



N+2 UP リカバリ

- [変更履歴, on page 1](#)
- [機能説明, on page 1](#)
- [機能の仕組み, on page 4](#)
- [N+2 UP リカバリの設定, on page 22](#)
- [モニタリングおよびトラブルシューティング, on page 24](#)

変更履歴

マニュアルの変更履歴



Note 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

3GPP に従い、CP は UP からの Sx キープアライブメッセージ応答に依存する Sx ベースの障害検出を使用します。

このアプローチでは、CP は UP からの応答が受信されない場合、その UP をダウン状態と宣言してセッションの切断を開始する前に、一定の回数（設定可能） Sx メッセージを再送信します。信頼性の高い方法で UP のダウン状態を判別するため、再試行の回数と再試行の間隔によっては、障害検出期間が 10 秒以上になる場合があります。Sx パス障害が CP で検出されるまで、CP は引き続き失敗した UP を選択し、失敗した UP に UE からの新しい PDN 接続を配置します。

CP による UP のダウン状態の検出にかかる時間を短縮するため、Cisco CP は Bidirectional Forwarding Detection (BFD) プロトコル (RFC 5883 - Bidirectional Forwarding Protocol Detection (BFD) for Multihop Paths) を使用するように設定できます。

BFD は大幅に短い再試行期間 (約 200 ミリ秒) を使用するため、より迅速な UP ダウン検出が可能です。他の展開シナリオ (UP の 1:1 冗長性など) の Sx キープアライブメカニズムに加えて、これを使用できます。

注：PFD は共通する Day-N 設定を UP 全体にプッシュするため、この機能はパケットフローの記述 (PFD) に依存しません。

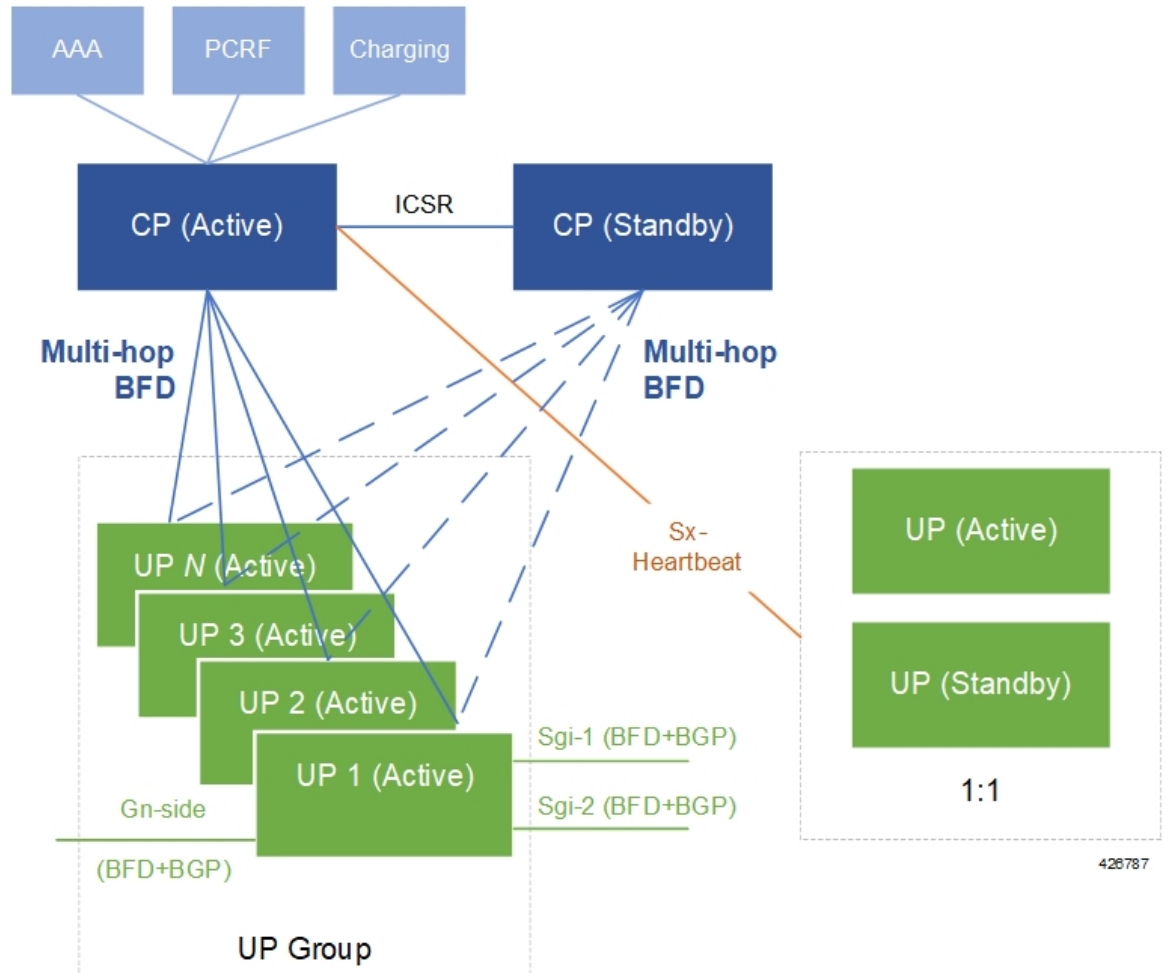
導入アーキテクチャ

この機能は、データセッションを処理する UP の「N+2」展開シナリオでのみ有効にできます。このシナリオでは、CP はアクティブ/スタンバイペアとして展開されます。「N」個のアクティブな UP を展開して CP と通信できます。展開した UP はすべて、デフォルト以外の特定の UP グループに含まれている必要があります。

注：N+2 では、すべての UP がアクティブなため、この機能はデータの UP リカバリ時間を短縮するためにのみ機能し、冗長性モデルではありません。IMS トラフィックを処理する UP は、1:1 冗長性モデルでのみ展開することを強く推奨します。

