シャーシ間セッションリカバリ

この章では、シャーシ間セッションリカバリ（ICSR）を設定する方法について説明します。製品アドミニストレーションガイドには、システム上での基本サービスの設定例と手順が示されています。以下で説明する手順を実行する前に、それぞれの製品管理ガイドの説明に従って、サービスモデルに最適な設定例を選択し、そのモデルに必要な要素を設定する必要があります。

VPC-SI のコンテキストでは、シャーシはハイパーバイザ内で VPC-SI を実行するように設定されたサーバーです。ICSR は、同様に設定された別のサーバーで実行されている VPC-SI インスタンスに対してフェールオーバー保護を提供します。

重要 ICSR は、別個のライセンスを必要とするライセンス供与されたシスコの機能です。特定のライセンス要件の詳細については、シスコのアカウント担当者にお問い合わせください。ライセンスのインストールと確認の詳細については、「ソフトウェア管理操作」の「ライセンスキーの管理」の項を参照してください。

この章では、次の項目について説明します。

概要

ICSR 機能は、サブスクライバのサービスを中断することなく、継続的なコール処理を可能にする最も高い可用性を提供します。ICSR により、オペレータは冗長性を確保するために地理的に離れたゲートウェイを設定することができます。ノードまたはゲートウェイで障害が発生した場合、ICSR はその障害を迂回してセッションを透過的にルーティングできるため、ユーザーエクスペリエンスが維持されます。ICSR では、セッション情報と状態も維持されます。

ICSR は冗長シャーシを使用して実装されます。シャーシはプライマリとバックアップとして設定されます。1つはアクティブで、もう1つはスタンバイです。両方のシャーシが同じAAAサーバーに接続されています。チェックポイントの期間タイマーは、アクティブシャーシからスタンバイシャーシにサブスクライバデータが送信されるタイミングを制御します。コールトラフィックを処理しているアクティブシャーシがアウトオブサービスになると、スタンバイシャーシはアクティブ状態に移行し、サブスクライバセッションを中断せずにコールトラフィックの処理を続行します。

シャーシは、サービス冗長性プロトコル（SRP）リンクと呼ばれる独自のTCPベースの接続を介して、どちらがアクティブであるかを判別します。SRP リンクは、プライマリシャーシとバックアップシャーシの間で Hello メッセージを交換するために使用され、適切なシステム運用のために維持する必要があります。

ICSR ライセンスは、次のサービスに対して現在サポートされています。

- eHRPD：Evolved High-Rate Packet Data
- ePDG：Evolved Packet Data Gateway
- GGSN：ゲートウェイ GPRS サポートノード
- HA：ホームエージェント
- P-GW：Packet Data Network Gateway
- PDSN：パケット データ サービング ノード
- S-GW：サービングゲートウェイ
- SAEGW：System Architecture Evolution ゲートウェイ
- SaMOG ：S2a Mobility over GTP

ICSRのL2TPアクセスコンセントレータ（LAC）機能は、次のプロトコルおよびサービスでサポートされています。

- eGTP：拡張 GPRS トンネリングプロトコル
- GGSN：ゲートウェイ GPRS サポートノード
- P-GW：Packet Data Network Gateway
- SAEGW：System Architecture Evolution ゲートウェイ

ICSRのL2TPアクセスコンセントレータ（LAC）機能は、次のサービスでサポートされていません。

- HA：ホームエージェント
- PMIP：プロキシモバイル IP

ICSRのL2TPネットワークサーバー（LNS）機能は、どのサービスでもサポートされていません。

重要 LAC の ICSR サポートには、個別の LAC のライセンスとシャーシ間セッションリカバリのライセンスが必要です。

重要 特定のサービスが ICSR をオプションとしてサポートしているかどうかを確認するには、シスコのアカウント担当者にお問い合わせください。

ICSR 機能は、サブスクライバのサービスを中断することなく、継続的なコール処理を可能にする最も高い可用性を提供します。ICSR により、オペレータは冗長性を確保するためにゲートウェイを設定することができます。ゲートウェイで障害が発生した場合、ICSR はその障害を迂回してセッションを透過的にルーティングできるため、ユーザーエクスペリエンスが維持されます。ICSR では、セッション情報と状態も維持されます。

システムは、同じ StarOS リリースで ICSR をサポートする 2 つのインスタンス間で ICSR をサポートしています。複数のサービスタイプが使用されている VM の組み合わせでは、ICSR をサポートするサービスのみが ICSR を使用できます。

ICSR は、サイト/行/ラック/ホストの停止や主要なソフトウェア障害に冗長性を提供できます。重複しないホストとネットワークインターコネクト上で 2 つのインスタンスを実行する必要があります。ICSR は、同じように設定されている VPC-DI インスタンスまたは VPC-SI インスタンスの間でのみサポートされます。

ASR 5500VPC-SIL2 と L3 の両方の ICSR をサポートします。

ICSR は冗長仮想シャーシを使用して実装されます。各 ASR 5500VPC-SI インスタンスの仮想シャーシは、プライマリとバックアップとして設定されます。1 つはアクティブで、もう 1 つはスタンバイです。両方の仮想シャーシが同じ AAA サーバーに接続されています。チェックポイントの期間タイマーは、アクティブシャーシからスタンバイシャーシにサブスクライバデータが送信されるタイミングを制御します。コールトラフィックを処理しているアクティブシャーシがアウトオブサービスになると、スタンバイシャーシはアクティブ状態に移行し、サブスクライバセッションを中断せずにコールトラフィックの処理を続行します。

仮想シャーシは、サービス冗長性プロトコル（SRP）リンクと呼ばれる独自の TCP ベースの接続を介して、どちらがアクティブであるかを判別します。SRP リンクは、プライマリシャーシとバックアップシャーシのアクティブな CF 間で Hello メッセージを交換するために使用され、適切なシステム運用のために維持する必要があります。詳細については、「セッションリカバリ」の章を参照してください。

ICSR ライセンスは、次のサービスに対して現在サポートされています。

- GGSN ゲートウェイ GPRS サポートノード
- P-GW Packet Data Network Gateway
- S-GW サービングゲートウェイ
- SAE-GW System Architecture Evolution ゲートウェイ

ICSR の L2TP アクセスコンセントレータ（LAC）機能は、次のプロトコルおよびサービスでサポートされています。

- eGTP 拡張 GPRS トンネリングプロトコル
- GGSN ゲートウェイ GPRS サポートノード

- P-GW Packet Data Network Gateway
- SAEGW System Architecture Evolution ゲートウェイ

ICSR の L2TP アクセスコンセントレータ（LAC）機能は、次のサービスでサポートされていません。

- PMIP プロキシモバイル IP

ICSR の L2TP ネットワークサーバー（LNS）機能は、どのサービスでもサポートされていません。

（注） LAC の ICSR サポートには、個別の LAC のライセンスとシャーシ間セッションリカバリのライセンスが必要です。

（注） 特定のサービスが ICSR をオプションとしてサポートしているかどうかを確認するには、シスコのアカウント担当者にお問い合わせください。

シャーシ間の通信

ICSR をサポートするように設定されたシャーシは、定期的に Hello メッセージを使用して通信します。これらのメッセージは、各シャーシによって、現在の状態をピアに通知するために送信されます。Hello メッセージには、設定や優先順位などのシャーシに関する情報が含まれています。dead 間隔は、シャーシのピアから受信される Hello メッセージの時間制限を設定するために使用されます。スタンバイシャーシが dead 間隔の間にアクティブシャーシから Hello メッセージを受信しない場合、スタンバイシャーシはアクティブ状態に移行します。

SRP リンクがアウトオブサービスになる状況では、どのシャーシがセッションを処理するかを決定するために優先順位スキームが使用されます。次の優先順位スキームが使用されます。

- route modifier
- chassis priority
- MIO/UMIO MAC address

チェックポイントメッセージ

チェックポイントメッセージは、アクティブシャーシからスタンバイシャーシに送信されます。これらのメッセージは特定の間隔で送信され、そのシャーシがアクティブになった場合にスタンバイシャーシ上のセッションを再作成するために必要なすべての情報が含まれます。セッションがチェックポイント期間を超えると、そのセッションでチェックポイントデータが収集されます。

詳細については、付録の「*ICSR* のチェックポインティング」を参照してください。

SRP CLI コマンド

Exec モード CLI コマンド

Exec モードの **srp** CLI 設定コマンドを使用して、SRP 機能を有効または無効にしたり、開始することができます。次の表に、これらのコマンドの一覧と簡単な説明を示します。詳細については、『*Command Line Interface Reference*』の「*Exec Mode Commands (D-S)*」の章を参照してください。

表 *1 : srp CLI* コマンド

コマンド	説明
srp disable nack micro-chkpt-cmd	アクティブシャーシから完全なチェックポイントをトリガーす可能性があるスタンバイシャーシからのNACKメッセージの送を無効にします。完全なチェックポイントを送信すると、SRP帯域幅が増加します。このコマンドは、継続的に障害が発生しいる特定のマイクロチェックポイントのNACK機能を無効にします。
srp initiate-audit manual-with-sync	ICSR シャーシ間の強制監査を開始します。この監査により、2のICSR ピアが同期され、スケジュール済みまたは予定外のスイチオーバーイベントの前に不一致が識別されます。
srp initiate-switchover	アクティブから非アクティブへの強制スイッチオーバーを実行ます。このコマンドをアクティブシャーシで実行した場合、アティブシャーシを非アクティブ状態、非アクティブシャーシをクティブ状態に切り替えます。 下記の注を参照してください。
srp reset-auth-probe-fail	認証プローブモニターの障害情報を 0 にリセットします。
srp reset-diameter-fail	Diameter モニターの障害情報を 0 にリセットします。
srp terminate-post-process	スイッチオーバー後の処理を強制的に終了します。
srp validate-configuration	アクティブシャーシの設定を検証します。
srp validate-switchover	予定済みの SRP スイッチオーバーの準備がアクティブシャーシスタンバイシャーシの両方で整っていることを検証します。

重要 ICSR は手動スイッチオーバーを許可する前に、両方のシャーシでセッションマネージャの接続を確認します。アクティブシャーシ内の1つ以上のセッションマネージャがスタンバイシャーシに接続されていない場合は、スイッチオーバーは開始されません。セッションマネージャの数が一致していないことを通知するメッセージが画面に表示されます。**force** キーワードを使用すると、不一致があってもスイッチオーバーを開始できます。**show checkpoint statistics verbose** コマンドの出力では、ピアシャーシに接続されていないインスタンスについては「peer conn」列の セッション マネージャ インスタンス（「smgr inst」）に「Ready」が示されません。

show コマンド

Exec モードの **show srp** コマンドは、SRP 機能に関連するさまざまな情報を表示します。次の表に、これらのコマンドの一覧と簡単な説明を示します。これらのコマンドの詳細については、『*Command Line Interface Reference*』の「*Exec Mode show Commands*（*Q* ～ *S*）」の章を参照してください。

表 *2 : show srp* コマンド

コマンド	説明
show srp audit-statistics	外部監査の統計情報を表示します。
show srp call-loss statistics	スイッチオーバー中に失われたコールの履歴を表示します。
show srp checkpoint statistics	セッションの冗長性データ（セッションマネージャ、現在のコールリカバリレコードなど）の統計情報のチェックポイントを表示します。
show srp info	サービス冗長プロトコル情報（コンテキスト、シャーシの状態、ピア、接続状態など）を表示します。
show srp monitor	SRP モニター情報を表示します。
show srp statistics	SRP 統計情報（送信された hello メッセージ、設定の検証、リソースメッセージ、スイッチオーバーなど）を表示します。

show srp コマンドの出力の詳細については、*Statistics and Counters Reference* を参照してください。

AAA モニター

AAA サーバーは、認証プローブメカニズムを使用してモニターされます。認証プローブが有効な応答を受信した場合、AAA サーバーは稼働していると見なされます。AAA サーバーの設定で指定された **max-retries count** に達した場合、AAA サーバーは停止していると見なされます。設定済みの AAA サーバーのいずれも認証プローブに応答しない場合、SRP はスイッチオーバーを開始します。AAA プローブは、アクティブシャーシでのみ実行されます。

重要 AAA モニタリング障害によるスイッチオーバーのイベントは、非リバーティブです。

新しくアクティブになったシャーシが設定済みの AAA サーバーのモニターに失敗した場合、次のいずれかが発生するまでアクティブシャーシのままになります。

- 手動スイッチオーバー。
- 別の非 AAA 障害イベントによって、システムがスイッチオーバーする。
- CLI コマンドを使用して AAA 障害フラグをクリアし、シャーシをスタンバイに切り替えられるようにする。

BGP の連携動作

サービス冗長プロトコルは、アドバタイズされたループバック/IP プールルートのルート修飾子値を調整するメカニズムを介して、復元可能なスイッチオーバー動作を実装します。ルート修飾子値の初期値は、設定されたシャーシのロールによって決定され、通常の動作値よりも大きい値に初期化されます。これにより、SRP リンク障害や SRP タスク障害が発生した場合でも、ルーティングドメイン内では適切なシャーシが優先されるようになります。

