタンバイ UP があります。1:1 UP 冗長性アーキテクチャは、UP から UP へのシャーシ間セッションリカバリ（ICSR）接続に基づいています。

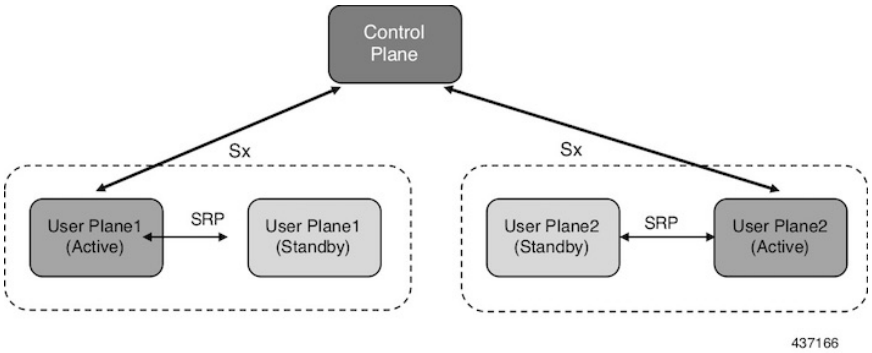
機能の仕組み

ここでは、4G CUPS ユーザープレーンの 1:1 冗長性機能の仕組みについて簡単に説明します。

4G CUPS 展開では、次の図に示すように、ICSR フレームワーク インフラストラクチャを活用して UP ノードのチェックポインティングとスイッチオーバーを実現します。アクティブ UP

は、UP 間でプロビジョニングされたサービス冗長性プロトコル（SRP）リンクを介して専用のスタンバイ UP と通信します。

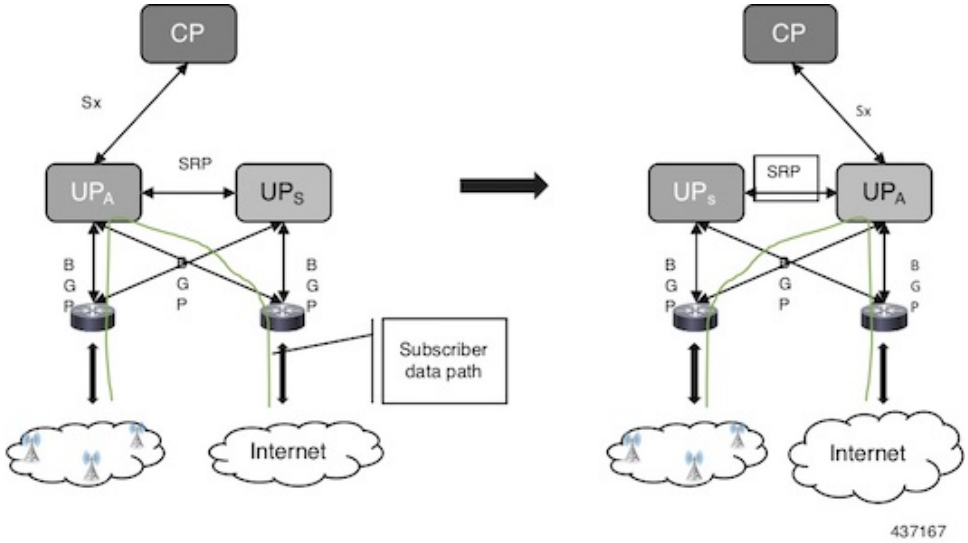
図 *1 : SRP* を使用した *UP* の *1:1* 冗長性



コントロールプレーン（CP）ノードには、UP グループ設定で使用可能なスタンバイ UP 情報がありません。このため、UP の冗長性設定と UP 間のスイッチオーバーイベントは CP には認識されません。

アクティブ UP は、UP で設定された Sx インターフェイスアドレスを介して CP と通信します。スタンバイ UP は、スイッチオーバーイベント中にアクティブに移行する際に、同じ Sx インターフェイスアドレスを引き継ぎます。これは、Sx インターフェイスが SRP によってアクティブ化され、既存の設定方法に準拠していることを意味します。したがって、UP スイッチオーバーは CP に対して透過的です。

図 *2 : UP* の *1:1* 冗長性スイッチオーバー



1:1 の冗長性に完全に準拠するため、CUPS 環境の SRP ベースの ICSR に対する次の依存関係に対応します。

- PFD 設定の同期

- Sx 関連付けチェックポイント
- Sx リンクのモニタリング

上記の依存関係に加えて、UP は UP ノードに固有のデータ収集およびチェックポイント手順を実装します。たとえば、IP プールチャンクのチェックポインティングなどです。UP は、これらの手順を既存の ICSR チェックポインティング フレームワークに統合します。