CP と UP 間の BFD 通信には、CP/UP ごとに 1 つの追加のループバック IP アドレスを設定する必要があります。

Figure 1: N+2 展開での BFD モニタリング



制限事項

- BFD ベースの CP 障害検出は、このリリースではサポートされていません。CP 障害は、Sx パス障害検出の既存のメカニズムを UP で使用して引き続き検出できます。
注：古い UP セッションをより迅速に防ぐために、Sx パス障害タイマーをより積極的に設定することを推奨します。
- UP の Gi/Gn インターフェイスでの BGP モニタリングはサポートされていません。
- マルチ BFD はサポートされていません。
- BFD は、CP と UP の両方で Sx が設定されているのと同じコンテキスト（Gn 側）で設定する必要があります。

機能の仕組み

次の図と表に、UP がダウンと検出された場合のセッションの切断および再接続プロセスの概要を示します。

Figure 2: N+2 UP リカバリフロー

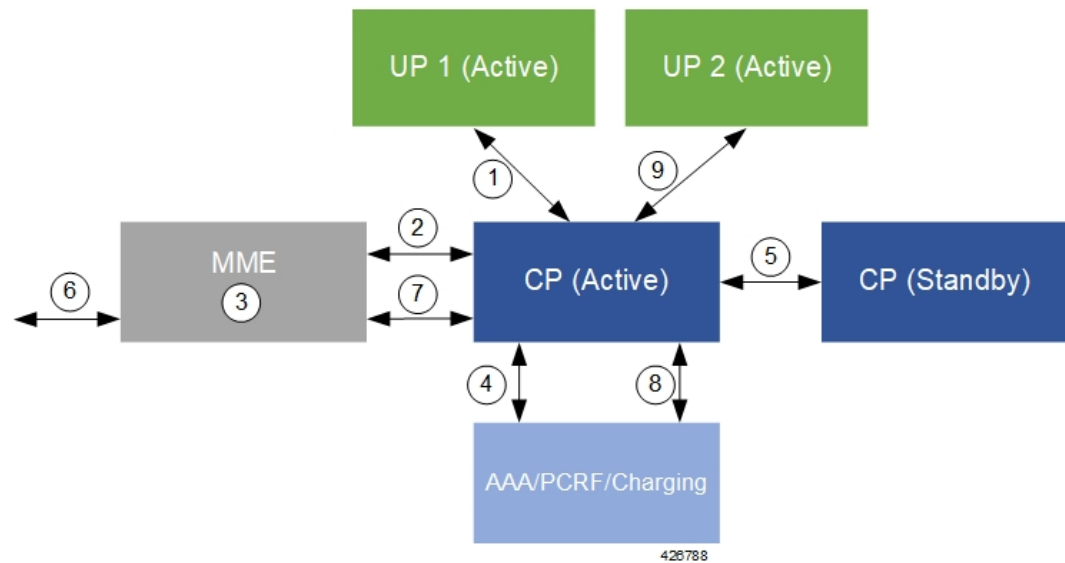


Table 1: N+2 UP リカバリフロー

ケース	説明
1	CP が UP 障害を検出します。
2	CP は、原因コードが Local-Detach の UP 切断セッションメッセージを MME に送信します。
3	MME は要求を処理し、セッションを切断します。
4	CP は、AAA/PCRF/課金インフラストラクチャと通信して、セッションを切断します。
5	CP (アクティブ) はスタンバイ CP と通信して、UP 切断のチェックポイント処理を実行します。
6	以前にセッションが切断された UE は、MME に再接続します。
7	MME は CP と通信して、UE セッションを再接続します。
8	CP は、AAA/PCRF/課金インフラストラクチャと通信して、セッションを再接続します。
9	CP は、代替アクティブ UP を使用して Sx インターフェイスを介してセッション再接続プロセスを完了します。

SAEGW CP/UP、P-GW CP/UP、S-GW CP/UP、および GnGp GGSN CP/UP のパス障害フローの切り離しと再アタッチの詳細については、次の項を参照してください。