重要 ICSR では、SRP 検証の失敗を回避するために、アクティブシャーシとスタンバイシャーシで **busyout ip pool** コマンドを同じ順序で設定する必要があります。

アクティブシャーシとスタンバイシャーシは、現在のルート修飾子値を共有します。BGP は、ループバックルートと IP プールルートをアドバタイズするときに、ルート修飾子を自律システム（AS）パスのプリペンドカウントに変換します。アクティブシャーシは常により小さいルート修飾子を持つため、AS パス属性の前により小さい値が付加されます。これにより、ルーティングドメイン内ではこのルートが優先されます。

SRP リンク上の通信が失われ、冗長ペアのシャーシが両方ともアクティブであると主張している場合、以前にアクティブだったシャーシが引き続き優先されます。これは、より小さい AS パスを BGP ルーティングドメインにアドバタイズしているためです。スイッチオーバーイベントが発生すると、ルート修飾子が増分されます。ロールオーバーを回避するために、ルート修飾子を初期値にリセットするタイミングはしきい値によって決まります。

要 件

ICSR の設定には、次のものが必要です。

- 同じサービスタイプに対して同じように設定された VPC-SI インスタンス。サービスは、SRP によってアクティブ化されたループバック インターフェイスでバインドされている必要があります。両方のインスタンスが同一のハードウェアを備えている必要があります。

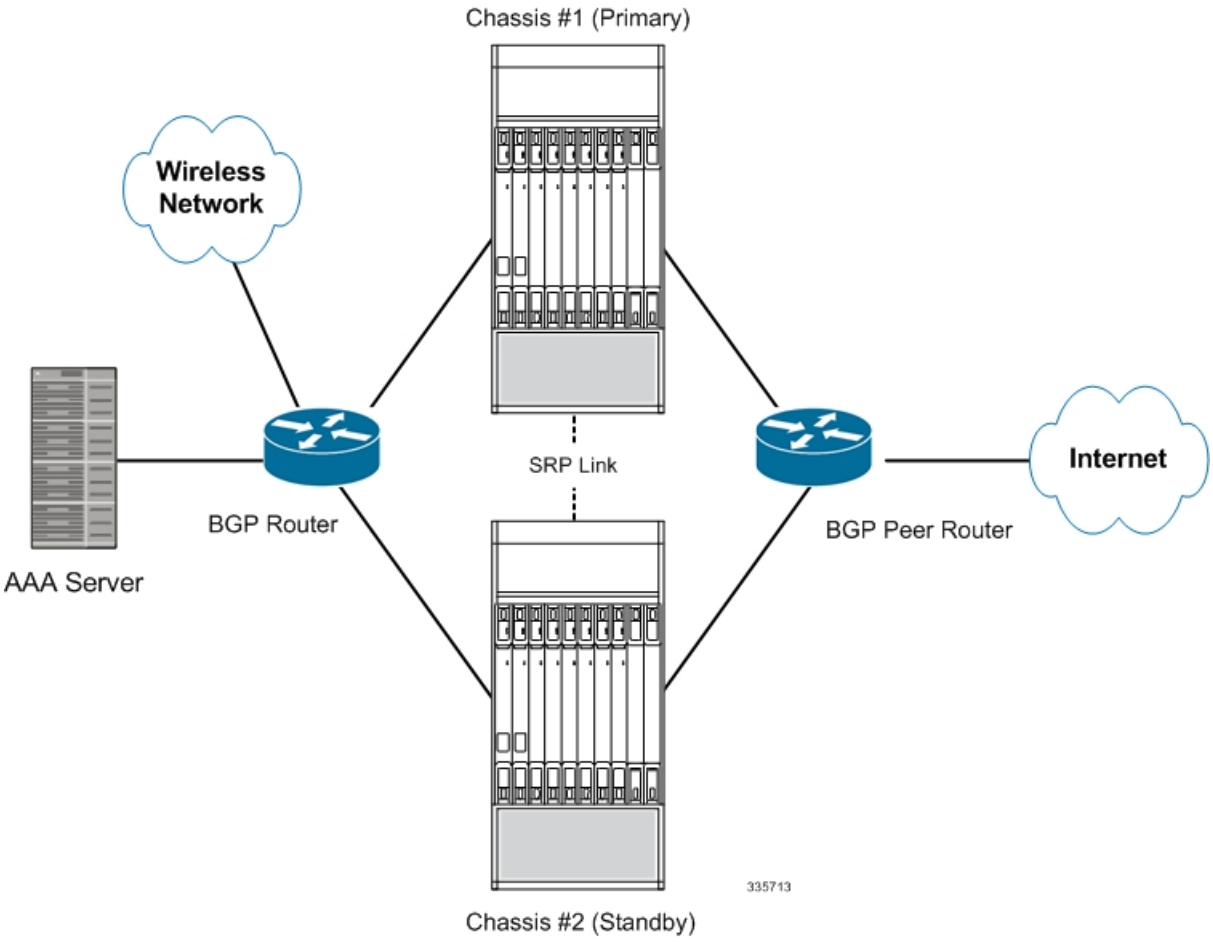
- 同じサービスタイプ用に設定された 2 つのシャーシ。サービスは、SRP によってアクティブ化されたループバック インターフェイスでバインドされている必要があります。
- 両方のシャーシが同一のハードウェアを備えている必要があります。
- 3 つのコンテキスト：
  - **冗長性**：プライマリシャーシとバックアップシャーシの冗長性を設定します。
  - **送信元**：指定された nas-ip-address の AAA 設定は、HA にバインドされたインターフェイスの IP アドレスであるか、または同じコンテキスト内で設定されたコアネットワークサービスである必要があります。
  - **接続先**：PDN へのモニタリングとルーティングを設定します。
- ボーダー ゲートウェイ プロトコル（BGP）：ICSR はルート修飾子を使用してシャーシの優先順位を決定します。
- 自律システム（AS）番号が同じ場合、SRP でアクティブ化されたルートはスタンバイシャーシで自動的に除外されます。それ以外の場合、SRP でアクティブ化されたルートは、ICSR シャーシに接続しているルータでフィルタ処理されるポリシーまたはルートマップによってフィルタ処理されます。
- L3 ICSR は、AS 番号が同じ場合に機能する AS-Path 属性によってデュアルアクティブシナリオを処理します。
- StarOS はスタンバイのアドバタイズ機能もサポートしています。この機能では、AS-Path 属性がスタンバイシャーシのアドバタイズプールを処理します。

重要 ICSR は、ライセンス供与されたシスコの機能です。これらの手順を使用する前に、各シャーシに適切なライセンスがあることを確認します。これを行うには、両方のシャーシにログインし、**show license information** コマンドを実行します。「シャーシ間セッションリカバリ」を探します。シャーシにライセンスがない場合は、シスコのアカウント担当者にお問い合わせください。