図 *3 : UP* の *1:1* 冗長性設定時の *CP-CP ICSR*（*CP* スイッチオーバー前）

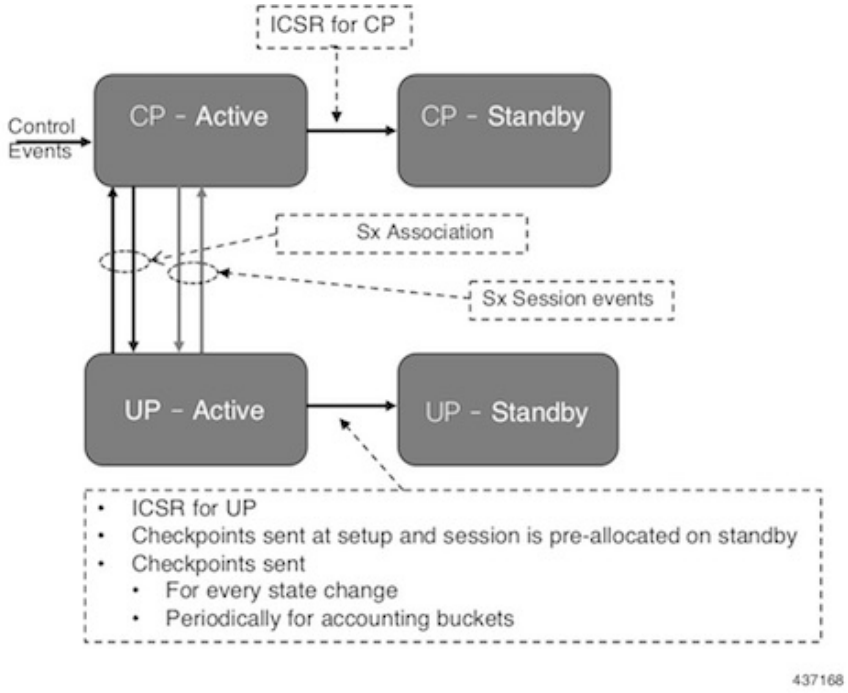
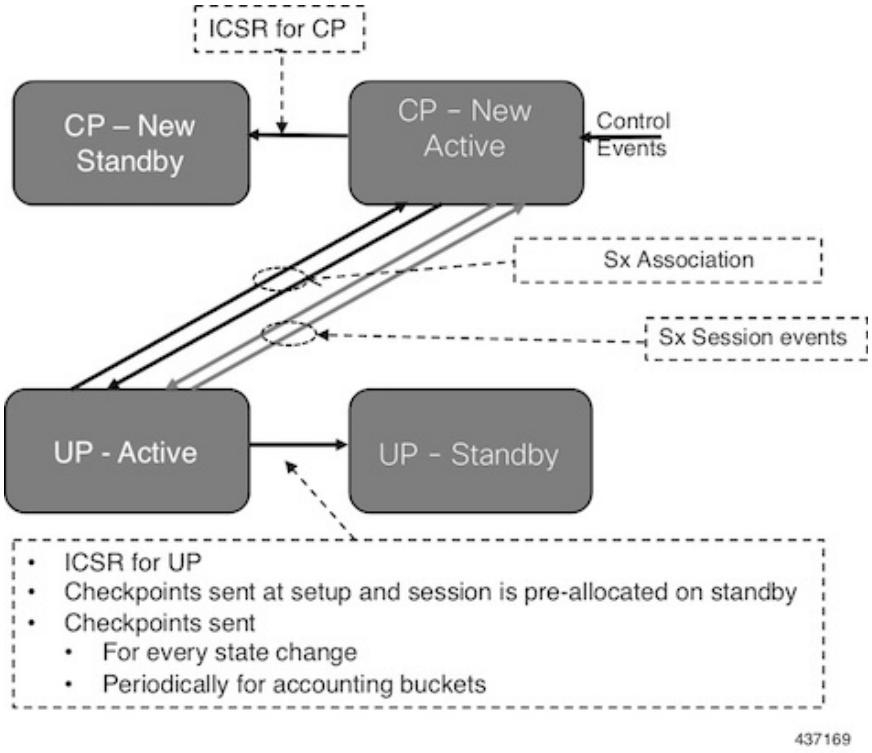


図 *4 : UP* の *1:1* 冗長性設定時の *CP-CP ICSR*（*CP* スイッチオーバー後）

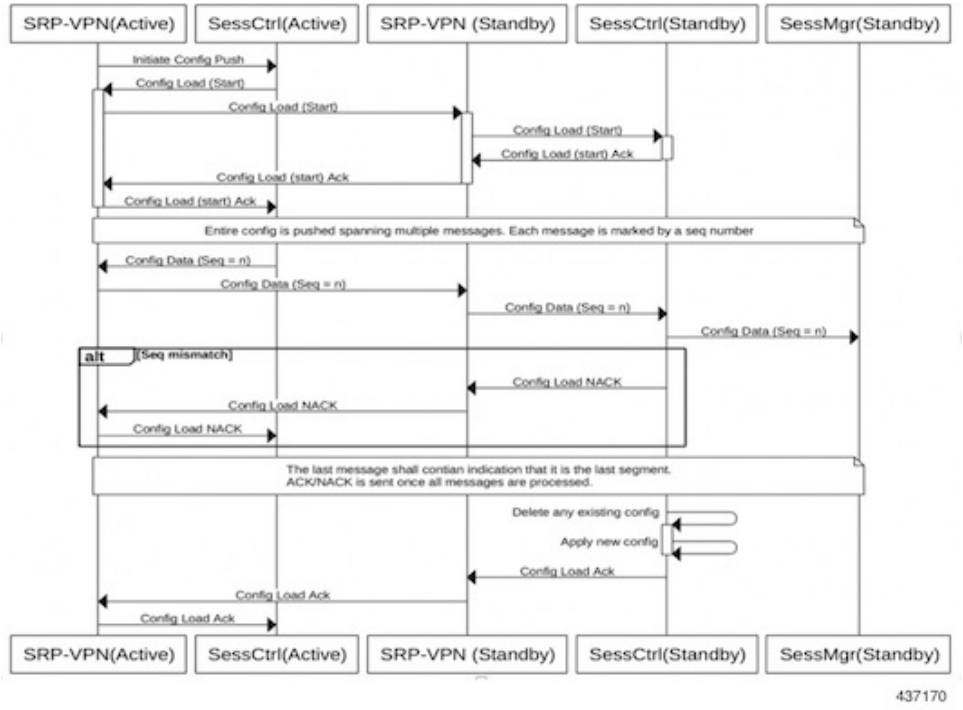


PFD 設定の同期

CP ノードは、パケットフロー記述（PFD）メッセージを介して UP 設定をプッシュします。UP の Sx IP アドレスはアクティブ UP およびスタンバイ UP を介して SRP によってアクティブ化されるため、CP はアクティブ UP からスタンバイ UP に PFD 設定を送信します。