コールフロー

パス障害発生時の SAEGW の接続解除および再接続

次の図と表で、SAEGW CP および UP のパス障害発生時の接続解除および再接続プロセスについて説明します。

Figure 3: パス障害発生時の SAEGW CP/UP 接続解除および再接続プロセス

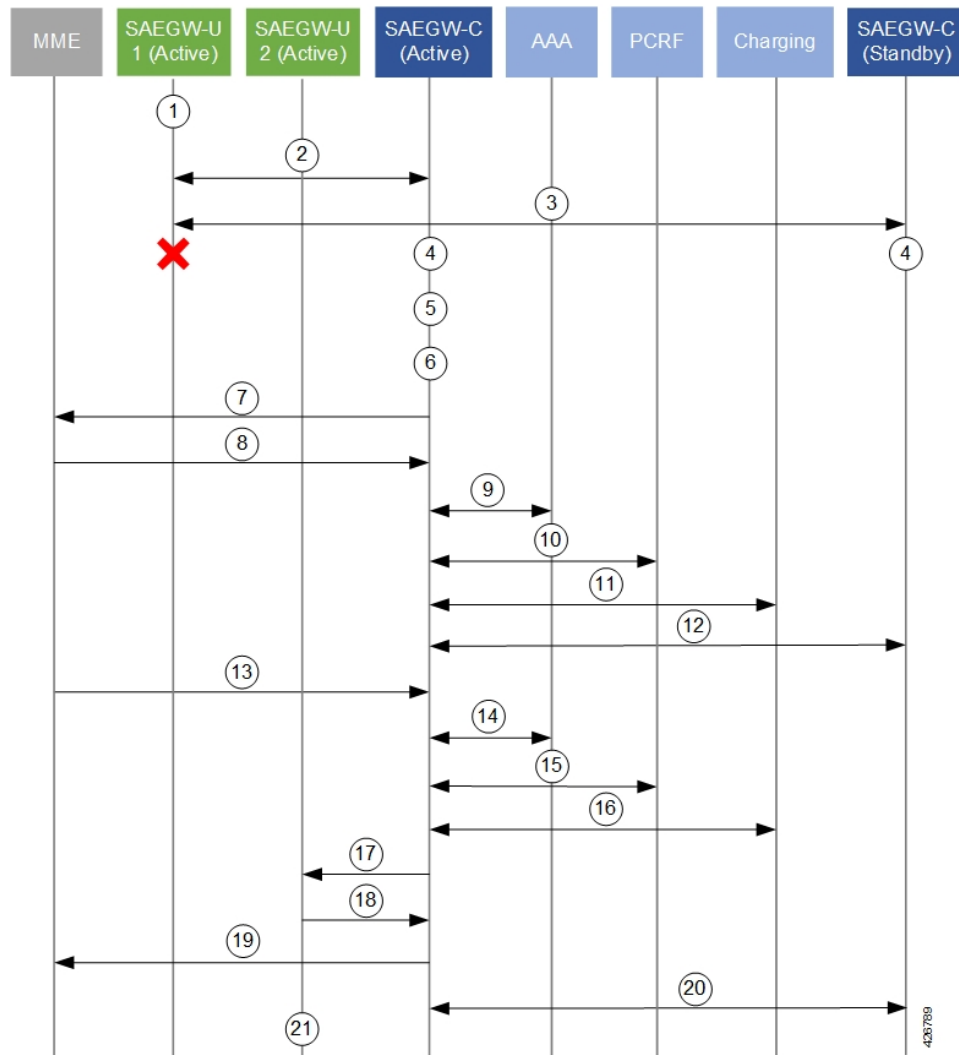


Table 2: パス障害発生時の SAEGW CP/UP 接続解除および再接続プロセス

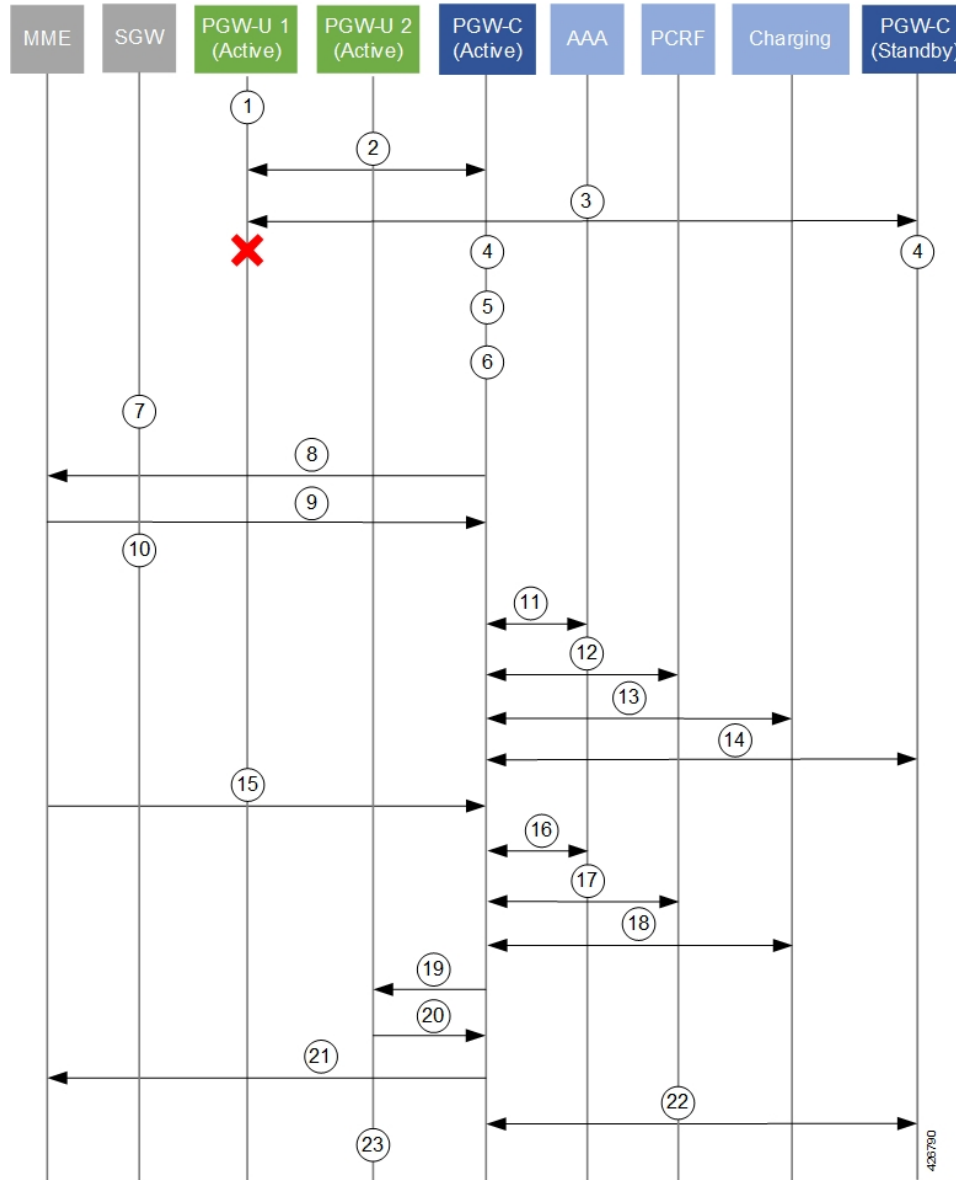
ケース	説明
1	UE データセッションは、アクティブな SAEGW UP によって処理されます。
2	アクティブ SAEGW CP は、BFD および Sx-Heartbeat メッセージを介して SAEGW UP をモニターします。
3	セカンダリ CP も、BFD を介して SAEGW UP をモニターします。
4	アクティブ CP とスタンバイ CP が、eNB 検出 (Sx タイマー (間隔、再送信、タイムアウト) のリレー) の前に、UP で BFD 障害を検出します。
5	アクティブ CP の BFD/VPNMGR が、Sx-demux プロセスに BFDDown イベントを通知します。
6	アクティブ CP 上の Sx-demux プロセスが、CP 上のすべてのセッションマネージャに対するパス障害通知を開始します。
7	すべてのセッションマネージャは、MME に Local-Detach の原因を含む Delete-bearer-req メッセージを送信することで、セッションの接続解除プロセスを開始します。事前定義されたレートで接続解除が開始されます。
8	MME が Delete-bearer-resp メッセージを CP に送り返します。 MME はセッションが切断されているアイドル状態の UE をページングしません。 また、セッションが切断されているアクティブな UE に E-RAB リリースメッセージを送信します。
9	アクティブ CP が、AAA サーバーとのセッションを解放します。
10	アクティブ CP が、PCRF とのセッションを解放します。
11	アクティブ CP が、課金インフラストラクチャとのセッションを解放します。
12	アクティブ CP が、セッション切断情報をセカンダリ CP と同期します。
13	UE がセッションを再開する場合、MME がアクティブ CP に Create-session-request メッセージを送信します。 MME が負荷アルゴリズム (DNS、ローカル設定など) に基づいて CP を選択します。
14	アクティブ CP が、AAA サーバーとのセッション接続要求を処理します。
15	アクティブ CP が、PCRF を使用してセッション接続要求を処理します。
16	アクティブ CP が、課金インフラストラクチャとのセッション接続要求を処理します。
17	アクティブ CP が、代替アクティブ UP に Sx セッション確立要求メッセージを送信します。 CP が負荷アルゴリズムに基づいて UP を選択します。