スイッチオーバーをトリガーするために、RADIUS プロトコルおよび Diameter のプロトコルをモニターできます。

次の図は、ICSR のネットワークを示しています。

図 *1 : ASR 5500* の *ICSR* のネットワーク

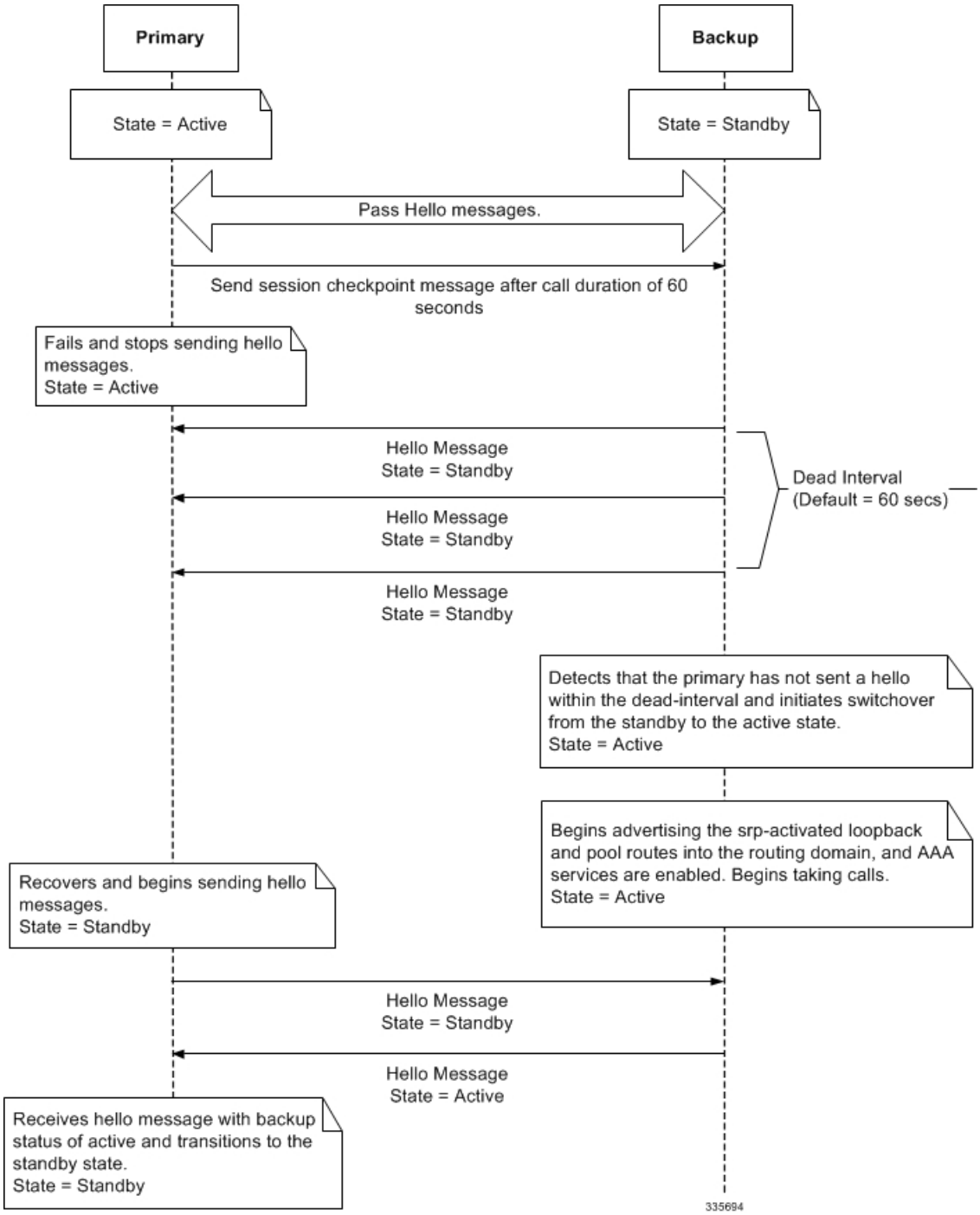


ICSR の運用

このセクションには、ICSR の運用フローが表示されます。

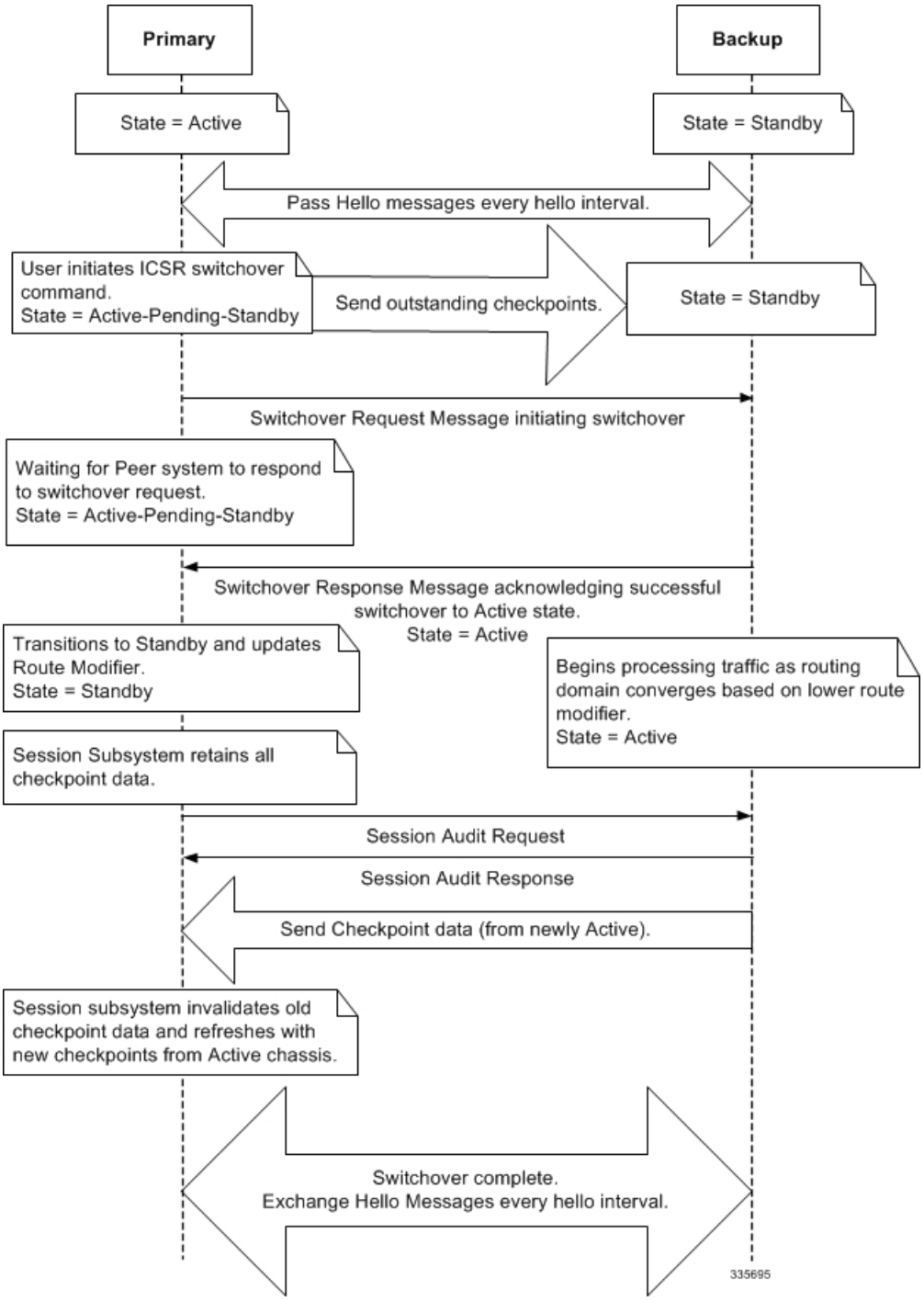
次の図は、プライマリ障害による ICSR プロセスフローを示しています。

図 *2 : ICSR* プロセスフロー（プライマリ障害）



次の図は、手動スイッチオーバーによる ICSR プロセスフローを示しています。

図 *3 : ICSR* プロセスフロー（手動スイッチオーバー）



シャーシの初期化

シャーシが同時に初期化されると、設定されたピアに Hello メッセージが送信されます。ピアは応答を送信し、シャーシ間の通信を確立し、設定情報を含むメッセージを送信します。

初期化中に、両方のシャーシが同じモードで誤設定されている場合（両方ともアクティブ（プライマリ）または両方ともスタンバイ（バックアップ））、最も高い優先順位を持つシャーシ（ICSR の **priority** コマンドで設定した最も小さい数字）がアクティブになり、もう一方のシャーシはスタンバイになります。

シャーシの優先順位が同じ場合は、システムが 2 つの MAC アドレスを比較し、より高い MIO/UMIO MAC アドレスを持つシャーシがアクティブになります。たとえば、シャーシの MAC アドレスが *00-02-43-03-1C-2B* と *00-02-43-03-01-3B* の場合、最後の 3 つのオクテットセット（最初の 3 つのセットはベンダーコード）が比較されます。この例では、*03-1C-2B* と *03-01-3B* が左から右に比較されます。両方の MAC アドレス内の最初のオクテットのペアが同じであるため、次のペアが比較されます。*01* は *1C* よりも低いため、MIO/UMIO の MAC アドレス *00-02-43-03-1C-2B* を持つシャーシがアクティブになり、もう一方のシャーシはスタンバイになります。

StarOS が各 VPC-SI 仮想シャーシ上で同時に初期化されると、シャーシは設定されたピアに Hello メッセージを送信します。ピアは応答を送信し、シャーシ間の通信を確立し、設定情報を含むメッセージを送信します。

初期化中に、両方の仮想シャーシが同じモードで誤設定されている場合（両方ともアクティブ（プライマリ）または両方ともスタンバイ（バックアップ））、最も高い優先順位を持つシャーシ（ICSR の **priority** コマンドで設定した最も小さい数字）がアクティブになり、もう一方のシャーシはスタンバイになります。

シャーシの優先順位が同じ場合は、StarOS がアクティブ 2 つの MAC アドレスを比較し、高い MAC アドレスを持つシャーシがアクティブになります。たとえば、VPC-SI インスタンスの MAC アドレスが *00-02-43-03-1C-2B* と *00-02-43-03-01-3B* の場合、最後の 3 つのオクテットセット（最初の 3 つのセットはベンダーコード）が比較されます。この例では、*03-1C-2B* と *03-01-3B* が左から右に比較されます。両方の MAC アドレス内の最初のオクテットのペアが同じであるため、次のペアが比較されます。*01* は *1C* よりも低いため、MAC アドレス *00-02-43-03-1C-2B* を持つ VPC-SI 仮想シャーシがアクティブになり、もう一方のシャーシはスタンバイになります。

シャーシの動作

この項では、シャーシがどのように通信し、サブスクライバセッションを維持し、シャーシのスイッチオーバーを実行するかについて説明します。

シャーシ通信

1 つのシャーシがアクティブ状態で、もう 1 つのシャーシがスタンバイ状態の場合は、両方の hello インターバルで Hello メッセージが送信されます。チェックポイントのセッション期間を超えるサブスクライバセッションは、スタンバイシャーシに送信されるチェックポイントメッセージに含まれます。チェックポイントメッセージにはサブスクライバセッション情報が含ま

れているため、アクティブなシャーシがアウトオブサービスになると、バックアップシャーシがアクティブになり、サブスクライバセッションの処理を続行できるようになります。スタンバイシャーシでサブスクライバセッション情報が更新されるたびに、追加のチェックポイントメッセージがさまざまな間隔で発生します。

SRP 構成モードの**checkpoint session** コマンドには、次のことを可能にする多数のキーワードが含まれています。

- SRP ペイロードメッセージに使用する圧縮アルゴリズムのタイプを設定します。
- 既存のコールセッションを指していることを確認するまでに、シャーシが待機する時間を設定します。チェックポイントは、IMS や非 IMS セッション用に個別に設定できます。
- アクティブシャーシとスタンバイシャーシ間のマクロチェックポイント（完全なチェックポイント）の送信間隔を設定します。

詳細については、『*Command Line Interface Reference*』の「*Service Redundancy Protocol Configuration Mode Commands*」の章を参照してください。

シャーシスイッチオーバー

アクティブシャーシがサービスを提供できなくなった場合、スタンバイシャーシは Hello メッセージを送信し続けます。スタンバイシャーシが dead 間隔内に Hello メッセージへの応答を受信しない場合、スタンバイシャーシがスイッチオーバーを開始します。スイッチオーバー中に、スタンバイシャーシは SRP によってアクティブ化されたループバックとルーティングドメインへのプールルートのアドバタイズを開始します。シャーシがアクティブになると、既存の AAA サービスと、チェックポイント情報を備えていたサブスクライバセッションの処理は続行されますが、新しいサブスクライバセッションを確立することもできます。

プライマリシャーシが復帰すると、設定されているピアに Hello メッセージを送信します。ピアは応答を送信し、シャーシ間の通信を確立し、設定情報を含む Hello メッセージを送信します。プライマリシャーシはバックアップシャーシの状態がアクティブであることを示す Hello メッセージを受信した後、スタンバイに移行します。Hello メッセージの送信は各ピアに対して継続され、チェックポイント情報がアクティブなシャーシからスタンバイシャーシに定期的に送信されるようになります。

シャーシのスイッチオーバーが発生すると、セッションタイマーが回復します。セッションの潜在的な損失の可能性と、更新が過渡的なチェックポイント更新プロセス時に損失する可能性を回避するため、アクセスゲートウェイのセッションリカバリはフルライフタイムで再作成されます。

ICSR の設定

重要 ICSR の設定は、プライマリシャーシとバックアップシャーシで同じである必要があります。各シャーシに異なるサービス冗長性プロトコル（SRP）の設定がある場合、セッションリカバリ機能は機能せず、アクティブシャーシがアウトオブサービスになったときにセッションをリカバリできません。

この項では、各シャーシ上の基本的な ICSR の設定方法を説明します。追加のパラメータとオプションを設定するコマンドについては、『*Command Line Interface Reference*』を参照してください。

次に説明する手順は、下記のものを前提としています。

- シャーシは、コアネットワークサービスを使用してインストールおよび設定されている。

  サービスの設定に関する詳細情報と手順については、それぞれの製品のアドミニストレーション ガイドを参照。

- さらに、IP アドレスプールは **SRP によってアクティブ化**されている必要がある。
- AAA サーバーがインストールされ、設定されており、両方のシャーシでアクセス可能であること。

  AAA サーバーの設定の詳細については、『*AAA Interface Administration and Reference*』を参照。

- BGP ルータがインストールされ、設定されていること。BGP サービスの設定の詳細については、「ルーティング」を参照。

プライマリシャーシやバックアップシャーシに ICSR を設定するには、次のようにします。

手順

ステップ 1 サービス冗長性プロトコル（SRP）コンテキストの設定 （16 ページ）の設定例を適用して、SRP コンテキストを設定します。

ステップ 2 ICSR の送信元コンテキストの変更 （27 ページ）の設定例を適用して、コアネットワークサービスの送信元コンテキストを変更します。

ステップ 3 ICSR の接続先コンテキストの変更 （29 ページ）の設定例を適用して、コアネットワークサービスの接続先コンテキストを変更します。

ステップ 4 オプション：スタンバイシステムでのバルク統計情報収集の無効化 （30 ページ）の設定例を適用して、スタンバイシステムでバルク統計情報収集を無効にします。

ステップ 5 プライマリ設定とバックアップ設定の確認 （30ページ）の説明に従って、プライマリシャーシおよびバックアップシャーシの設定を確認します。

ステップ 6 「設定の確認と保存」の説明に従って、設定を保存します。

SRP チェックポイントの設定

SRP チェックポイントの設定

シャーシ間セッションリカバリ（ICSR）の設定では、アクティブシャーシとスタンバイシャーシの両方で一部の設定が同一である必要があります。Service Redundancy Protocol（SRP）チェックポイントまたはチェックサムは、アクティブシャーシとスタンバイシャーシの設定を検証します。それらが同一であれば、その設定は適切です。設定が同一でない場合、エラーが発生する可能性があります。SRP チェックポイントをサポートするために、BGP ルータ設定の下に VRF 設定が追加されています。

SRP チェックポイントを設定するには、次の設定を使用します。

```
configure
  context context_name
    service-redundancy-protocol
      [ no ] monitor bgp vrf-srp-validate
      end
```

注：

- **vrf-srp-validate**：BGP VRF 設定の SRP 検証を有効にします。
- **no**：BGP VRF 設定の SRP 検証を無効にします。

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、この機能をサポートするために show コマンドを使用して監視およびトラブルシューティングする方法について説明します。

show コマンドと出力

この項では、この機能の show コマンドとそれらの出力に関する情報を示します。

show configuration srp

このコマンドの出力が強化され、次のフィールドが表示されるようになりました。

表 *3 : show configuration srp* コマンド出力の説明

フィールド	説明
vrf-srp-validate	BGP VRF 設定の SRP 検証が有効になっていることを示します。
srp-validate access-list	SRP チェックポイント検証の IP および IPv6 アクセスリスト設定が有効になっていることを示します。

サービス冗長性プロトコル（SRP）コンテキストの設定

ICSR と連携するようにシステムを設定するには、次のようにします。

手順

ステップ 1 SRP コンテキストの作成とバインド （16 ページ）の設定例を適用して、シャーシ冗長性コンテキストを作成し、プライマリシャーシの IP アドレスにバインドします。VPC-DI インスタンスの場合、これはプライマリ VPC-DI インスタンス内のアクティブな CF の IP アドレスとなります。

ステップ 2 SRP コンテキストパラメータの設定 （17 ページ）の設定例を適用し、優先順位、シャーシモード、hello 間隔、dead 間隔、およびピア IP アドレスを使用してシャーシ冗長性コンテキストを設定します。

ステップ 3 SRP コンテキストのインターフェイス パラメータの設定 （24 ページ）の設定例を適用し、シャーシ間通信のインターフェイスパラメータ（インターフェイス名、IP アドレス、およびポート番号を含む）を使用して SRP コンテキストを設定します。

ステップ 4 SRP 設定の確認 （27 ページ）の説明に従って、SRP コンテキストの設定を確認します。

ステップ 5 「設定の確認と保存」の説明に従って、設定を保存します。

SRP コンテキストの作成とバインド

次の例を使用して SRP コンテキストを作成し、プライマリシャーシの IP アドレスにバインドします。

重要 ICSR は 2 つのシャーシ上に設定されます。両方のシステム上で冗長性コンテキストを必ず作成してください。CLI コマンドは両方のシステムで実行する必要があります。続行する前に、両方のシャーシにログインします。常に、プライマリシャーシで設定の変更を最初に行います。この設定を開始する前に、プライマリとして設定するシャーシを特定し、そのログインセッションを使用します。