SRP VPN マネージャが UP 間のトランスポートを提供し、アクティブ UP のセッションコントローラが設定のプッシュをアンカーします。次の図にイベントのシーケンスを示します。

図 *5 : PFD* 設定の同期



アクティブ UP とスタンバイ UP 間の BFD モニター

BFD は、アクティブ UP とスタンバイ UP 間の SRP リンクをモニターして、迅速な障害検出とスイッチオーバーを実現します。スタンバイ UP がこのリンクで BFD 障害を検出すると、アクティブ UP を引き継ぎます。

BFD リンクは、シングルホップまたはマルチホップが可能です。

（注） SRP バインドインターフェイスには、カードサービスポートに接続するイーサネットインターフェイスを推奨します。ループバックアドレスでは、BFD 制御パケットが 1 つのサービスポートのみを通過するようにすることを推奨します。ECMP の場合は、ルートコンバージェンス時間が BFD タイムアウトを超えないようにします。

アクティブ UP とスタンバイ UP 間の BFD モニターを設定するには、「アクティブ UP とスタンバイ UP 間の BFD モニタリングの設定」を参照してください。

マルチホップ BFD モニタリングの設定例

プライマリ UP：

```
config
  context srp
    bfd-protocol
      bfd multihop-peer 209.165.200.225 interval 50 min_rx 50 multiplier 20
    #exit
    service-redundancy-protocol
```

```
      monitor bfd context srp 209.165.200.225 chassis-to-chassis
      peer-ip-address 209.165.200.225
      bind address 209.165.200.227
    #exit
    interface srp
      ip address 209.165.200.227 255.255.255.224
    #exit
    ip route static multihop bfd bfd1 209.165.200.227 209.165.200.225
    ip route 192.168.210.0 255.255.255.224 209.165.200.228 srp
  #exit
end
```

バックアップ UP：

```
config
  context srp
    bfd-protocol
      bfd multihop-peer 209.165.200.227 interval 50 min_rx 50 multiplier 20
    #exit
    service-redundancy-protocol
      monitor bfd context srp 209.165.200.227 chassis-to-chassis
      peer-ip-address 209.165.200.227
      bind address 209.165.200.225
    #exit
    interface srp
      ip address 209.165.200.225 255.255.255.224
    #exit
    ip route static multihop bfd bfd1 209.165.200.225 209.165.200.227
    ip route 192.168.209.0 255.255.255.224 209.165.200.226 srp
  #exit
End
```

プライマリ UP とバックアップ UP 間のルータ：

```
config
  context one
    interface one
      ip address 209.165.200.228 255.255.255.224
    #exit
    interface two
      ip address 209.165.200.226 255.255.255.224
    #exit
  #exit
end
```

シングルホップ BFD モニタリングの設定例

プライマリ UP：

```
config
  context srp
    bfd-protocol
    #exit
    service-redundancy-protocol
      monitor bfd context srp 255.255.255.230 chassis-to-chassis
      peer-ip-address 255.255.255.230
      bind address 209.165.200.227
    #exit
    interface srp
      ip address 209.165.200.227 255.255.255.224
      bfd interval 50 min_rx 50 multiplier 10
    #exit
    ip route static bfd srp 255.255.255.230
```

```
  #exit
end
```

バックアップ UP：

```
config
  context srp
    bfd-protocol
    #exit
    service-redundancy-protocol
      monitor bfd context srp 209.165.200.227 chassis-to-chassis
      peer-ip-address 209.165.200.227
      bind address 255.255.255.230
    #exit
    interface srp
      ip address 255.255.255.230 255.255.255.224
      bfd interval 50 min_rx 50 multiplier 10
    #exit
    ip route static bfd srp 209.165.200.227
  #exit
end
```

VPP モニター

VPP サブシステムに障害が発生すると、SRP VPP モニターはスタンバイ UP へのスイッチオーバーを開始します。

（注） VPP モニターは、VPC-SI インスタンス UP でのみ使用できます。ASR 5500 の VPP 障害はカードレベルの冗長性によって対処されるため、VPP モニターは、ハイブリッド CUPS ASR 5500 UP では使用できません。VPP によって複数のカード障害が発生する場合は、SRP カードモニターを使用する必要があります。

VPP モニターを設定するには、「アクティブ UP およびスタンバイ UP での VPP モニターの設定」を参照してください。

Sx 関連付けチェックポイント

アクティブ UP が設定済み CP ノードへの Sx 関連付けを開始すると必ず、スタンバイ UP がこのデータのチェックポイントを生成します。これにより、UP スイッチオーバー後も関連付け情報が保持されます。

Sx ハートビートメッセージが送信され、アクティブ UP は連続した UP スイッチオーバー後であっても応答する必要があります。

Sx モニター

UP と CP 間の Sx インターフェイスのモニタリングは重要です。Sx ハートビート機能を有効にすることは、モニター障害の検出に役立つため不可欠です。

（注） Sx モニタリングは UP でのみ使用できます。

アクティブ UP の Sx インターフェイスは障害を検出し、SRP VPN マネージャに通知して、スタンバイ UP による引き継ぎに向けた UP スイッチオーバーイベントがトリガーされるようにします。