ケース	説明
18	UP が Sx セッション確立応答メッセージを CP に送り返します。
19	CP が Create-session-response メッセージを MME に送信します。
20	アクティブ CP が、新しく接続されたセッションの情報をセカンダリ CP と同期します。
21	これで、UE データセッションがアクティブな SAEGW UP によって処理されます。

パス障害時の P-GW の切断と再接続

次の図と表は、P-GW CP および UP のパス障害時の切断および再接続プロセスを示しています。

Figure 4: パス障害時の P-GW CP/UP 切断および再接続プロセス



パス障害時の P-GW CP/UP 切断および再接続プロセス

Table 3: パス障害時の P-GW CP/UP 切断および再接続プロセス

ケース	説明
1	UE データセッションが、アクティブな P-GW UP によって処理されます。
2	アクティブな P-GW CP が、BFD および Sx ハートビートメッセージを介して P-GW UP をモニターします。
3	セカンダリ CP が、BFD を介して P-GW UP もモニターします。

ケース	説明
4	アクティブ CP とスタンバイ CP が、eNB 検出 (Sx タイマー (間隔、再送信、タイムアウト) のリレー) の前に、UP で BFD 障害を検出します。
5	アクティブ CP の BFD/VPNMGR が、Sx-demux プロセスに BFDDown イベントを通知します。
6	アクティブ CP 上の Sx-demux プロセスが、CP 上のすべてのセッションマネージャへのパス障害通知を開始します。
7	S-GW が MME に対して db-req を開始します。
8	すべてのセッションマネージャが、MME に Local-Detach の原因を含む Delete-bearer-req メッセージを送信することで、セッションの切断プロセスを開始します。事前定義されたレートで切断が開始されます。
9	MME が Delete-bearer-resp メッセージを CP に送り返します。 MME はセッションが切断されているアイドル状態の UE をページングしません。 また、セッションが切断されているアクティブな UE に E-RAB リリースメッセージを送信します。
10	S-GW が db-resp を PGW-C に転送し、その PDN セッションを削除します。
11	アクティブ CP が、AAA サーバーとのセッションを解放します。
12	アクティブ CP が、PCRF とのセッションを解放します。
13	アクティブ CP が、課金インフラストラクチャとのセッションを解放します。
14	アクティブ CP が、セッション切断情報をセカンダリ CP と同期します。
15	セッションを再開する UE の場合、MME がアクティブ CP に Create-session-request メッセージを送信します。 MME が負荷アルゴリズム (DNS、ローカル設定など) に基づいて CP を選択します。
16	アクティブ CP が、AAA サーバーとのセッション接続要求を処理します。
17	アクティブ CP が、PCRF を使用してセッション接続要求を処理します。
18	アクティブ CP が、課金インフラストラクチャとのセッション接続要求を処理します。
19	アクティブ CP が、代替アクティブ UP に Sx セッション確立要求メッセージを送信します。 CP が負荷アルゴリズムに基づいて UP を選択します。
20	UP が Sx セッション確立応答メッセージを CP に送り返します。
21	CP が Create-session-response メッセージを MME に送信します。

ケース	説明
22	アクティブ CP が、新しく接続されたセッションの情報をセカンダリ CP と同期します。
23	これで、UE データセッションがアクティブな SAEGW UP によって処理されます。