重要 ICSR は 2 つの VPC-DI インスタンス上に設定されます。両方のシステム上で冗長性コンテキストを必ず作成してください。CLI コマンドは両方のシステムで実行する必要があります。続行する前に、両方のアクティブ CF にログインします。常に、プライマリ VPC-DI インスタンスのアクティブ CF で設定の変更を最初に行います。この設定を開始する前に、プライマリとして設定する VPC-DI を特定し、そのログインセッションを使用します。

```
configure
  context srp_ctxt_name [-noconfirm]
    service-redundancy-protocol
      bind address ip_address
      end
```

注：

- ICSR は個別のコンテキストで設定および維持する必要があります。
- 必ず、ローカル IP アドレスをプライマリシャーシにバインドしてください。バックアップシャーシを設定するときは、必ずローカル IP アドレスをバックアップシャーシにバインドしてください。

SRP コンテキストパラメータの設定

重要 CLI コマンドは、両方のシャーシで実行する必要があります。続行する前に、両方のシャーシにログインします。常に、プライマリシャーシで設定の変更を最初に行います。

CLI コマンドは、両方の VPC インスタンスで実行する必要があります。続行する前に、両方のアクティブ CF にログインします。最初にプライマリ VPC インスタンスで設定の変更を行います。

基本パラメータ

この設定では、シャーシモードと優先順位が割り当てられ、プライマリシャーシとバックアップシャーシ間の冗長性リンクも設定されます。

```
configure
  context srp_ctxt_name
    service-redundancy-protocol
      chassis-mode { primary | backup }
      priority priority
      peer-ip-address ip_address
      hello-interval dur_sec
      dead-interval dead_dur_sec
      end
```

注：

- ICSR は個別のコンテキストで設定および維持する必要があります。
- バックアップシャーシにシャーシモードを割り当てる場合は、**backup** キーワードを必ず入力します。
- **checkpoint** コマンドは、シャーシが既存のコールセッションを指していることを確認するまでに待機する時間を設定します。チェックポイントは、IMS（VoLTE）や非 IMS セッションに設定できます。チェックポイントは、障害が発生した場合に実行を再開するために使用できる現在のアプリケーションの状態のスナップショットです。デフォルトの設定は 60 秒です。
- この**優先順位**によって、両方のシャーシが同じシャーシモードで誤って設定されている場合に、どのシャーシがアクティブになるかが決定されます（シャーシの初期化 （12 ページ）を参照）。優先順位の高いシャーシの方が小さい番号になります。各シャーシに異なる優先順位を割り当てるようにしてください。

- バックアップシャーシの IP シャーシを **peer-ip-address** として、プライマリシャーシに入力します。プライマリシャーシの IP アドレスを **peer-ip-address** として、バックアップシャーシに割り当てます。
- **dead 間隔** は、**hello 間隔** の 3 倍以上にする必要があります。たとえば、hello 間隔が 10 の場合、dead 間隔は 30 以上にする必要があります。Hello 間隔とデッド間隔が適切に設定されていない場合、システムパフォーマンスに重大な影響が及びます。オプションの **delay-interval** コマンドを使用すると、構成ファイルのロード後のある一定の時間間隔にわたって、デッド間隔の開始を遅延させることができます。

SRP 冗長性、AAA ガートタイマー、Diameter ガードタイマー

ガードタイマーを使用すると、再起動やタスクの再起動といったローカルの障害が発生しても、ICSR イベントが中断することはありません。

guard timer コマンドは、SRP サービスのモニタリングのための edundancy-guard-period と monitor-damping-period を設定します。

```
configure
  context context_name
    service-redundancy-protocol variable
      guard-timer { aaa-switchover-timers { damping-period seconds |
guard-period seconds } | diameter-switchover-timers { damping-period
seconds | guard-period seconds } | srp-redundancy-timers { aaa  {
damping-period seconds | guard-period seconds } | bgp { damping-period
seconds | guard-period seconds } | diam  { damping-period seconds |
guard-period seconds } }
      end
```

注：

- **aaa-switchover-timers**：ネットワークのコンバージ中に AAA の障害（post ICSR switchover）が発生した場合に、バックツーバックの ICSR スイッチオーバーを防止するタイマーを設定します。
  - **damping-period**：guard-period 内のモニタリング障害による ICSR スイッチオーバーをトリガーする遅延時間を設定します。
  - **guard-period**：local-failure-recovery と network-convergence のタイマーを設定します。
- **diameter-switchover-timers**：ネットワークのコンバージ中に Diameter の障害（post ICSR switchover）が発生した場合に、バックツーバックの ICSR スイッチオーバーを防止するタイマーを設定します。
  - **damping-period**：guard-period 内のモニタリング障害による ICSR スイッチオーバーをトリガーする遅延時間を設定します。
  - **guard-period**：local-failure-recovery と network-convergence のタイマーを設定します。
- **srp-redundancy-timer**：システムがローカルの card-reboot/critical-task-restart の障害からリカバリされている間に、ICSR スイッチオーバーを防止するタイマーを設定します。

- **aaa**：ローカル障害に続いて AAA のモニタリングの障害が発生する。
- **bgp**：ローカル障害に続いて BGP のモニタリングの障害が発生する。
- **diam**：ローカル障害に続いて Diameter のモニタリングの障害が発生する。

SRP メッセージの DSCP マーキング

SRP 制御およびチェックポイントメッセージの個別の DSCP マーキングを有効にすることができます。**dscp-marking** コマンドは、SRP 制御およびチェックポイント（セッションメンテナンス）メッセージの DSCP マーキング値を設定します。

```
configure
  context context_name
    service-redundancy-protocol
      dscp-marking { control | session } dscp_value
```

注：

- *dscp_value* は次のようになります。
  - **af11**：Assured Forwarding Class 1 Low（ホップごとの動作）
  - **af12**：Assured Forwarding Class 1 Medium ドロップ PHB
  - **af13**：Assured Forwarding Class 1 High ドロップ PHB
  - **af21**：Assured Forwarding Class 2 Low ドロップ PHB
  - **af22**：Assured Forwarding Class 2 Medium ドロップ PHB
  - **af23**：Assured Forwarding Class 2 High ドロップ PHB
  - **af31**：Assured Forwarding Class 3 Low ドロップ PHB
  - **af32**：Assured Forwarding Class 3 Medium ドロップ PHB
  - **af33**：Assured Forwarding Class 3 High ドロップ PHB
  - **af41**：Assured Forwarding Class 4 Low ドロップ PHB
  - **af42**：Assured Forwarding Class 4 Medium ドロップ PHB
  - **af43**：Assured Forwarding Class 4 High ドロップ PHB
  - **be**：ホップ単位のベストエフォート型動作（デフォルト）
  - **cs1**：クラスセレクタ 1 PHB
  - **cs2**：クラスセレクタ 2 PHB
  - **cs3**：クラスセレクタ 3 PHB
  - **cs4**：クラスセレクタ 4 PHB
  - **cs5**：クラスセレクタ 5 PHB
  - **cs6**：クラスセレクタ 6 PHB
  - **cs7**：クラスセレクタ 7 PHB
  - **ef**：低遅延トラフィック用の Expedited Forwarding（EF; 完全優先転送）

スイッチオーバー移行の最適化

複数の SRP 設定オプションがあります。これにより、VoLTE トラフィックのサポートにおいて、アクティブゲートウェイからスタンバイゲートウェイ（主に P-GW）への移行時間が短縮されます。

重要 これらの機能には、機能拡張をサポートするために、更新された ICSR ライセンスが必要です。詳細については、シスコのアカウント担当者にお問い合わせください。

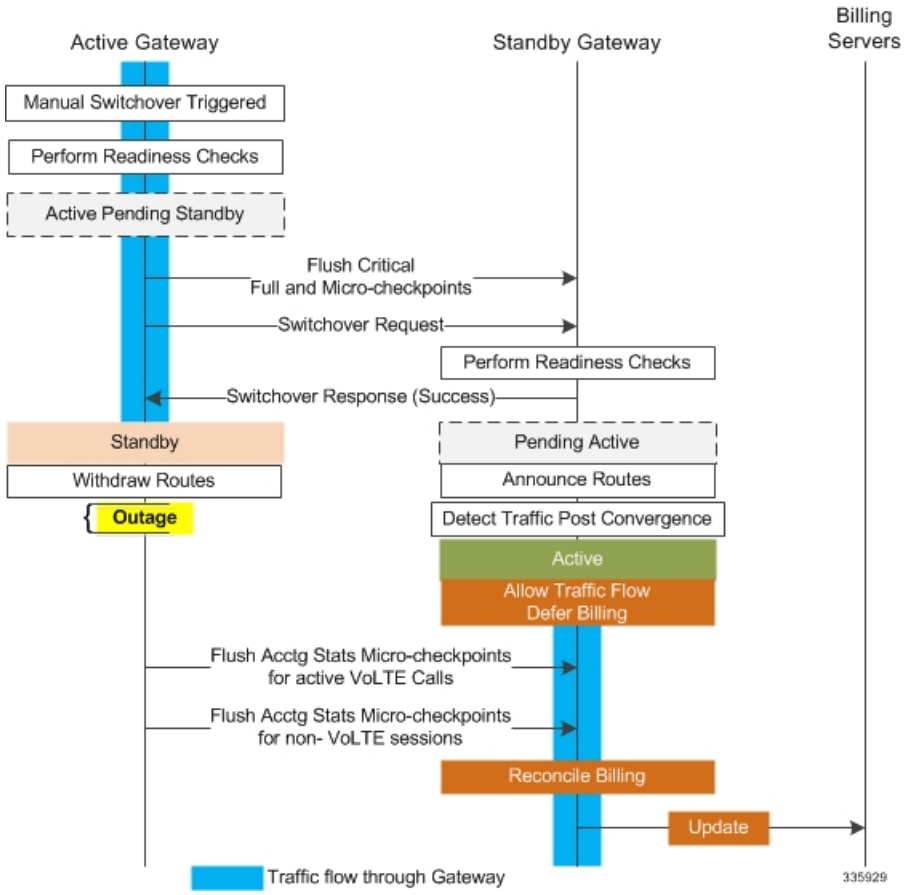
ICSR スイッチオーバー時の非 VoLTE トラフィックの許可

ICSR フレームワークは、課金情報を調整する前に、新しくアクティブになったゲートウェイ上で VoLTE トラフィックを有効にし、アカウンティングが重要ではないと判断された場合に新しくアクティブになったゲートウェイとの通信を有効にすることで、VoLTE トラフィックのスイッチオーバーの中断を軽減します。

この機能は、データセッションや IMS/e911 のデフォルトのベアラートラフィックなど、他のすべてのトラフィックに拡張され、すべての非 VoLTE データトラフィックに対して次の ICSR 機能が提供されます。

- スイッチオーバーが発生すると、新しくアクティブになったゲートウェイは、ゲートウェイがアクティブになった時点ですべてのトラフィックを転送します。
- 課金サーバーとの外部通信は保留されています。次のトラフィックフロー図参照してください。
- 新しくアクティブになったゲートウェイは、以前のアクティブなゲートウェイから課金関連のチェックポインティング情報をすべて受信すると、外部課金サーバー OCS（オンライン課金システム）または OFCS（オフライン課金システム）と通信する前に課金データを調整します。

図 *4 :* コールフロー：非 *VoLTE* データ停止の削減



SRP 構成モードの **switchover allow-all-data-traffic** CLI コマンドを使用すると、スイッチオーバーの移行中にすべてのデータトラフィック（VoLTE および非 VoLTE）が許可されます。このコマンドは、P-GW で有効になっている場合、**switchover allow-volte-data-traffic** コマンドを上書きします。

```
configure
  context context_name
    service-redundancy-protocol
      switchover allow-all-data-traffic
```

重要 この機能を有効にするには、**switchover allow-all-data-traffic** コマンドを両方のシャーシで実行する必要があります。

SRP 構成モードの **switchover allow-volte-data-traffic** CLI コマンドは、ICSR スイッチオーバーの移行中に VoLTE データトラフィックを許可します。

```
configure
  context context_name
```

```
service-redundancy-protocol
  switchover allow-volte-data-traffic [ maintain-accounting ]
```

注：

- **maintain-accounting** が有効になっている場合、VoLTE コールのアカウンティング精度が維持されます。VoLTE アカウンティングの統計情報がフラッシュされた後、アクティブなゲートウェイで VoLTE データが許可されます。

すべてのデータトラフィックの許可

SRP 構成モードの **switchover allow-all-data-traffic** コマンドを使用すると、スイッチオーバーの移行中にすべてのデータトラフィック（VoLTE および非 VoLTE）が許可されます。このコマンドは、P-GW で有効になっている場合、**switchover allow-volte-data-traffic** コマンドを上書きします。この機能により、スイッチオーバー中のデータトラフィックの停止を短くします。