CP Sx ハートビートタイムアウトが、UP Sx ハートビートタイムアウトと UP ICSR スイッチオーバー時間の合計よりも大きくなるようにすることが重要です。これは、UP Sx モニター障害が原因で、UP スイッチオーバー中に CP が Sx パス障害を検出しないようにするためです。

コントロールプレーンのハートビートタイムアウトの防止

UP ICSR スイッチオーバー中に CP ハートビートがタイムアウトする可能性はわずかながらあります。これを軽減するには、次の手順を実行します。

1. CP から UP への Sx ハートビートを削除します。
2. 上記が不可能な場合は、CP から UP への Sx ハートビートに複数の再試行タイムアウトを設けるようにします。また、この再試行回数が UP Sx ハートビートタイムアウトと UP ICSR スイッチオーバー時間の合計よりも大きくなるようにします。

   次に例を示します。

   A = CP ハートビート間隔（*sx-protocol Heartbeat interval*）

   B = CP ハートビートの最大再送信回数（*sx-protocol Heartbeat max-retransmissions*）

   C = CP ハートビート再送信タイムアウト（*sx-protocol Heartbeat retransmission-timeout*）

   D = UP ハートビート間隔（*sx-protocol Heartbeat interval*）

   E = UP ハートビートの最大再送信回数（*sx-protocol Heartbeat max-retransmissions*）

   F = UP ハートビート再送信タイムアウト（*sx-protocol Heartbeat max-retransmissions*）

   G = スイッチオーバー時間（BGP ルートコンバージェンス時間を含む）

   したがって、Sx モニター障害スイッチオーバーを成功させるための式は次のようになります。

   B * C > D + (E * F) + G

   値の例：

   CP：

   A：

   ```
   sx-protocol heartbeat interval 60
   ```

   B：

   ```
   sx-protocol heartbeat max-retransmissions 10
   ```

   C:

   ```
   sx-protocol heartbeat retransmission-timeout 10
   ```

   UP：

   D：

sx-protocol heartbeat interval 30

E：

sx-protocol heartbeat max-retransmissions 3

F：

sx-protocol heartbeat retransmission-timeout 3

BGP：

G：ルートコンバージェンス時間の例 = 30 秒

したがって、B * C > D + (E * F) + G

=> 10 * 10 > 30 + (3 * 3) + 30

=> 100 > 69

B の最大値は 15 で、C の最大値は 20 です。したがって、Sx モニター障害検出と UP スイッチオーバー（D +（E * F）+ G）を設定して、15 * 20 = 300 秒（5 分）の最大遅延に耐えられるようにします。

BGP ルートコンバージェンス時間（G）を最小限に抑えるには、BFD フェールオーバーを使用して BGP を実行します。

Sx モニターを設定するには、「アクティブ UP およびスタンバイ UP での Sx モニタリングの設定」を参照してください。

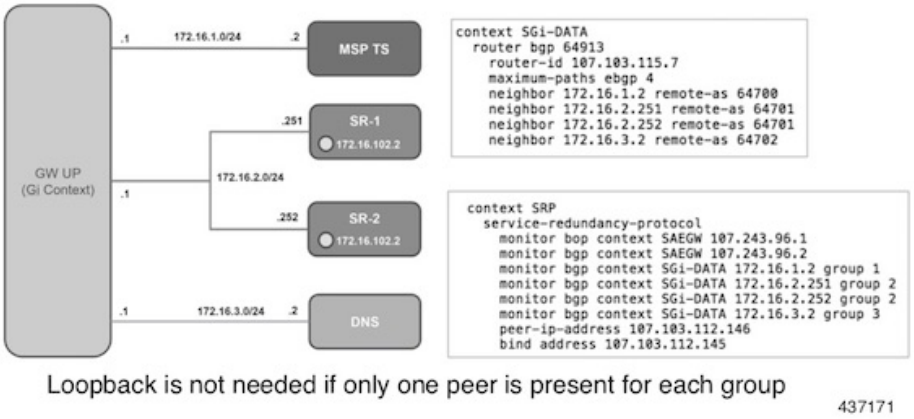
スタンバイ UP 自体に CP との独立した接続はありません。アクティブ UP の Sx コンテキストがスタンバイ UP に複製され、SRP スイッチオーバー時のテイクオーバーの準備が整います。これは、Sx モニター障害のためにアクティブ UP がスタンバイに切り替わった場合、新しいスタンバイは UP から CP へのリンクが機能しているかどうかを把握できないことを意味します。新しいアクティブ UP での Sx モニター障害が原因で、新しいスタンバイ UP が再びアクティブ状態にスイッチバックされないようにするには、新たな **monitor sx** CLI コマンドで **disallow-switchover-on-peer-monitor-fail** キーワードを使用します。

Sx モニタリング障害が原因でシャーシがスタンバイになった後、Sx UP チェックポイントが新しいアクティブ UP から受信されても、Sx 障害ステータスはリセットされません。これは、前回のスイッチオーバーを引き起こしたそもそもの原因が Sx モニター障害であった場合に、Sx モニター障害によって、再び新しいアクティブの計画外のスイッチバックが起こるのを防ぐためです。これにより、CP のダウン時に、連続したピンポン方式のスイッチオーバーが起こるのを防ぎます。Sx モニター障害ステータスは、ネットワーク接続が正常であるという確信が得られたら、オペレータが手動でリセットする必要があります。リセットするには、スタンバイシャーシで新しい **srp reset-sx-fail** CLI コマンド（「Sx モニター障害のリセット」を参照）を使用します。