パス障害時の S-GW の切断と再接続

次の図と表は、S-GW CP および UP のパス障害時の切断および再接続のプロセスフローを示しています。

Figure 5: パス障害時の S-GW CP/UP の切断と再接続プロセス

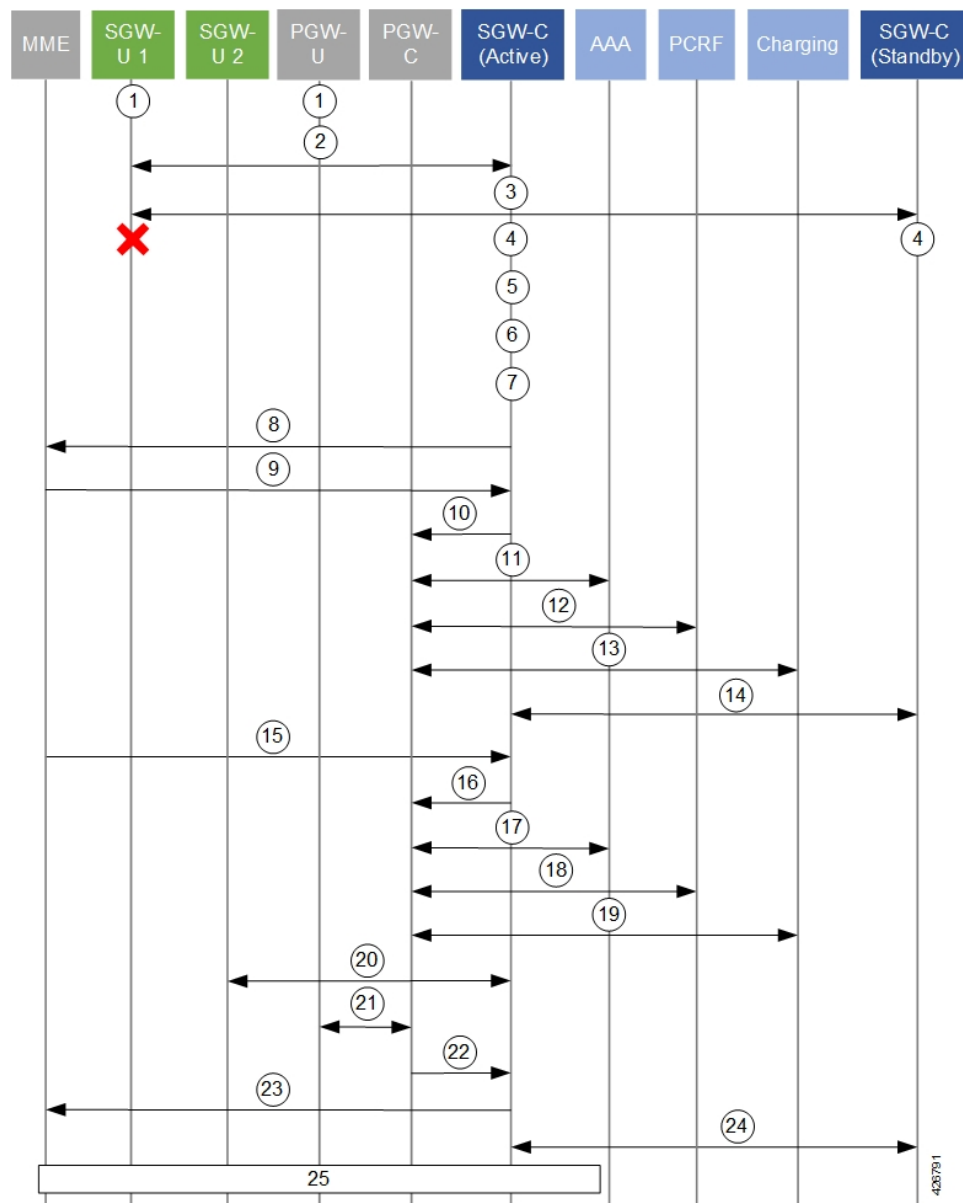


Table 4: パス障害時の S-GW CP/UP の切断と再接続プロセス

ケース	説明
1	アクティブ S-GW UP およびアクティブ PGW UP は、UE データセッションを処理します。
2	アクティブ S-GW CP は、BFD および Sx ハートビートメッセージを介して S-GW UP をモニターします。
3	セカンダリ S-GW CP も BFD を介して S-GW UP をモニターします。
4	アクティブ S-GW CP とスタンバイ S-GW CP は、eNB 検出 (Sx タイマー (間隔、再送信、タイムアウト) のリレー) の前に、S-GW UP で BFD 障害を検出します。
5	アクティブ S-GW CP 上の BFD/VPNMGR は、Sx-demux プロセスに BFDDown イベントを通知します。
6	アクティブ CP 上の Sx-demux プロセスは、CP 上のすべてのセッションマネージャへのパス障害通知を開始します。
7	S-GW CP は MME に対して db-req を開始します。
8	すべてのセッションマネージャは、MME にローカル切断の原因を含む ベアラー削除要求メッセージを送信することで、セッションの切断プロセスを開始します。事前定義されたレートで切断が開始されます。
9	MME はベアラー削除応答メッセージを S-GW CP に送り返します。 MME はセッションが切断されているアイドル状態の UE をページングしません。 また、セッションが切断されているアクティブな UE に E-RAB リリースメッセージを送信します。
10	アクティブ S-GW CP は、PGW UP を使用してセッションを解放します。
11	PGW CP は AAA サーバーとのセッションを解放します。
12	PGW CP は PCRF とのセッションを解放します。
13	PGW CP は、課金インフラストラクチャとのセッションを解放します。
14	アクティブ S-GW CP は、セッション切断情報をセカンダリ S-GW CP と同期します。
15	セッションを再開する UE の場合、MME がアクティブな S-GW CP にセッション作成要求メッセージを送信します。 MME は負荷アルゴリズム (DNS、ローカル設定など) に基づいて CP を選択します。
16	アクティブ S-GW CP は、セッション作成要求メッセージを PGW CP にリレーします。
17	PGW CP は、AAA サーバーとのセッション接続要求を処理します。
18	PGW CP は、PCRF を使用してセッション接続要求を処理します。

ケース	説明
19	PGW CP は、課金インフラストラクチャとのセッション接続要求を処理します。
20	アクティブ S-GW CP は、代替のアクティブ S-GW UP と Sx セッション確立要求および応答メッセージを交換します。
21	アクティブ PGW CP は、アクティブ PGW UP と Sx セッション確立要求および応答メッセージを交換します。
22	PGW CP は、セッション作成応答メッセージを S-GW CP に送信します。
23	S-GW CP は、セッション作成応答メッセージを MME に送信します。
24	アクティブ S-GW CP は、新しく接続されたセッションの情報をセカンダリ S-GW CP と同期します。
25	UE データがアクティブ UP を通過する前に、S-GW CP とは、MME と連携してベアラ変更要求手順を完了します。