重要 この機能を有効にするには、このCLIコマンドがアクティブシャーシとスタンバイシャーシの両方で実行されている必要があります。

フラッシュおよび内部監査中は、すべてのデータトラフィックがアクティブシャーシで許可されます。フラッシュが完了すると、課金情報はバックグラウンドで調整されます。

早期にアクティブへの移行を許可

SRP 構成モードの**スイッチオーバーの allow-early-active-transition** コマンドを実行すると、ICSR スイッチオーバー中にアクティブ状態への早期の移行が可能になります。デフォルトでは、この機能はディセーブルになっています。

このコマンドは、計画されたスイッチオーバー時のデータ停止時間をさらに短縮するために、**allow-all-data-traffic** または **allow-volte-data-traffic**（**アカウンティングの維持**オプションは指定しない）コマンドと組み合わせて使用します。停止時間とは、ICSR スイッチオーバーを開始してから、新しくアクティブになったシャーシがデータの処理を開始するまでの時間です。

重要 このコマンドを有効にする前に、両方の ICSR シャーシで上記のコマンドのいずれかを有効にする必要があります。

失敗したコールの監査後における ICSR の正常なクリーンアップ

セッションリカバリまたは ICSR イベント後のゲートウェイ（P-GW/S-GW/GGSN/SAE-GW）の監査中に、内部または外部でサブスクライバセッションに関連する重要な情報が矛盾していると思われる場合、ICSR は関連するセッション情報をローカルで消去します。

外部ゲートウェイ（ピアノード）はこのセッションの消去を認識していないため、UEセッションは他のノードで維持される場合があります。これにより、ゲートウェイの外部のリソースが占有され、VoLTE コール用の UE に到達できなくなります。

この機能を有効にすると、失敗したコールの ICSR 監査のために正常なクリーンアップが行われます。外部シグナリングは、セッションを消去する前にセッションの終了をピアに通知します。ゲートウェイは、セッションの削除を外部ピアに通知しようとします。ローカルゲートウェイへの外部ノードには、S-GW、P-GW、SGSN、MME、AAA、PCRF および IMSA が含まれます。

監査エラーは、セッション情報が欠落しているか不完全であることが原因で発生する可能性があります。したがって、情報が使用可能なピアのみに通知されます。

グローバル構成モードの **require graceful-cleanup-during-audit-failure** CLI コマンドは、正常なクリーンアップの機能を有効または無効にします。

```
configure
  require graceful-cleanup-during-audit-failure [ del-cause non-ims-apn
   { system-failure | none } ]
```

スイッチオーバー制御の停止時間の最適化

ICSR フレームワークは、完全なチェックポイント統計情報のフラッシュ、ネットワークコンバージェンス、および内部監査に関連する制御停止時間を最小限に抑えます。

次のアクティビティによって消費される時間は、スイッチオーバー時の制御停止時間に影響します。

- **クリティカルフラッシュ**：アクティブから保留中への移行中に、すべての sessmgrs が保留中の重要な FC をフラッシュします（完全なチェックポイント）。この間、アクティブシャーシはすべての制御パケットをドロップします。この段階で制御シグナリングが許可されている場合は、制御メッセージタイプに基づいてコールが切断され、アカウンティング情報が失われます。
- **ネットワークコンバージェンス**：ルートを更新し、新たにアクティブになったシャーシに制御およびデータを送信するのにかかる時間が含まれます。制御メッセージは、移行中にドロップされます。
- **アカウンティング フラッシュ**：このフラッシュの段階で、シャーシ間でデータカウントが同期されます。フラッシュ中に制御シグナリングが許可されている場合、コールは制御メッセージタイプに基づいて切断される可能性があり、スイッチオーバー前に存在したコールについてはアカウンティング情報が失われます。
- **監査**：コールリソースの同期によってコールがクリアされる可能性があるため、監査中に新しいコールは許可されません。

switchover control-outage-optimization CLI コマンドは、監査が完了するとすぐに、アカウンティングのフラッシュ中に新しいコールを許可します。この SRP 構成モードコマンドは、ICSR スイッチオーバー後の制御トラフィック（コールセットアップ、変更、削除）の迅速な復元を可能にします。

```
configure
  context context_name
    service-redundancy-protocol
      switchover control-outage-optimization
      end
```

SRP コンテキストのインターフェイス パラメータの設定

この手順では、SRP コンテキスト内の IP アドレスとポート番号を使用して通信インターフェイスを設定します。このインターフェイスはシャーシ間通信をサポートします。

重要 CLI コマンドは、両方のシャーシで実行する必要があります。続行する前に、両方のシャーシにログインします。常に、プライマリシャーシで設定の変更を最初に行います。

```
configure
  context vpn_ctxt_name [-noconfirm]
     interface srp_if_name
     ip-address { ip_address | ip_address/mask }
     exit
   exit
  port ethernet slot_num/port_num
    description des_string
    medium { auto | speed { 10 | 100 | 1000 } duplex { full | half } }
    no shutdown
    bind interface srp_if_name srp_ctxt_name
    end
```

SRP チェックポイント メッセージング エラーに対する NACK 生成の設定

スタンバイシャーシからの NACK メッセージングの有効化

ICSR シャーシ間の SRP リンクでは、トランスポート（TCP）レベルの再送信がサポートされています。SRP の設定では、スタンバイシャーシでチェックポイントを確実に受信できるようにするために、オプションのアプリケーションレベルのチェックもサポートされています。チェックポイントの受信と適用が失敗すると、NACK メッセージがアクティブシャーシに送信されます。

この機能が有効になっていて、スタンバイシャーシが正常に適用されなかったマイクロチェックポイント（MC）の受信に応答して NACK を送信した場合、スタンバイシャーシは別の NACK を送信します。マクロチェックポイント（FC）が受信されない場合、スタンバイシャーシは 10 分間により多くの NACK（設定可能、デフォルトは 3）を送信します。FC が受信されて適用されるか、または設定された最大応答数に達するまで、NACK は送信され続け、10 分のリセットが行われます。

障害が発生した MC または FC への応答として、10 分間に NACK を送信する回数を指定することもできます（デフォルトは 3）。

SRP 構成モードの **checkpoint session** コマンドで **nack** キーワードを使用すると、スタンバイ ICSR シャーシのチェックポイントメッセージの障害に応じて、NACK メッセージの生成を有効にすることができます。

重要 **nack** キーワードは、特別な ICSR 最適化機能のライセンスが購入およびインストールされている場合にのみ表示されます。詳細については、シスコのアカウント担当者にお問い合わせください。

```
configure
   context context_name
      service-redundancy-protocol variable
         checkpoint session nack { macro | micro } [ max-response number
]
         no checkpoint session nack { macro | micro }
         end
```

注：

- **max-response** は、障害が発生した MC または FC への応答として、10 分間に NACK が送信された回数で、0 ～ 65535 の整数で表されます（デフォルトは 3）。

SRP 構成モードの **checkpoint session** コマンドの **periodic-interval** キーワードを使用すると、アクティブシャーシとスタンバイシャーシ間のマクロチェックポイント（FC）の送信間隔を設定できます。

重要 **eriodic-interval** キーワードは、特別な ICSR 最適化機能のライセンスが購入およびインストールされている場合にのみ表示されます。詳細については、シスコのアカウント担当者にお問い合わせください。

```
configure
   context context_name
      service-redundancy-protocol variable
         checkpoint session periodic-interval minutes
         default checkpoint session periodic-interval
         no checkpoint session periodic-interval
         end
```

NACK メッセージングの選択的無効化

NACK メカニズムは、スタンバイシャーシで ICSR チェックポイント障害が発生した場合に、NACK メッセージを送信します。スタンバイシャーシから送信されたすべての NACK がアクティブシャーシからの完全なチェックポイントをトリガーします。

マイクロチェックポイントが継続的に失敗し、NACK を送信している場合、アクティブシャーシは完全なチェックポイントを送信し続けます。これにより、SRP の帯域幅が増加します。

CLI コマンドを使用すると、オペレータは特定のマイクロチェックポイントに対する NACK メッセージを選択的に無効にしたり、再度有効にしたりできます。

Exec モード **srp disable nack micro-chkpt-cmd** は、スタンバイシャーシからの NACK の送信を無効にします。

srp disable nack micro-chkpt-cmd *chkpt_number*

chkpt_number は、無効にするチェックポイント番号を 1 ～ 255 の整数として指定します。**show srp checkpoint info** コマンドの出力からチェックポイント番号（CMD ID）を取得できます。

srp enable nack micro-chkpt-cmd コマンドを使用して、マイクロチェックポイントを再度有効にすることができます。

srp enable nack micro-chkpt-cmd *chkpt_number*

LZ4 圧縮アルゴリズムの設定

必要に応じて、SRP メッセージングペイロードの 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。

LZ4 は非常に高速な無損失圧縮アルゴリズムであり、マルチスレッドアプリケーションに対して直線的なスケーラビリティを備えています。

SRP 構成モードの **checkpoint session** コマンドの **compression** キーワードを使用すると、LZ4 圧縮アルゴリズムの使用を有効にすることができます。

重要 **compression** キーワードは、特別な ICSR 最適化機能のライセンスが購入およびインストールされている場合にのみ表示されます。詳細については、シスコのアカウント担当者にお問い合わせください。

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
      service-redundancy-protocol
         checkpoint session compression lz4
         end
```

LZ4 圧縮は、両方のシャーシが LZ4 を使用して設定されている場合にのみ有効です。いずれかのシャーシに zlib（デフォルト）が設定されている場合、圧縮アルゴリズムは zlib に戻ります。このアルゴリズムは、最初のソケットの確立時にのみネゴシエートされます。同意すると、TCP ソケット接続がリセットされるまでネゴシエーションは行われません。

スタンバイの ICSR シャーシによる同期時間の短縮

SRP データベースを同期するためのデフォルトの方法では、アクティブなセッションマネージャとスタンバイセッションマネージャの間に TCP 接続が確立されるたびに、10 秒間の遅延が必要です。TCP 接続が確立されると、ハートビートメッセージが両方の ICSR シャーシ間で 3 秒ごとに交換されます。スタンバイシャーシは、データを受け入れる準備が整うまで、アクティブなシャーシから 7 つのハートビートメッセージを待機します。これにより、スタンバイシャーシでのセッションマネージャデータベースの同期が大幅に遅延する可能性があります。

セッション マネージャ データベースを同期するためのアグレッシブな方式を有効にすると、次のシナリオでのリカバリ時間が短縮されます。

- スタンバイ セッション マネージャのクラッシュ
- スタンバイシャーシでのパケット処理カードの障害
- スタンバイシャーシの再起動
- SRP 接続の一時的な損失とリカバリ

アグレッシブな方式は、ICSR シャーシ間で交換されるハートビートメッセージの数とハウスキーピング情報の量を削減します。

SRP 構成モードの **standby database-recovery aggressive** コマンドを使用すると、SRP データベースの通常またはアグレッシブな復元を選択できます。

次のコマンドシーケンスは、アグレッシブリカバリモードを有効にします。

```
configure
   context context_name
      service-redundancy-protocol
         standby database-recovery aggressive
         end
```

このコマンドのデフォルト形式は、SRP データベースリカバリの通常モードを復元します。

SRP 設定の確認

各シャーシで **show SRP info** コマンド（Exec モード）を実行して、SRP コンテキストが作成され、適切に設定されていることを確認します。

注：

- 間隔は、30 ～ 1440 の範囲で 15 で割り切れる整数で指定されます（デフォルトは 45 分）。完全なチェックポイントを送信する間隔の範囲は、30 分 ～ 24 時間（1440 分）です。

ICSR の送信元コンテキストの変更

コアサービスの送信元コンテキストを変更するには、次のようにします。

手順

ステップ 1 ボーダー ゲートウェイ プロトコル（BGP）のルータの AS パスを追加し、BGP ルータとゲートウェイアドレスの設定 （28 ページ）の設定例を適用して、コアネットワークサービスが設定されている送信元コンテキストのゲートウェイ IP アドレス、ネイバー IP アドレス、リモート IP アドレスを設定します。

ステップ 2 BGP 用の SRP コンテキストの設定 （28 ページ）の設定例を適用して、BGP ネイバーコンテキストと IP アドレスを使用してサービス冗長性コンテキストを設定し、BGP リンクアクティビティをモニターします。

ステップ 3 BGP 設定の確認 （29 ページ）の手順に従って、BGP コンテキストの設定を確認します。

ステップ 4 「設定の確認と保存」の説明に従って、設定を保存します。

BGP ルータとゲートウェイアドレスの設定

BGP コンテキストとネットワークアドレスを作成するには、次の例を使用します。

```
configure
  context source_ctxt_name
    router bgp AS_num
      network gw_ip_address
      neighbor neighbor_ip_address remote-as AS_num
      end
```

注：

- *source_ctxt_name* は、コアネットワークサービスが設定されているコンテキストです。

BGP 用の SRP コンテキストの設定

次の例を使用して、SRP コンテキストでの BGP コンテキストと IP アドレスを設定します。