BGP モニター

次の図に示すように、UP（Gi 側と Gn 側の両方）からネクストホップルータの BGP ピアモニターとピアグループモニターを設定します。これは既存の ICSR 設定です。BGP は、迅速な BGP ピア障害の検出のため、BFD によるサポートと併せて実行できます。

図 *6 : BGP* ピアグループと回送



BGP モニタリングを設定し、BPG モニタリング障害にフラグを設定するには、BGP モニタリング障害のフラグ付け （13 ページ）を参照してください。

UP セッションチェックポイント

アクティブシャーシは、次のシナリオで、UP データのコレクションをチェックポイントとしてピアスタンバイシャーシに送信します。

- 新しいコールのセットアップ時
- コールの状態が変化するたびに
- アカウンティングバケット用に定期的に

これらのチェックポイントを受信すると、スタンバイシャーシはデータに基づいて動作し、コールレベルまたはノード/インスタンスレベルで必要な情報を更新します。

VPN IP プールのチェックポイント

PFD 設定メッセージとともに、CP は IP プール割り当てを各 UP に送信します。VPN マネージャは、UP でこのメッセージを受信し、SRP が設定されている場合、スタンバイ UP で同じ情報を使ってチェックポイントを生成します。

IP プール情報は、SRP VPNMGR の再起動中、および SRP リンクのダウンおよびアップシナリオ中にも送信されます。

スイッチオーバーの前に、スタンバイに IP プール情報が存在することを検証することが重要です。IP プール情報が存在しない場合、ルートアドバタイズメントができないため、トラフィックは UP に到達しません。

外部監査と PFD 設定監査のインタラクション

アクティブ UP は、外部監査と PFD 設定監査のインタラクションを実行します。セッションマネージャが PFD 設定監査の開始通知と完了通知を受け取ります。PFD 設定監査の進行中は、セッションマネージャは外部監査を開始しません。外部監査の進行中に PFD 設定監査の開始

通知が届いた場合、セッションマネージャは PFD 設定監査の完了後に外部監査を再開するようにフラグを立てます。PFD監査の進行中に外部監査が発生しても目的を達成できないため、外部監査の再開が必要です。

ユーザープレーンのゼロアカウンティング損失

アカウンティングデータ/課金情報の損失が 18 秒より小さくなるよう、ゼロアカウンティング損失機能がユーザープレーン（UP）に実装されます。この時間は、アクティブUPからスタンバイ UP へのデフォルトチェックポイント時間、または設定されるアカウンティング チェックポイント時間のデフォルトチェックポイント時間です。

UP でのこの変更は、Gz、Gy、VoGx、および RADIUS URR をサポートするためです。ゼロアカウンティング損失/URR データカウンタ損失では、計画的スイッチオーバーのみがサポートされます。この機能は、現行の ICSR フレームワークや、チェックポイントの生成およびリカバリ方法には影響しません。

Sx 使用状況レポートは、シャーシが [pending active] 状態から [Active] になるまでブロックされます。

UP セッション回復のための早期 PDU リカバリ

早期 PDU リカバリ機能は、これまでのセッションリカバリ機能が抱えていた、リカバリ対象として選択された CRR に優先順位付けが行われないという制限を克服します。これまでは、すべての CRR が AAAMgr から取得され、コールが順番に回復されていました。すべての CRR を取得するのにかかる時間が、セッションリカバリ中に認識される遅延の主な要因でした。障害が発生した際に、セッションマネージャに多数のセッションがあると、遅延が非常に長くなることがありました。また、コールのリカバリに特定の順序がないため、アクティブセッションよりも前にアイドルセッションが回復されることもありました。

（注） 早期 PDU リカバリ機能は、最大 5% のセッションを回復できます。

リカバリ中のセッションの優先順位付け

このリリース以前は、セッションリカバリ機能はリカバリ対象として選択されたセッションに優先順位を付けず、コールリカバリリスト内のすべてのコールをループ処理し、セッションリカバリがトリガーされると順番に回復していました。

リカバリにおけるセッションの優先順位付けの一環として、優先コールのみを対象に別途スキップリストを保持します。該当するレコードがループ処理によらず、AAAMgrからすぐに送信できるようにするためです。その結果、優先コールの迅速なリカバリとデータ停止時間の短縮につながります。

ユーザープレーンには、優先セッションと通常セッションの2種類のセッションがあります。セッションが優先セッションかどうかは、コントロールプレーンから受信したメッセージの優先順位フラグに基づいて判別され、優先セッションがまず回復され、その後に通常のコールが続きます。

これらの優先セッションは、早期 PDU 処理でも優先されます。通常コールの早期 PDU リカバリは、すべての優先セッションのリカバリが完了してはじめて開始されます。

クリティカルフラッシュ（GR）の場合、まず優先セッションのチェックポイントが送信され、その後に通常のコールが送信されます。スイッチオーバー中は、すべてのコール（通常コールと優先コールの両方）のデータが許可されます。

（注） コントロールプレーンがすべてのコールに優先順位フラグを設定します。ユーザープレーンは、コントロールプレーンから受信した優先コールの詳細を、セッションの優先順位付け機能に使用します。

4G CUPS の 1:1 ユーザープレーン冗長性の設定

以下の項では、機能を有効または無効にするために使用できる CLI コマンドについて説明します。

アクティブ UP とスタンバイ UP 間の BFD モニタリングの設定

アクティブ UP およびスタンバイ UP で Bidirectional Forwarding Detection（BFD）のモニタリングを設定するには、次のコマンドを使用します。このコマンドは、SRP コンフィギュレーション モードで設定します。

```
configure
  context context_name
    service-redundancy-protocol
      [ no ] monitor bfd context context_name { ipv4_address | ipv6_address
} { chassis-to-chassis | chassis-to-router }
      exit
```