パス障害時の GnP GGSN の切断と再接続

次の図と表は、GnP GGSN CP および UP のパス障害時の切断および再接続プロセスフローを示しています。

Figure 6: パス障害時の GnP GGSN CP/UP 切断および再接続プロセス

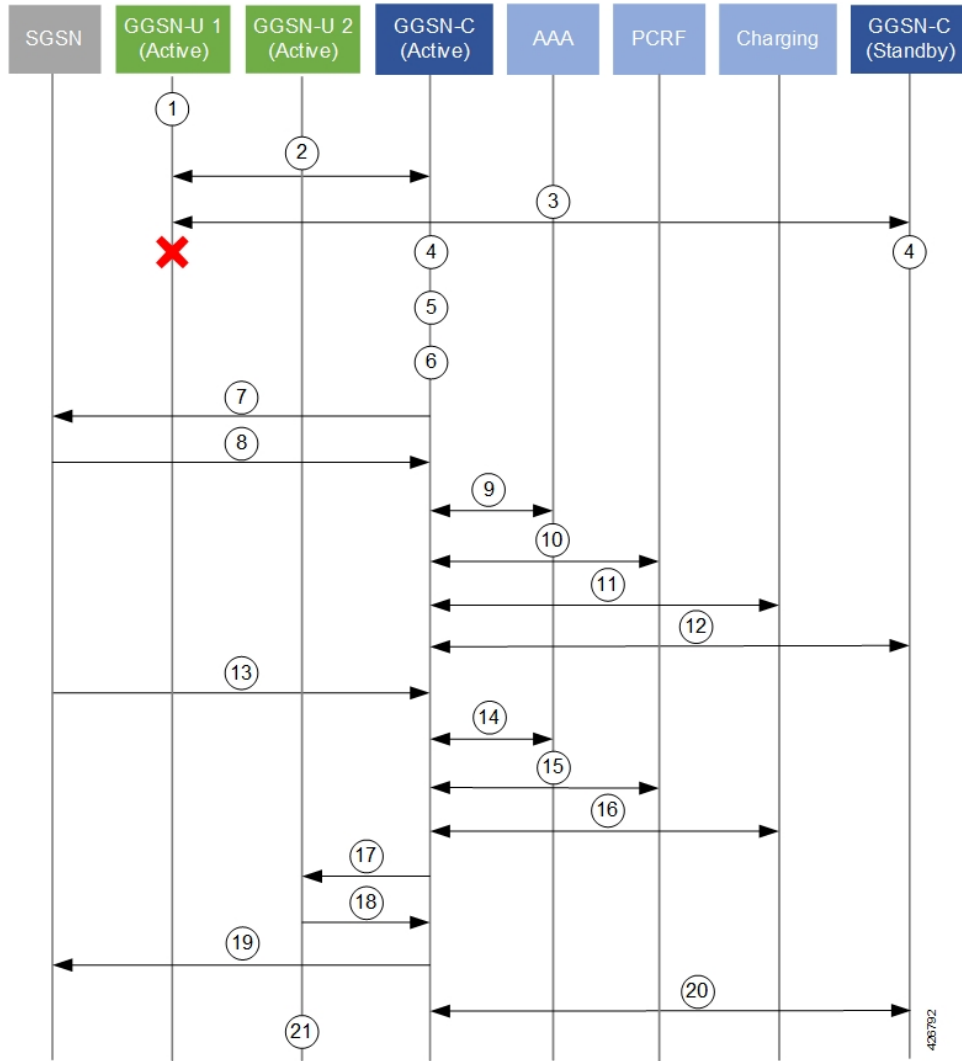


Table 5: パス障害時の GnP GGSN CP/UP 切断および再接続プロセス

ケース	説明
1	アクティブ GGSN UP は、UE データセッションを処理します。
2	アクティブ GGSN CP は、BFD および Sx ハートビートメッセージを介して GGSN UP をモニターします。
3	セカンダリ CP も BFD を介して GGSN UP をモニターします。
4	アクティブ CP とスタンバイ CP は、eNB 検出 (Sx タイマー (間隔、再送信、タイムアウト) のリレー) の前に、UP で BFD 障害を検出します。
5	アクティブ CP 上の BFD/VPNMGR は、Sx-demux プロセスに BFDDown イベントを通知します。

ケース	説明
6	アクティブ CP 上の Sx-demux プロセスは、CP 上のすべてのセッションマネージャへのパス障害通知を開始します。
7	すべてのセッションマネージャは、原因コードを含まない Delete-pdp-context-req メッセージを SGSN に送信することによって、セッションの切断プロセスを開始します。事前定義されたレートで切断が開始されます。
8	SGSN は Delete-pdp-context-resp メッセージを CP に送り返します。 SGSN はセッションが切断されているアイドル状態の UE をページングしません。 また、セッションが切断されているアクティブな UE に E-RAB 解放メッセージを送信します。
9	アクティブ CP は AAA サーバーとのセッションを解放します。
10	アクティブ CP は PCRF とのセッションを解放します。
11	アクティブ CP は課金インフラストラクチャとのセッションを解放します。
12	アクティブ CP はセッション切断情報をセカンダリ CP と同期します。
13	セッションを再開する UE の場合、SGSN はアクティブ CP に Create-pdp-request メッセージを送信します。 SGSN はロードアルゴリズム（DNS、ローカル設定など）に基づいて CP を選択します。
14	アクティブ CP は、AAA サーバーとのセッション接続要求を処理します。
15	アクティブ CP は、PCRF を使用してセッション接続要求を処理します。
16	アクティブ CP は、課金インフラストラクチャとのセッション接続要求を処理します。
17	アクティブ CP は、代替アクティブ UP に Sx セッション確立要求メッセージを送信します。 CP は負荷アルゴリズムに基づいて UP を選択します。
18	UP は Sx セッション確立応答メッセージを CP に送り返します。
19	CP は Create-pdp-context 応答メッセージを SGSN に送信します。
20	アクティブ CP は、新しく接続されたセッションの情報をセカンダリ CP と同期します。
21	これで、UE データセッションがアクティブな GGSN UP によって処理されます。

追加の N+2 処理シナリオ

前の項で説明したフロー以外に、N+2 が設定されたさまざまな条件下でのネットワーク機能 (NF) やシステムの動作について次の表で説明します。

Table 6: N+2 処理シナリオ

ID	シナリオ	ハンドル	注意
1	アクティブ UP がクラッシュ	<p>アクティブ CP が UP で BFD 障害を検出すると、その UP に属するセッションを切断します。</p> <p>アクティブ CP は、SRP を介してスタンバイ CP に切断を伝達します。</p> <p>UP がアクティブに戻ると、アクティブ CP に再度関連付けられます。</p>	<p>検出は BFD タイムアウト間隔内で実行されます。</p> <p>CP Sx は BFD をモニターします。</p>
2	アクティブ CP がクラッシュ	<p>アクティブ CP がスタンバイ CP に切り替わります。</p> <p>アクティブ UP は、アクティブ CP とスタンバイ CP の両方の Sx ハートビートセッションをモニターします。</p> <p>アクティブ UP は、ICSR フェールオーバー時間に達するまでセッションを消去しません。</p>	<p>スタンバイ CP はフェールオーバー時に Sx ハートビートの送信を開始します。アクティブ UP によってセッションが消去されることはありません。</p>
3	スタンバイ CP がクラッシュ	<p>スタンバイ CP が起動し、アクティブ CP でチェックポイント処理を実行してセッションを回復します。</p>	<p>アクティブ CP とアクティブ UP のセッションはそのまま残ります。</p>