```
configure
  context srp_ctxt_name
    service-redundancy-protocol
      monitor bgp context source_ctxt_name neighbor_ip_address
      end
```

neighbor_ip_address は、IPv4 のドット付き 10 進表記または IPv6 のコロンで区切られた 16 進表記で入力できます。コンテキストごとに、IPv4 アドレスまたは IPv6 IP アドレスとして複数の IP アドレスを追加できます。

ICSR フェールオーバーは、コンテキスト内のすべての BGP ピアがダウンしたときにトリガーされます。

必要に応じて、コンテキスト内に SRP ピアグループを設定できます。ICSR フェールオーバーは、グループ内のすべてのピアで障害が発生した場合に発生します。このオプションは、IPv4 と IPv6 のピアの組み合わせが複数ペアの VLAN に分散され、ピアグループのすべてのメンバーによって IPv4 または IPv6 の接続が失われる展開で役立ちます。

コンテキスト内の SRP ピアグループの設定例（「PGWin」）を次に示します。

```
monitor bgp context PGWin 10.1.1.16 group 1
monitor bgp context PGWin 10.1.1.17 group 1
monitor bgp context PGWin 69.2.215.0 group 2
monitor bgp context PGWin 69.2.215.1 group 2
monitor bgp context PGWin 2001:4333:201:1102:103:2a1:: group 3
monitor bgp context PGWin 2001:4333:201:1102:103:2a1:0:1 group 3
```

上記の設定例では、グループ 1、2、または 3 のすべてのアドレスで接続を失った場合、ICSR フェールオーバーが発生します。

詳細については、『*Command Line Interface Reference*』と「*Service Redundancy Protocol Configuration Mode Commands*」の章の **monitor bgp**、**monitor diameter**、および **monitor authentication-probe** の各コマンドの説明を参照してください。

BGP 設定の確認

show srp monitor bgp コマンド（Exec モード）を入力して、BGP 設定を確認します。

ICSR の接続先コンテキストの変更

コアサービスの接続先コンテキストを変更するには、次の手順を実行します。

手順

ステップ 1 BGP ルータを追加し、接続先コンテキストでの BGP ルータとゲートウェイアドレスの設定 （29 ページ）の設定例を適用してコアネットワークサービスが設定されている接続先コンテキストの ゲートウェイ IP アドレス、ネイバー IP アドレス、リモート IP アドレスを設定します。

ステップ 2 BGP ネイバーコンテキストと IP アドレスを使用してサービス冗長性コンテキストを設定し、接続先コンテキスト用の BGP の SRP コンテキストの設定 （29 ページ）の設定例を適用して BGP リンクアクティビティをモニターします。

ステップ 3 サブスクライバをデフォルトモードに設定 （30 ページ）の手順に従って、サブスクライバモードを **default** に設定します。

ステップ 4 接続先コンテキストでの BGP 設定の確認 （30 ページ）の手順に従って、BGP コンテキストの設定を確認します。

ステップ 5 「設定の確認と保存」の説明に従って、設定を保存します。

接続先コンテキストでの BGP ルータとゲートウェイアドレスの設定

BGP コンテキストとネットワークアドレスを作成するには、次の例を使用します。

```
configure
  context dest_ctxt_name
    router bgp AS_num
      network gw_ip_address
      neighbor neighbor_ip_address remote-as AS_num
      end
```

注：

- *AS_num* は、この BGP ルータの自律システムのパス番号です。

接続先コンテキスト用の BGP の SRP コンテキストの設定

次の例を使用して、SRP コンテキストでの BGP コンテキストと IP アドレスを設定します。

```
configure
  context srp_ctxt_name
    service-redundancy-protocol
```

```
monitor bgp context dest_ctxt_name neighbor_ip_address
end
```

サブスクライバをデフォルトモードに設定

サブスクライバのモードを**デフォルト**に設定するには、次の例を使用します。

```
configure
  context dest_ctxt_name
    subscriber default
     end
```

接続先コンテキストでの BGP 設定の確認

show srp monitor bgp コマンド（Exec モード）を入力して、BGP 設定を確認します。

スタンバイシステムでのバルク統計情報収集の無効化

システムからのバルク統計情報の収集は、スタンバイ動作モードのときに無効にすることができます。

重要 この機能が有効になっていて、システムがスタンバイ状態に移行すると、保留中の累積統計データが最初の機会に転送されます。その後、システムがスタンバイ状態から抜け出すまで、追加の統計情報の収集は行われません。

スタンバイシステムでバルク統計情報収集を無効にするには、次の例を使用します。

```
configure
  bulkstat mode
    no gather-on-standby
    end
```

この手順を両方のシステムで繰り返します。

プライマリ設定とバックアップ設定の確認

この項では、プライマリシステムとバックアップシステムの ICSR 設定の比較方法について説明します。

手順

ステップ 1 各システム（Exec モード）で **show configuration srp** コマンドを入力します。

ステップ 2 両方のシャーシの SRP 設定情報が同じであることを確認します。

出力は次のようになります。

```
config
  context source
    interface haservice loopback
      ip address 172.17.1.1 255.255.255.255 srp-activate
    #exit
    radius attribute nas-ip-address address 172.17.1.1
    radius server 192.168.83.2 encrypted key 01abd002c82b4a2c port 1812
    radius accounting server 192.168.83.2 encrypted key 01abd002c82b4a2c port 1813
    ha-service ha-pdsn
      mn-ha-spi spi-number 256  encrypted secret 6c93f7960b726b6f6c93f7960b726b6f hash-algorithm
md5
      fa-ha-spi remote-address 192.168.82.0/24 spi-number 256 encrypted secret 1088bdd6817f64df
      bind address 172.17.1.1
    #exit
  #exit
  context destination
    ip pool dynamic 172.18.0.0 255.255.0.0 public 0 srp-activate
    ip pool static 172.19.0.0 255.255.240.0 static srp-activate
  #exit
  context srp
    service-redundancy-protocol
    #exit
  #exit
```

サブスクライバ状態管理の監査プロセスの設定

この監査は、2 つの ICSR ピアが同期していることを確認し、スケジュール済みまたは予定外のスイッチオーバーイベントの前に不一致を識別します。

手順

ステップ 1 SRP コンテキストモードを開始し、**service-redundancy-protocol** コマンドを入力します。

ステップ 2 **audit daily-start-time** コマンドを入力します。毎日の開始時刻を時間と分で指定します。たとえば、06 00 の開始時刻は、監査が 6:00 AM に開始されることを示しています。

ステップ 3 **audit periodicity** コマンドを入力します。SRP 監査統計情報を生成する間隔を、60 ～ 1440 の整数として分単位で指定します。たとえば、90 の周期は、指定された開始時間以降に、SRP 監査統計情報が 90 分ごとに生成されることを示します。デフォルト = 60 です。

設定シーケンスの例を次に示します。