注：

- **no**：アクティブおよびスタンバイ UP で BFD モニタリングを無効にします。
- **context** *context_name* ：使用するコンテキストを指定します。BFD ピアが設定されているコンテキスト（SRP コンテキスト）を参照します。

  context_name は、1 ～ 79 文字の英数字で表される既存のコンテキストである必要があります。
- *ipv4 _address* | *ipv6_address*：モニターする BFD ネイバーの IP アドレスを定義します。これは、IPv4 ドット付き 10 進表記または IPv6 コロン区切り 16 進表記を使用して入力します。

  設定された BFD（ICSR）ピアの IP アドレスを参照します。
- **chassis-to-chassis** | **chassis-to-router**：

chassis-to-chassis：非 SRP リンク上のプライマリシャーシとバックアップシャーシの間で BFD を実行できるようにします。

chassis-to-router：BFD はシャーシとルータの間で動作します。

⚠

注意　アクティブ UP とスタンバイ UP 間の SRP リンクでは、BFD モニタリングに **chassis-to-router** キーワードを使用しないでください。

- このコマンドは、デフォルトで無効になっています。

BGP モニタリング障害のフラグ付け

単一の BGP ピア（ユーザープレーン）障害時に BGP モニター障害のフラグを設定するには、次のコマンドを使用します。このコマンドは、SRP コンフィギュレーション モードで設定します。

（注）

- このリリースでは、**exclusive-failover** キーワードが既存の **monitor bgp** CLI コマンドに追加され、BGPモニタリング障害にフラグを立てるための代替（新しい）アルゴリズムとして使用されます。
- **monitor bgp** CLI コマンドの詳細については、『Command Reference Guide』の「Service Redundancy Protocol Configuration Mode Commands」の項 [英語] を参照してください。
- **exclusive-failover** キーワードを既存の **monitor bgp** CLI コマンドに追加する前に **monitor bgp** コマンドを実装すると、次のように動作しました。
  - BGP ピアグループ内のいずれかの BGP ピアが稼働している場合、BGP ピアグループは稼働していました。
  - BGPモニターのグループ設定を省略すると、そのモニターがグループ0に含まれていました。
  - BGPグループ0は暗黙的なグループからのコンテキストでモニターされました。各コンテキストは、個別の BGP グループ 0 の暗黙的モニターグループを形成しました。
  - いずれかの BGP ピアグループがダウンしている場合、BGP モニターはダウンしていました。

```
configure
  context context_name
    service-redundancy-protocol
      [ no ] monitor bgp exclusive-failover
      end
```

注：

- **no**：単一の BGP ピア障害時の BGP モニター障害のフラグ設定を無効にします。
- 新しい **exclusive-failover** キーワードを実装すると、動作は次のようになります。
  - BGP ピアグループ内のいずれかの BGP ピアが稼働している場合、BGP ピアグループは稼働します。
  - BGP ピアをグループ 0 に含めることは、非グループ化（グループを省略する）と同じです。
  - いずれかの BGP ピアグループまたは非グループ BGP ピアがダウンすると、BGP モニターはダウンします。
  - モニター対象の BGP ピアを削除すると、BGP モニター障害が発生します。
- このコマンドは、デフォルトで無効になっています。

アクティブ UP とスタンバイ UP での Sx モニタリングの設定

アクティブ UP およびスタンバイ UP で Sx モニタリングを設定するには、次のコマンドを使用します。このコマンドは、[SRP Configuration] モードで設定します。

```
configure
  context context_name
    service-redundancy-protocol
      [ no ] monitor sx [ { context context_name | bind-address
{ipv4_address |ipv6_address } | { peer-address {ipv4_address | ipv6_address } }
 ]
       exit
```

注：

- **no**：アクティブおよびスタンバイ UP で Sx モニタリングを無効にします。
- **context***context_name*：Sx サービスのコンテキストを指定します。

  context_name は、1 ～ 79 文字の英数字で表される既存のコンテキストである必要があります。
- **bind-address {** *ipv4 _address* **|** *ipv6_address***}**：Sx サービスのサービス IP アドレスを定義します。IPv4 ドット付き 10 進表記または IPv6 コロン区切り 16 進表記を使用して入力します。

（注） **bind-address** および **peer-address** の IP アドレスファミリは同じである必要があります。

- **peer-address {** *ipv4 _address* **|** *ipv6_address***}**：Sx ピアの IP アドレスを定義します。IPv4 ドット付き 10 進表記または IPv6 コロン区切り 16 進表記を使用して入力します。
- **disallow-switchover-on-peer-monitor-fail** ：

UP から CP へのリンクの動作ステータスが不明な場合に、UP がアクティブ状態にスイッチバックされるのを防止します。

- 複数の Sx 接続をモニタリングする場合には、この CLI コマンドを複数回実装できます。
- モニター対象の Sx 接続のいずれかがダウンすると、Sx のモニター状態も停止します。
- このコマンドは、デフォルトで無効になっています。

アクティブ UP とスタンバイ UP での SRP over IPSec の設定

IPSec は、IP ネットワーク全体でセキュアなプライベート通信を提供するために相互にデータをやり取りする一連のプロトコルです。これらのプロトコルにより、システムはピアセキュリティ ゲートウェイとセキュアなトンネルを確立して維持できます。IPSec は、IP データグラムに機密性、データの完全性、アクセス制御、およびデータソース認証を提供します。