ID	シナリオ	ハンドル	注意
4	<p>アクティブ CP とアクティブ UP 間でネットワークフラップが発生し。スタンバイ CP とアクティブ UP 間のネットワークは稼働中</p>	<p>アクティブ CP は、UP の BFD-Down を検出すると、セッション切断プロセスを開始し、UP の関連付けを解除します。</p> <p>アクティブ CP は、SRP を介してスタンバイ CP に切断を伝達します。</p> <p>アクティブ UP は、アクティブ CP を使用して Sx ハートビートをモニターします。</p> <p>アクティブ UP は、設定された Sx ハートビート/パス障害検出タイムアウトが発生する（SRP スイッチオーバー時間を超える）まで待機してから、セッションをクリアします。</p>	
5	<p>スタンバイ CP とアクティブ UP 間でネットワークフラップが発生し。アクティブ CP とアクティブ UP Sx ハートビートもダウン</p>	<p>アクティブ UP が Sx パス障害を検出します。</p> <p>アクティブ UP は、設定された Sx ハートビート/パス障害検出タイムアウトが発生する（SRP スイッチオーバー時間を超える）まで待機してから、セッションをクリアします。</p> <p>アクティブ CP は、UP の BFD-Down を検出すると、セッション切断プロセスを開始し、UP の関連付けを解除します。</p>	<p>UP は、Sx ハートビートのタイムアウトによりセッションを削除します。</p>

ID	シナリオ	ハンドル	注意
6	スタンバイ CP とアクティブ UP 間でネットワークフラップが発生し、アクティブ CP とアクティブ UP 間のネットワークは稼働中	スタンバイ CP は正常に動作します。 アクティブ CP-active は動作中で、ハートビートに反応します。 アクティブ UP は正常に動作します。	
7	Sx は到達不能だが、BFD は到達可能	アクティブ UP が Sx パス障害を検出します。 アクティブ UP は、設定された Sx ハートビート/パス障害検出タイムアウトが発生する (SRP スイッチオーバー時間を超える) まで待機してから、セッションをクリアします。 アクティブ CP は、UP の Sx パス障害を検出すると、セッション切断プロセスを開始し、UP の関連付けを解除します。	現在の動作ごとに Sx パス障害として扱われるコーナーケース (N+2 の前)。
8	アクティブ CP とスタンバイ CP 間で ICSR リンクがダウンし、スタンバイ CP もアクティブになる (デュアルアクティブの場合)	デュアルアクティブになると、スタンバイ CP はより高いメトリックでアクティブ UP にメッセージを送信します。	デュアルアクティブ構成のスタンバイ CP によってアドバタイズされるすべてのサービスで、IP のメトリックが高くなります。
9	アクティブ UP の BGP 障害の Gn 側	N+2 に関連するアクションは実行されません。	
10	アクティブ UP の BGP 障害の SGI 側	N+2 に関連するアクションは実行されません。	
11	アクティブ UP で SessMgr がクラッシュ	セッション回復プロセスがアクティブ UP で発生します。	

ID	シナリオ	ハンドル	注意
12	アクティブ UP で Sx-demux がクラッシュ	Sx-demux 回復プロセスがアクティブ UP で発生します。	
13	アクティブ UP で VPP がクラッシュ	NPUMgr が UP を再起動すると、BFD 損失が発生し、UP 障害検出がトリガーされます。 この表の ID 1 および 5 の処理に関する情報を参照してください。	
14	アクティブ UP で VPNMgr がクラッシュ	VPNMgr 回復プロセスがアクティブ UP で発生します。	
15	アクティブ UP で BFD がクラッシュ	BFD 回復プロセスがアクティブ UP で発生します。	
16	アクティブ CP で Sx-demux がクラッシュ	Sx-demux 回復プロセスがアクティブ CP で発生します。 Sx-demux は、リカバリの一環として CP とすべでの UP 間の BFD を再登録し、各 UP の状態を再検出します。 Sx-demux は SessMgr から再起動タイムスタンプを回復します。	アクティブ CP での Sx-demux リカバリ中に UP 状態の遷移が発生する可能性があります（たとえば、UP は再起動しますが、リカバリ後に CP に対してアクティブと示されません）。 次の状態が検出されます。 <ul style="list-style-type: none"> • Sx-demux が回復し、CP が Sx ハートビートまたは UP 障害から UP 再起動タイムスタンプを検出します。 • アクティブ CP はこの情報に基づいて、セッションの消去を開始します。

ID	シナリオ	ハンドル	注意
17	アクティブ CP で VPNMgr がクラッシュ	VPNMgr 回復プロセスがアクティブ CP で発生します。 アクティブ CP の SCT から BFD 登録情報が回復されます。 アクティブ CP は UP で BFD を再起動します。	
18	アクティブ CP で BFD がクラッシュ	BFD 回復プロセスがアクティブ CP で発生します。	
19	アクティブ CP で SessMgr がクラッシュ	SessMgr 回復プロセスがアクティブ CP で発生します。	

二重障害処理シナリオ

N+2 二重障害シナリオは、BFD 障害の後に別のイベント/障害が発生した場合に発生します。このようなシナリオの処理については、次の表で説明します。

Table 7: N+2 二重障害シナリオの処理

ID	シナリオ	ハンドル	注意
1	セッションの接続解除中にアクティブ CP に障害が発生する	CP 間で ICSR スイッチオーバーが発生します。 スタンバイ CP がアクティブ CP になります。 アクティブ CP が BFD を介して UP 障害を検出します。 アクティブ CP が Sx ハートビートを介して UP の再起動を検出します。	影響： 二重障害で UP が再起動した場合、スタンバイ CP によるセッションの回復が完了していても、UP にはセッションがありません。 これらのセッションは、セッションの置換時または UE からのセッション接続解除時に消去されます。 UP が再起動しない場合、CP-new-active は障害が発生した UP のセッションをクリアします。

ID	シナリオ	ハンドル	注意
2	セッションの接続解除中にスタンバイ CP に障害が発生する	スタンバイ CP は、アクティブ CP の状態情報のチェックポイントを生成します。 削除されたセッションに関する情報は、アクティブ CP から無効化されます。	
3	アクティブ CP がルータフラップによる UP 障害と判断する。アクティブ CP がセッションの接続解除を開始した後に UP BFD を受信する	まず UP BFD のダウン状態が検出され、すべてのセッションが接続解除されます。	