```
config
  context srp
    service-redundancy-protocol
      audit daily-start-time 06 00
      audit periodicity 90
      end
```

ICSR 運用のトラブルシューティング

SSD

StarOS は、Exec モードの一連の **show** コマンドの結果を出力する ICSR 固有の **show support details**（SSD）コマンドをサポートしています。このミニ SSD によって、アクティブとスタンバイのシャーシ間で ICSR のタイミングに関する問題をデバッグする際のキャプチャ時間を短縮し、問題の迅速な解決を助長します。

show support details icsr コマンドは、次の **show** コマンドの出力を含むミニ SSD を生成します。

- show srp info
- show srp checkpoint statistics
- show srp checkpoint statistics verbose
- show srp checkpoint statistics debug-info
- show srp checkpoint statistics sessmgr all
- show srp checkpoint statistics sessmgr all debug-info
- show srp checkpoint statistics ipsecmgr all
- show srp checkpoint statistics sessmgr all write-list-stats
- show srp checkpoint info
- show srp monitor
- show srp monitor all
- show srp monitor diameter debug
- show srp statistics
- show srp call-loss statistics
- show srp audit-statistics
- show session subsystem facility sessmgr all debug-info

SSD の出力は、**/flash** またはシャーシ外に保存できるファイルに転送できます。詳細については、『*Command Line Interface Reference*』を参照してください。

show srp details

Exec モードの **show srp details** コマンドは、ICSR/SRP の問題をトラブルシューティングするために TAC 担当者が使用する包括的な情報を表示します。

オペレーティングシステムの更新

ICSR システム上のオペレーティングシステム（StarOS™）の更新は、スタンバイモードの間にシステムごとに個別に実行されます。スタンバイシステムが更新されている間、アクティブなシステムがコールセッションを処理するため、トラフィックの中断は最小限に抑えられます。

一般的な更新手順は次のとおりです。

1. StarOSのソフトウェアイメージをダウンロードし、アクティブとスタンバイの両方のシステムにコピーまたは転送します。
2. 両方のシステムで現在実行中の設定を保存します。
3. スタンバイ バックアップ システムを最初に更新します。
4. スタンバイ バックアップ システムがアクティブになるように、アクティブなプライマリ システムから SRP スイッチオーバーを開始します。
5. スタンバイ プライマリ システムを更新します。
6. スタンバイ プライマリ システムがアクティブになるように、アクティブなバックアップ システムから SRP スイッチオーバーを開始します。

次に、StarOSのアップグレードプロセスを完了するために必要なすべての手順を詳しく説明した、4 つのパートから成るフローチャートを示します。

⚠

注意 MIO/UMIO機能でデマルチプレクサを有効にすると、システム内のリソース割り当てが変更されます。これは、ICSR 設定内の StarOS バージョン間のアップグレードまたはダウングレードに直接影響を与えます。Star OS 21.24 リリースでは、2 つのリリース（N-2）より上の ICSR アップグレードは完全には認定されていません。詳細については、ICSRの展開をアップグレードまたはダウングレードする前に、シスコのアカウント担当者に連絡して手順についてのサポートを受けてください。

図 *5 : ICSR* ソフトウェアアップグレード：パート *1*

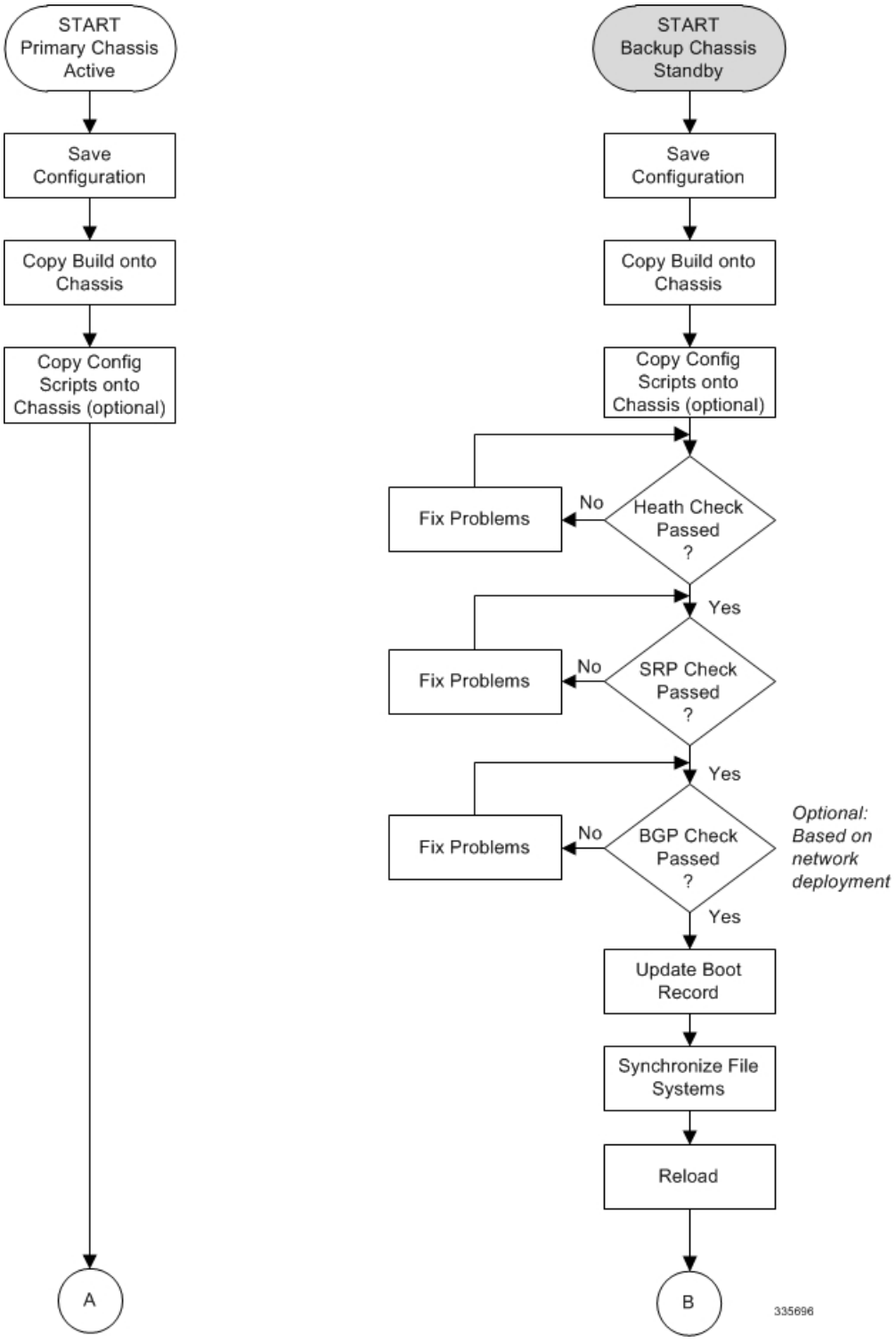


図 *6 : ICSR* ソフトウェアアップグレード：パート*2*

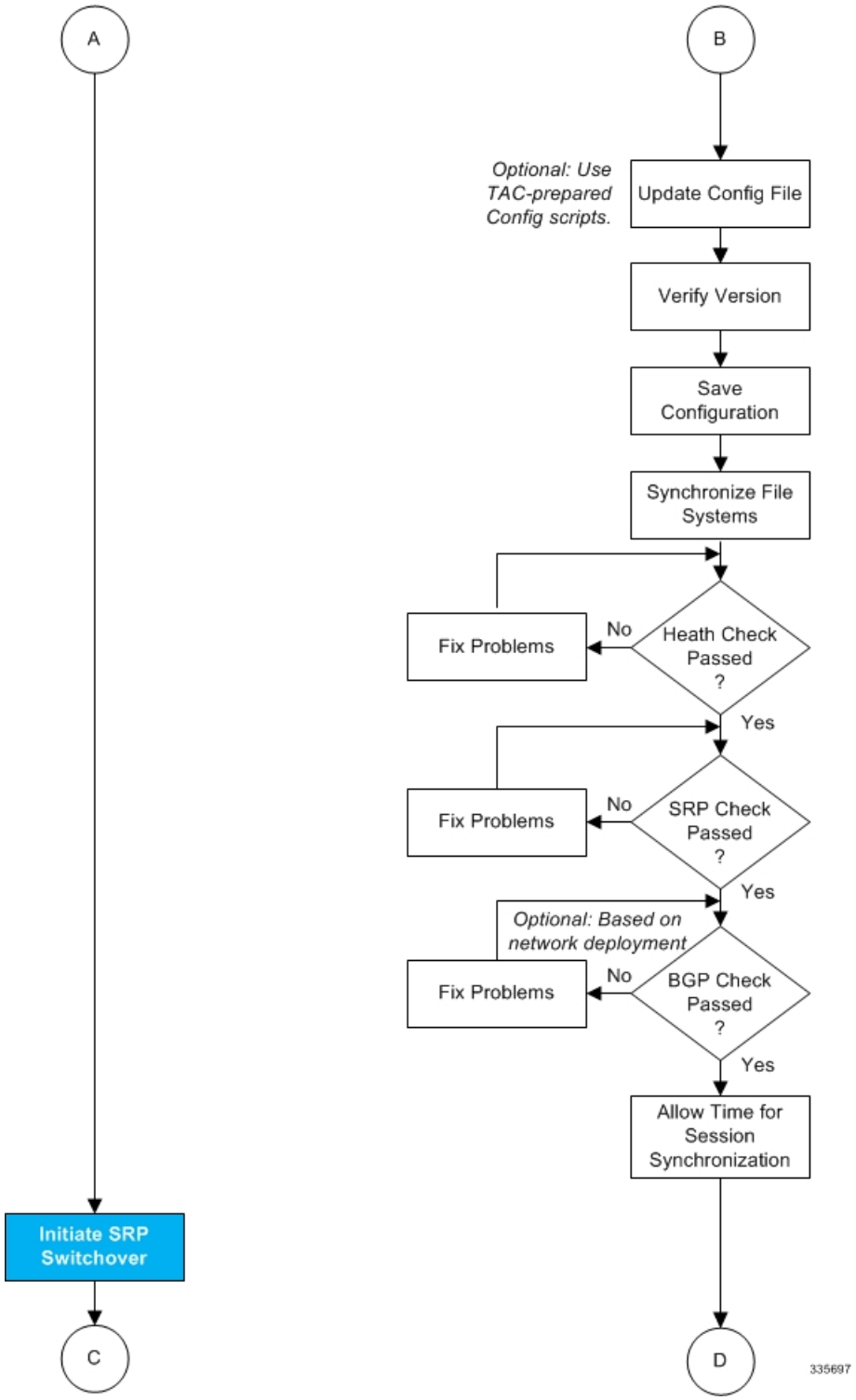


図 *7: ICSR* ソフトウェアアップグレード：パート*3*

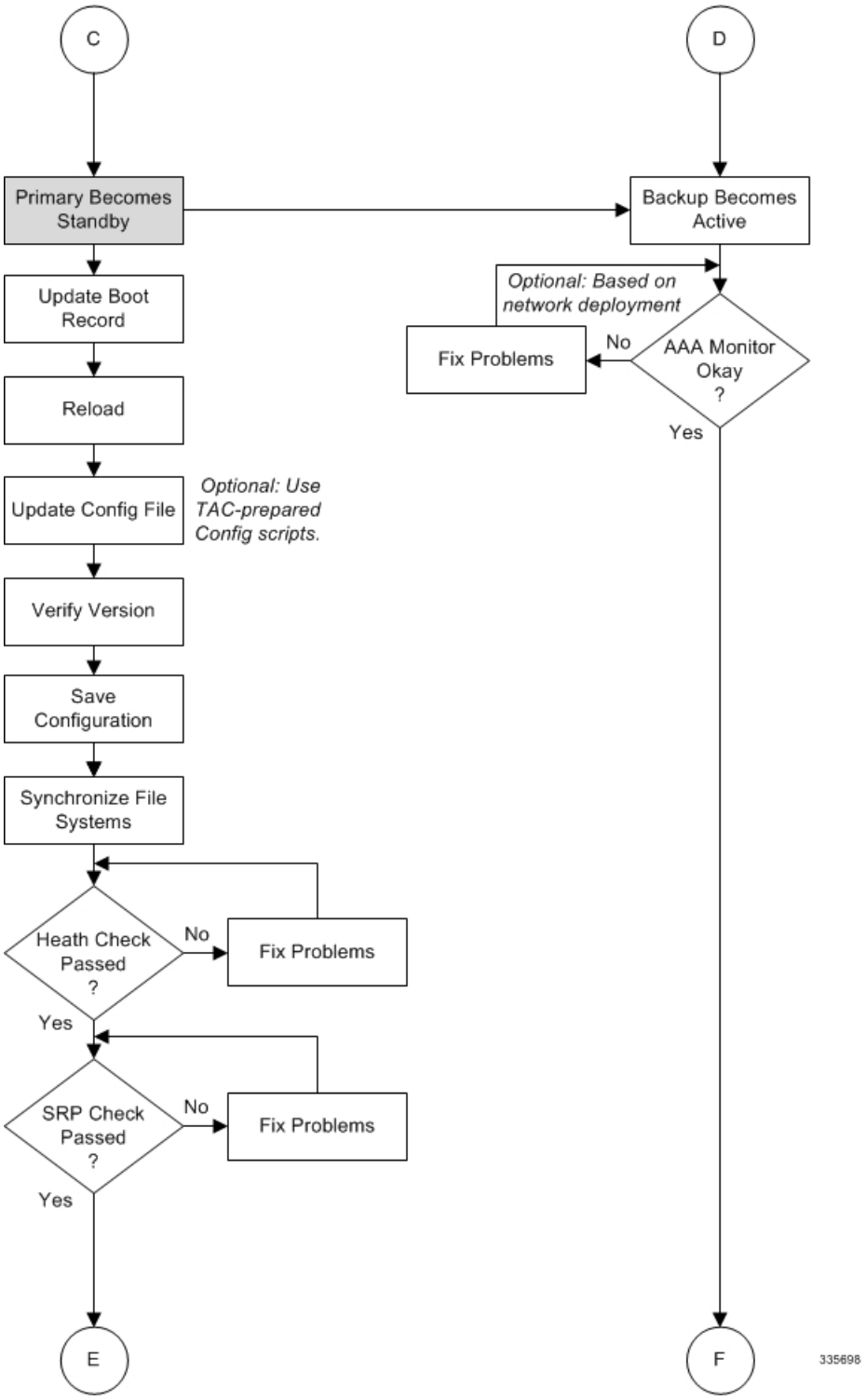
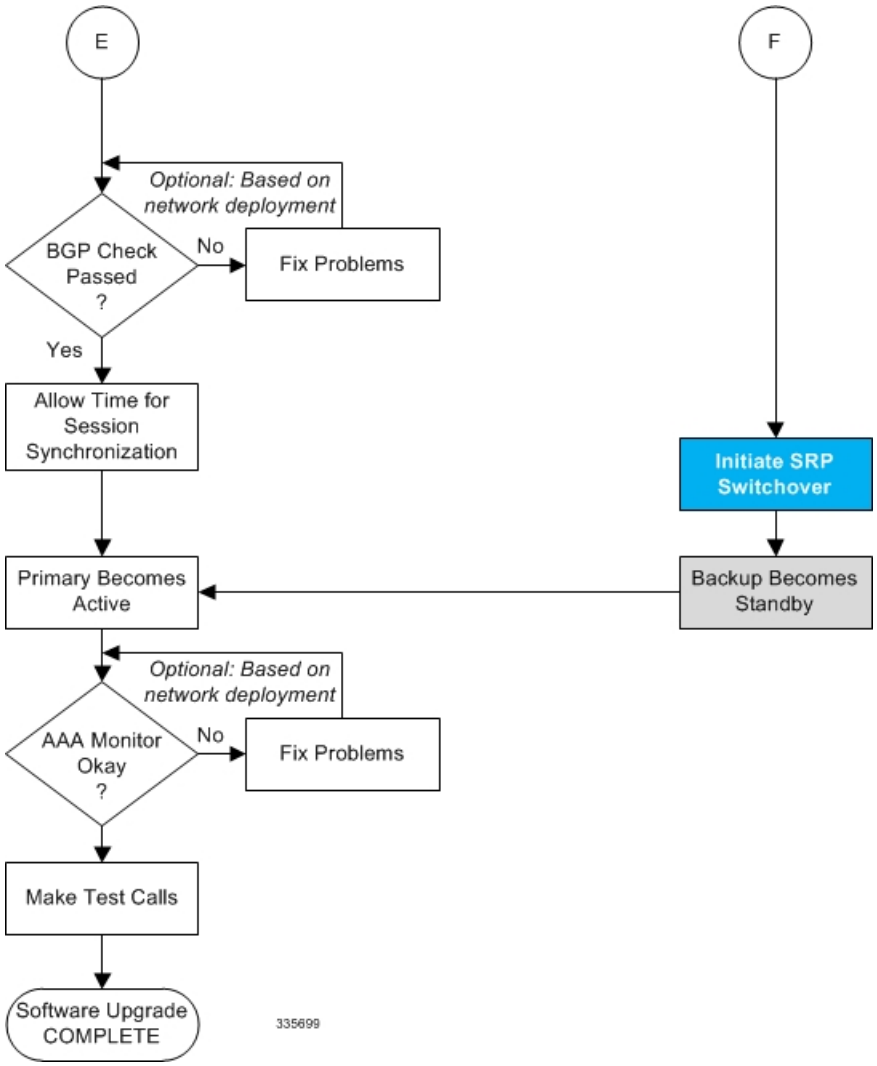


図 *8 : ICSR* ソフトウェアアップグレード：パート *4*



両方の ICSR システム

プライマリ（アクティブ）とバックアップ（スタンバイ）の両方の ICSR システムで、次に説明するタスクを実行します。

StarOS イメージのダウンロードと転送

手順

ステップ 1 次の Exec モードのコマンドを入力して、新しいオペレーティングシステムのイメージファイルに対応するために、**/flash** デバイスに十分な空き領域があることを確認します。[local]*host_name*# **directory /flash**

ステップ 2 シスコのサポートサイトとダウンロードファシリティへのアクセスは、ユーザー名とパスワードで制御されています。**/flash**デバイスにアップロードできるネットワークの場所または物理デバイス（USB スティック）に、ソフトウェアイメージをダウンロードします。

ステップ 3 次のいずれかの方法を使用して、新しいオペレーティングシステムのイメージファイルを MIO/UMIO 上の **/flash** デバイスに転送します。

a) **copy** コマンドを使用して、MIO/UMIO に接続されているネットワークの場所またはローカルデバイスからファイルをコピーします。