CUPS アーキテクチャでは IPSec プロトコルを使用して、アクティブ UP とスタンバイ UP 間のシャーシ間セッションリカバリ（ICSR）接続を介して送信されるパケットを暗号化します。この暗号化を実現するために、Service Redundancy Protocol（SRP）ピア間のすべてのトラフィックを照合するアクセスリストが定義され、このリストがクリプトマップに関連付けられます。このクリプトマップは、UP に存在する IPSec ピア間のセキュリティ アソシエーションを確立するために使用されます。

（注） IPSec、その機能、および該当する CLI 設定の詳細については、StarOS の『*IPSec Reference*』[英語] を参照してください。

CLI コマンドを使用して UP で SRP over IPSec を設定する例を以下に示します。

```
context srp
   ip access-list srp-acl
   permit tcp host 209.165.200.225 host 209.165.200.226
   #exit
   ipsec transform-set A-foo
   #exit
   ikev2-ikesa transform-set ikesa-foo
   #exit
   crypto map srp-cm ikev2-ipv4
   match address srp-acl
   authentication local pre-shared-key key local key
   authentication remote pre-shared-key key remote key
   ikev2-ikesa transform-set list ikesa-foo
   payload foo-sa0 match ipv4
   ipsec transform-set list A-foo
   #exit
   peer 209.165.200.227
   #exit
   service-redundancy-protocol
   checkpoint session duration non-ims-session 30
   checkpoint session duration ims-session 30
   route-modifier threshold 18
   delta-route-modifier 2
   audit periodicity 60
   priority 2
```

```
monitor bgp context isp 209.165.200.228
monitor sx context EPC2 bind-address bbbb:abcd::77 peer-address bbbb:abcd::10
peer-ip-address 209.165.200.226
bind address 209.165.200.225
#exit
interface ike-lb loopback
ip address 209.165.200.228 255.255.255.224
crypto-map srp-cm
#exit
interface srp-rtr
ip address 209.165.200.229 255.255.255.224
#exit
interface srp-loopback loopback
ip address 209.165.200.225 255.255.255.224
#exit
ip route 209.165.200.226 255.255.255.224 209.165.200.231 srp-rtr
ip route 209.165.200.227 255.255.255.224 209.165.200.231 srp-rtr
#exit
```

（注） IKEv1：認証ヘッダー（AH）プロトコルを使用したトランスポートモードは推奨されません。ESP では認証と暗号化の両方が実行されるため、Encapsulating Security Payload（ESP）が推奨されます。

アクティブ UP およびスタンバイ UP での VPP モニターの設定

次のコマンドを使用して、VPP がダウンした場合にアクティブ UP で UP スイッチオーバーをトリガーするように Vector Packet Processing（VPP）モニターを設定します。このコマンドは、SRP コンフィギュレーション モードで設定します。

```
configure
  context context_name
    service-redundancy-protocol
      monitor system vpp delay-period 0-300 seconds
      exit

no monitor system vpp
```

注：

- **no**：アクティブおよびスタンバイ UP で VPP モニタリングを無効にします。
- **vpp delay-period***0-300 seconds* ：VPP 障害後のスイッチオーバーの遅延時間を秒単位で指定します。

  遅延時間が 0 より大きい値の場合、VPP に障害が発生すると、指定された遅延時間の後にスイッチオーバーが開始されます。遅延時間内の最後の VPP ステータス通知が、スイッチオーバーアクションの最終トリガーです。デフォルト値は 0 秒で、すぐにスイッチオーバーが開始されます。

  遅延は、VPP が一時的にダウンし、回復が進行中のシナリオに対処するために必要です。これは、スイッチオーバーが不要な場合があることを意味します。

- このコマンドは、デフォルトで無効になっています。

LZ4 圧縮アルゴリズムの設定

必要に応じて、RCM ソリューションの LZ4 圧縮アルゴリズムを有効にすることができます。zlib アルゴリズムはデフォルトのままになります。この設定は、セッション関連のチェックポイントにのみ適用されます。

Zlib アルゴリズムはデータのパッケージングに優れていますが、CPU 使用率が高くなります。それに対して、LZ4 圧縮アルゴリズムは CPU 使用率を抑えますが、データ圧縮率は低くなります。したがって、LZ4 圧縮アルゴリズムが有効になっている場合、UP でのセッションマネージャの CPU 使用率は名目上減少します。ただし、RCM に保存される各チェックポイントのサイズがわずかに増加するため、使用される RCM メモリが多くなります。

LZ4 圧縮アルゴリズムの使用を有効にするには、RCM コンフィギュレーション モードで **checkpoint session compression lz4** CLI コマンドを使用します。**checkpoint session compression zlib** CLI コマンドを使用して、圧縮アルゴリズムを zlib に戻すこともできます。

次のコマンドシーケンスは、LZ4 圧縮の使用を有効にします。

```
configure
  context context_name
    redundancy-configuration-module rcm_name
      checkpoint session compression lz4
      end
```

RCM システムレベルの MOP :

1. UP(F) スイッチオーバーを防ぐには、RCM オペレーションセンターで **rcm pause switchover true** CLI コマンドを使用します。
2. すべての UP で、冗長グループレベル全体の圧縮アルゴリズムを LZ4 に更新します（Day-0.5 設定および実行中の設定）。

   show config context *context_name* または **show config url** *url* CLI コマンドを使用して、**checkpoint session compression lz4** CLI コマンドが有効になっているかどうかを確認します。
3. すべてのチェックポイント マネージャ コンテナを再起動し、すべてのチェックポイントが再同期するのを待つか、RCM 高可用性を実行します。

   次の例を参考にしてください。

   ```
   kubectl -n rcm get pod rcm-checkpointmgr-0 -o yaml | grep -i
   "containerID:  docker
   - containerID:
   docker://3f7e6b10a1be3005424eae148cca2905df8e24e0a549069dfacba533c7b57bf3
   sudo docker restart
   3f7e6b10a1be3005424eae148cca2905df8e24e0a549069dfacba533c7b57bf3
   [sudo] password: 3f7e6b10a1be3005424eae148cca2905df8e24e0a549069dfacba533c7b57bf3
   ```

   RCM 高可用性の場合は、プライマリ RCM オペレーションセンターで **rcm migrate primary** CLI コマンドを実行します。
4. **rcm pause switchover false** CLI コマンドを使用して、**rcm pause switchover** の値を **false** に戻します。

冗長グループレベルの MOP：

1. UP(F) スイッチオーバーを防ぐには、RCM オペレーションセンターで **rcm pause switchover true red-group** *red_group_number* CLI コマンドを使用します。
2. すべての UP で、冗長グループレベル全体の圧縮アルゴリズムを LZ4 に更新します（Day-0.5 設定および実行中の設定）。

   show config context *context_name* または **show config url** *url* CLI コマンドを使用して、**checkpoint session compression lz4** CLI コマンドが有効になっているかどうかを確認します。
3. UP で、RCM インターフェイスを停止してから起動します。

   RCM インターフェイスを停止するための設定例を以下に示します。

```
Configure
  port ethernet 1/10
    vlan 2199
      shutdown
```

4. RCM オペレーションセンターで **rcm pause switchover false red-group** *red_group_number* CLI コマンドを使用して **rcm pause switchover** 値を **false** に戻します。

（注） 同じ MOP に従って、圧縮アルゴリズムを LZ4 から zlib に変更し、キーワード **lz4** を **zlib** に置き換えます。

ユーザー プレーン スイッチバックの防止

次のコマンドを使用して、新しいアクティブ UP での Sx モニター障害が原因で、新しいスタンバイ UP が再びアクティブ状態にスイッチバックされないようにします。このコマンドは、SRP Configuration モードで設定します。

```
configure
  context context_name
    service-redundancy-protocol
      monitor sx disallow-switchover-on-peer-monitor-fail [ timeout
seconds ]
      exit
```

次のいずれかの CLI を使用して、新しいスタンバイ UP からアクティブ状態へのスイッチバックを許可します。

```
no monitor sx disallow-switchover-on-peer-monitor-fail
```

または

```
monitor sx disallow-switchover-on-peer-monitor-fail timeout 0
```

注：

- **no**：スイッチオーバー防止を無効にします。
- **disallow-switchover-on-peer-monitor-fail [timeout** *seconds* **]** ：UP から CP へのリンクの動作ステータスが不明な場合に、UP のアクティブ状態へのスイッチバックを防止します。

  timeout *seconds*：スタンバイピアで Sx 障害ステータスがリセットされない場合でも、このタイムアウトの経過後にスイッチバックを許可します。有効な値の範囲は 0 ～ 2073600（24 日）です。

（注） タイムアウトを「0」秒に指定すると、計画外のスイッチオーバーが可能になります。

  timeout キーワードが指定されていない場合、アクティブシャーシはスタンバイピアで Sx 障害ステータスがリセットされるまで無期限に待機します。

- デフォルト設定では、あらゆる条件において、Sx モニター障害による計画外のスイッチオーバーが許可されます。

（注） 手動による計画的スイッチオーバーは、この CLI が設定されているかどうかに関係なく許可されます。

デュアル アクティブ エラー シナリオの防止

CP で次の CLI 設定を使用して、UP 1:1 冗長性のデュアル アクティブ エラー シナリオを回避します。

```
configure
    user-plane-group group_name
       sx-reassociation disabled
       end
```

注：

- **sx-reassociation disabled**：CP との関連付けがすでに存在する場合、UP Sx の再関連付けを無効にします。

Sx モニター障害のリセット

サービス冗長性プロトコル（SRP）の Sx モニター障害情報をリセットするための次のコマンドは、スタンバイシャーシでのみ使用できます。このコマンドは、EXEC モードで設定します。

```
srp reset-sx-fail
```

モニタリングおよびトラブルシューティング

この項では、機能のモニタリングとトラブルシューティングのサポートに使用できるCLIコマンドに関する情報を提供します。

コマンドや出力の表示

この項では、この機能のサポートにおけるshowコマンドまたはその出力について説明します。

show srp monitor bfd

この CLI コマンドの出力には、4G CUPS 1:1 UP 冗長性機能に関する次のフィールドが含まれています。

- タイプ
- 状態
- GroupId
- IP Addr
- Port
- Context（VRF Name）
- Last Update

show srp monitor bgp

この CLI コマンドの出力には、4G CUPS 1:1 UP 冗長性機能に関する次のフィールドが含まれています。

- タイプ
- 状態
- GroupId
- IP Addr
- ポート
- Context (VRF Name)
- Last Update

show srp monitor sx

この CLI コマンドの出力には、4G CUPS 1:1 UP 冗長性機能に関する次のフィールドが含まれています。

- タイプ
- 状態
- GroupId
- IP Addr
- ポート
- Context（VRF Name）
- Last Update

show srp monitor vpp

この CLI コマンドの出力には、4G CUPS 1:1 UP 冗長性機能に関する次のフィールドが含まれています。

- タイプ
- 状態
- GroupId
- IP Addr
- ポート
- コンテキスト（VRF 名）
- Last Update

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。