```
[local]host_name# copy from_url to_url [-noconfirm]
```

b) システムへのアクセス権を持つ FTP クライアントを使用して、ファイルを **/flash** デバイスに転送します。FTP クライアントは、バイナリモードを使用してファイルを転送するように設定する必要があります。

c) システムへのアクセス権を持つ SFTP クライアントを使用して、ファイルを **/flash** デバイスに転送します。

FTP はサポートされていません。

ステップ 4 Exec モードの次のコマンドを実行して、イメージファイルが **/flash** デバイスに正常に転送されたことを確認します。

```
[local]host_name# directory /flash
```

ステップ 5 **show version /flash/***image_filename* コマンドを実行して、ビルド情報を確認します。

CRC エラーは、このコマンドの出力に表示されます。エラーが表示された場合は、ビルドを確認し、シャーシに再転送します。正しいイメージバージョンとビルドの説明が表示されていることを確認します。

StarOS イメージのダウンロードと転送

手順

ステップ 1 次の Exec モードのコマンドを入力して、新しいオペレーティングシステムのイメージファイルに対応するために、**/flash** デバイスに十分な空き領域があることを確認します。

```
[local]host_name directory /flash
```

ステップ 2 シスコのサポートサイトとダウンロードファシリティへのアクセスは、ユーザー名とパスワードで制御されています。**/flash** デバイスにアップロードできるネットワークの場所またはローカルドライブにソフトウェアイメージをダウンロードします。

ステップ 3 次のいずれかの方法を使用して、新しいオペレーティングシステムのイメージファイルを **/flash** デバイスに転送します。

a) copy コマンドを使用して、ネットワークの場所またはローカルドライブからファイルをコピーします。

```
[local]host_name copy from_url to_url [-noconfirm]
```

b) システムへのアクセス権を持つ FTP クライアントを使用して、ファイルを **/flash** デバイスに転送します。FTP クライアントは、バイナリモードを使用してファイルを転送するように設定する必要があります。
c) システムへのアクセス権を持つ SFTP クライアントを使用して、ファイルを **/flash** デバイスに転送します。

ステップ 4 次の Exec モードのコマンドを実行して、イメージファイルが **/flash** デバイスに正常に転送されたことを確認します。

```
[local]host_name directory /flash
```

ステップ 5 **show version /flash/***image_filename* コマンドを実行して、ビルド情報を確認します。次に例を示します。

```
local]host_name show version /flash/image_filename.bin
```

（注）
CRC エラーは、上記のコマンドの出力に表示されます。エラーが表示された場合は、ビルドを確認し、シャーシに再転送します。正しいイメージバージョンとビルドの説明が表示されていることを確認します。

スタンバイ ICSR システム

バックアップ ICSR またはスタンバイ ICSR システムで、次に記述するタスクを実行します。

正常性チェックの実行

正常性チェックは、ソフトウェアの更新を処理するためのシステムの準備状況を確認する Exec モードの一連の **show** コマンドです。

手順

ステップ 1 **show card table all |grep unknown** を実行します。出力は表示されません。
ステップ 2 **show card table |grep offline** を実行します。出力は表示されません。
ステップ 3 **show resources |grep Status** を実行します。出力に「Within acceptable limits」と表示されます。
ステップ 4 **show alarm outstanding** を実行します。ソフトウェア更新の実行を妨げる可能性のある問題の有無を出力で確認します。

SRP チェックの実施

サービス冗長性プロトコル（SRP）のチェックは、ICSR システムステータスのモニタリングメカニズムが動作可能であることを確認します。

手順

ステップ 1 **show srp monitor all** を実行します。

ステップ 2 ソフトウェア更新の実行を妨げる可能性のある問題の有無を出力で確認します。

BGP チェックの実施

ボーダー ゲートウェイ プロトコル（BGP）のチェックは、BGP を使用して冗長シャーシ間通信をサポートする場合にのみ必要です。これらのチェックは、コンテキストごとおよびサービスタイプごとに実行されます。

手順

ステップ 1 各 BGP 対応コンテキストに対して、**show ip bgp summary** を実行します。BGP ピアが接続されており、IPv4 および IPv6 ピアが稼働していることを確認します。すべての BGP 対応コンテキストに対してこの手順を繰り返します。

ステップ 2 **show** *service_name* **all |grep "Service Status:"** を実行します。サービスを「開始」する必要があります。シャーシで実行されているすべてのサービスに対して手順を繰り返します。

ブートレコードの更新

最近ダウンロードしたソフトウェアイメージ（.bin）ファイルの新しい起動スタックエントリを追加する必要があります。

手順

ステップ 1 Exec モードの **show boot** コマンドを実行して、boot.sys ファイルに 10 未満のエントリがあることと、高い優先順位のエントリが使用可能である（最小で起動スタックに優先順位 1 のエントリがない）ことを確認します。

ステップ 2 次のグローバル構成コマンドを入力して、新しいオペレーティングシステムイのメージファイルと現在使用されている CLI 設定ファイルで構成される新しいファイルグループの新しい起動スタックエントリを作成します。

```
[local]host_name(config)# boot system priority number image image_url /flash/filename config
 cfg_url /flash/filename
```

ステップ 3 <N-1> 方式を使用して、このエントリに次に高い優先順位を割り当てます。この場合、優先順位番号は、現在の最高の優先順位よりも 1 つ小さい値を割り当てます。

優先順位 1 が使用されている場合は、既存のエントリの数字を再割り当てし、少なくともその優先順位 1 を使用できるようにします。

boot.sys ファイルに含めることができる起動スタックエントリの最大数は 10 です。起動スタックにすでに 10 個のエントリがある場合は、これらのエントリのうち少なくとも 1 つを削除する必要があります（通常は優先順位が最も低いエントリ）。また、必要に応じて、他のエントリの一部またはすべての番号を再割り当てしてから続行します。起動スタックエントリを削除するには、**no boot system priority** コマンドを使用します。

boot system priority コマンドの使用方法については、このガイドの「新しい起動スタックエントリの追加」の項を参照してください。

ファイルシステムの同期

次の Exec モードコマンドを入力して、ローカルファイルシステムを同期します。

```
[local]host_name# filesystem synchronize all
```

StarOS の再起動

次のコマンドを入力して、StarOS を再起動します。

```
[local]host_name# reload [-noconfirm]
```

システムが再起動すると、以前に設定した新しい起動スタックエントリを使用して、新しいオペレーティングシステムのソフトウェアイメージとそれに対応する CLI 構成ファイルがロードされます。

システムが再起動したら、CLI セッションを確立し、**show version** コマンドを入力して、アクティブなソフトウェアバージョンが正しいことを確認します。

PDSN のオプション：アップグレード中に IP プール共有プロトコルを使用している場合は、『*PDSN Administration Guide*』の「*Configuring IPSP Before the Software Upgrade*」を参照してください。

設定ファイルの更新

新しいオペレーティングシステムの機能によっては、構成ファイルの変更が必要になる場合があります。これらの変更は、手動で行うことも、Cisco TAC に用意されたカスタムスクリプトによって容易に行うこともできます。更新された構成ファイルを保存する前に、必要な変更を行います。

ソフトウェアバージョンの確認

システムが正常に起動したら、Exec モードの **show version** コマンドを実行して、新しい StarOS バージョンが実行されていることを確認します。

Exec モードの **show build** コマンドを実行すると、StarOS ビルドのリリースに関する追加情報を表示できます。

設定ファイルの保存

Exec モードの save 設定コマンドを使用して、現在の実行時設定を **/flash** デバイスとシャーシ外の場所（外部メモリデバイスやネットワーク URL）に保存します。シャーシ外コピーが、障害が発生した場合に使用できるフォールバック用のロード可能な設定ファイルとなります。

更新プロセスの完了

スタンバイ セカンダリ シャーシのアップグレードプロセスを完了するには、次のタスクを繰り返します。

- ファイルシステムの同期 （41 ページ）
- 正常性チェックの実行 （39 ページ）
- SRP チェックの実施 （39 ページ）
- BGP チェックの実施 （40 ページ）

セッションの同期の待機

次の手順に進む前に、ICSR シャーシ間で実行されるシステム同期の時間を割り当てます。

手順

ステップ 1 両方のシャーシで **how session recovery status verbose** コマンドを実行します。このコマンドの出力にエラーが表示されない場合にのみ、次の手順に進みます。

ステップ 2 スタンバイシャーシで **show srp checkpoint statistics |more** を実行します。

ステップ 3 アクティブシャーシで **show subs summary |grep Total** を実行します。

ステップ 4 アクティブシャーシのサブスクライバの数と、スタンバイシャーシの現在の事前に割り当てられたコール数（Current pre-allocated calls: ）を比較します。これらは同様（5% 以内）である必要があります。システムが同期を完了するまで数分間待ちます。

プライマリシステム（Primary System）

プライマリ（アクティブ）ICSR システムで次に説明するタスクを実行します。

SRP スイッチオーバーの開始

SRP スイッチオーバーでは、プライマリシャーシがスタンバイモードになり、バックアップシャーシがアクティブになります。セカンダリシャーシが、アップグレードされたソフトウェアとのセッションを処理するようになりました。

手順

ステップ 1 プライマリシャーシで、**srp initiate-switchover** コマンドを実行します。既存のすべてのセッションは、バックアップシャーシに移行され、新しいセッション要求の処理が開始されます。スイッチオーバープロセスが完了するのを許可します。

ステップ 2 プライマリシャーシで、**show srp info** コマンドを実行します。スイッチオーバーが完了すると、シャーシの状態は [Standby] を示します。

ステップ 3 バックアップシャーシで、**show srp info** コマンドを実行して、スイッチオーバーが完了していることを確認します。スイッチオーバーが完了すると、シャーシの状態は [Active] を示します。

新しくアクティブになったシステムでの AAA モニターステータスの確認

ネットワーク展開で AAA サーバーとの通信が必要な場合は、新しくアクティブになったシステムにログインし、AAA モニターチェックを実行します。システムが AAA サーバーと通信できないことを示す SNMP トラップ（**starSRPAAAUnreachable**）が存在するかどうかを確認します。

手順

ステップ 1 Exec モードコマンドの **show snmp trap history |grep starSRPAAAUnreachable** を実行します。

ステップ 2 このコマンドの出力がないか、または（イベントタイムスタンプに基づいて）最新の SNMP トラップ通知がないはずです。

ステップ 3 アクティブなシステムが 1 つ以上の AAA サーバーと通信できない場合、詳細については「AAA モニター」を参照してください。

ソフトウェア更新の実行

バックアップ（スタンバイ）システムにログインし、次のタスクを繰り返してバックアップ（スタンバイ）システムのアップグレードプロセスを実行します。

- ブートレコードの更新 （40 ページ）
- StarOS の再起動 （41 ページ）
- 設定ファイルの更新 （41 ページ）
- ソフトウェアバージョンの確認 （41 ページ）
- 設定ファイルの保存 （42 ページ）
- ファイルシステムの同期 （41 ページ）
- 正常性チェックの実行 （39 ページ）
- SRP チェックの実施 （39 ページ）
- BGP チェックの実施 （40 ページ）

• セッションの同期の待機 （42 ページ）

SRP スイッチオーバーの開始

この SRP スイッチオーバーは、プライマリシステムをアクティブモードにして、バックアップシステムをスタンバイに戻します。プライマリシャーシが、アップグレードされたソフトウェアとのセッションを処理するようになりました。

手順

ステップ 1 バックアップシャーシで、**srp initiate-switchover** コマンドを実行します。既存のすべてのセッションは、新しいセッション要求の処理を開始するプライマリシャーシに移行されます。スイッチオーバープロセスが完了するのを許可します。

ステップ 2 バックアップシステムで、**show srp info** コマンドを実行します。スイッチオーバーが完了すると、シャーシの状態は [Standby] を示します。

ステップ 3 プライマリシステムで、**show srp info** コマンドを実行して、スイッチオーバーが完了していることを確認します。スイッチオーバーが完了すると、シャーシの状態は [Active] を示します。

テストコールの実施

シャーシの状態が確認され、サブスクライバが移行されたら、新しい発信テストを実行してコールが成功したことを確認します。

フォールバック手順

以前の設定とソフトウェアビルドに戻すには、管理者権限を持つユーザーが次の手順を実行します。

手順

ステップ 1 Exec モードの **show boot** コマンドを実行します。表示される最上位の最小番号のエントリは、新しいソフトウェアビルドが搭載された新しい設定である必要があります。2 番目の最上位エントリはバックアップ設定である必要があります。

ステップ 2 最上位の起動エントリ n を削除し、管理カード間で設定を同期します。

```
[local]host_name# config
[local]host_name(config)# no boot system priority n
[local]host_name(config)# end
[local]host_name# filesystem synchronize all
```

ステップ 3 システムを再起動して、以前の設定をロードします。

```
[local]host_name# reload
```

ステップ 4 の説明に従って、正常性チェックを実行します。 正常性チェックの実行 （39 ページ）

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。