BFD フラッピングと VPC

N+2 は BFD を使用して、セッションエンドポイント間のネットワークパスの存在や実行可能性をモニターします。ループバックエンドポイントでマルチホップ BFD を使用することで、BFD セッション状態は、接続先のシステム状態のプロキシとして機能します。

ただし、相手側のシステム障害以外の理由（ARP ストームやルータの設定不備など）で、BFD セッションがダウンしたり、バウンス/フラップしたりする可能性があります。中断が大変深刻で長期間続く場合、両方のシステムが機能していても、両側のシステムで BFD セッション障害が検出される可能性があります。

設定を調整することで、このようなイベントの発生をオフセットできます。

次の推奨事項は、NF が展開されているプラットフォームに基づいて提供されます。

- VPC-SI : BFD マルチホップピア設定を調整して、BFD 検出時間を 2〜3 秒に増やし、それに応じて再試行回数を増やします。
- VPC-DI : CF スイッチオーバーと SF 移行により、BFD パケットの生成と処理が数秒間中断される可能性があります。これらのイベントが発生したときに BFD セッションのフラップが発生しないようにするには、VPC-DI システムが関わるセッションの BFD 検出時間を 7 秒以上に設定する必要があります。

Sx 関連付けのシナリオ

次の表に、N+2 を使用する場合の CP と UP の関連付けと関連付け解除に関する情報を示します。

Table 8: N+2 Sx 関連付けのシナリオ

シナリオ	メカニズム
UP から CP への Sx 関連付け解除	<ul style="list-style-type: none"> • Sx-demux が VPNMgr を使って BFD モニタリングを無効にする • SAEGW サービスが削除される • UP からの Sx 関連付け解除
UP の追加	<p>Day-0 の一環として :</p> <ul style="list-style-type: none"> • UP の BFD ループバックアドレスを追加する。 • CP で BFD を設定する。 • UP グループを追加し、CP で選択できるように設定する。
UP の削除	<p>CP で CLI コマンドを実行して、UP の IP アドレスを使ってサブスクライバをクリアし、その UP に振り向けられる新しいセッションをブロックするキーワードを指定します。</p> <ul style="list-style-type: none"> • UP 上ですべてのサブスクライバが切断されていることを確認する。 • UP で、CLI コマンドを実行して CP との関連付けを解除する。CP から UP の関連付けが解除され、CP では以降のセッションにこの UP を選択しない。すべてのセッションが切断されていることを確認する。 • CP で、UP グループから UP を削除する。 • CP で、UP グループから UP を削除する CLI コマンドを実行する (UP の BFD モニタリングも登録解除される)。 • UP および CP で BFD のモニタリング設定を無効にする。このときの CLI コマンドは no monitor-group。
UP によって開始された Sx 関連付け	CP の Sx-demux は、VPNMGr からの BFDUp および BFDDown 通知の処理を開始する。
UP によって解放された Sx 関連付け	CP の Sx-demux は、VPNMGr からの BFDUp および BFDDown 通知を無視する。

N+2 および IP アドレス指定

ループバック IP アドレス

N+2 に関連する BFD ループバックアドレスには、次のことが当てはまります。

- アクティブ CP およびスタンバイ CP の BFD ループバック IP アドレスは、Day-0 に設定する必要があります。
- BFD は、アクティブ CP とアクティブ UP の間、およびスタンバイ CP とアクティブ UP の間で動作します。そのため、3 つのコンポーネントすべてで一意的な BFD ループバック IP アドレスを使用する必要があります。
- CP および UP ごとに設定された BFD ループバック IP アドレスは、Sx インターフェイスに使用されるアドレスとは異なる必要があります。また、CP の場合は、SRP インターフェイスに使用されるアドレスとも異なる必要があります。

IP アドレスの可用性

N+2 展開シナリオでは、UE は高いレート（切断レートと同等）で再接続できます。このプロセスを円滑に進めるには、十分な数の IP アドレスが UP で使用可能になっている必要があります。

CUPS IP プール管理には、アドレスの「チャンク」を使用して UP をプロビジョニングする機能が含まれています。CP で設定したチャンクサイズとプールの数は、CP から UP への高い再接続レートに比例して増やす必要があります。IP アドレスが使用できないことが原因でセッションが UP によって拒否されないようにするためです。

予測される再接続レートは、UP セッションを処理するセッションマネージャのタスク数に 1000 セッション/秒を掛けて概算できます。

アドレスキャパシティは、チャンクのサイズ（16～8192）と IP プールの数を掛けて決定されます。両方ともに CP で設定されます。

N+2 UP リカバリの設定

N+2 UP リカバリを設定するには、次の手順を実行します。

1. CP および UP で BFD を設定します。

```
configure
  context bfd_context_name
    ip route static multihop bfd mhbfd_session_name
    local_endpoint_ip_address remote_endpoint_ip_address
    bfd-protocol
      bfd multihop-peer dst_ip_address interval tx_interval min_rx
      rx_interval multiplier value
    #exit
  #exit
```

注：

- *bfd_ctx_name* は、BFD を設定するコンテキストの名前です。これは、Sx が設定されているコンテキストと同じである必要があります。

- *mhbfd_session_name* は BFD セッションルートの名前です。ピア接続ごとに1つずつ、複数のセッションルートを作成できます。
- *local_endpoint_ip_address* は、現在のコンテキストのローカルインターフェイスに対応する IPv4 または IPv6 アドレスです。
- *remote_endpoint_ip_address* は、リモート BFD ピアに対応する IPv4 または IPv6 アドレスです。
 - このルートが CP で設定されている場合、リモートアドレスはピア UP のリモートアドレスになります。
 - このルートが UP で設定されている場合、リモートアドレスはピア CP のリモートアドレスになります。
- *dst_ip_address* は、リモート BFD ピアに対応する IPv4 または IPv6 アドレスです。これは、スタティックマルチホップ BFD ルート用に設定された *remote_endpoint_ip_address* インターフェイスと同じである必要があります。リモートピアごとに1つずつ、複数のピアを設定できます。
- **interval** *tx_interval* は、BFD パケット間の送信間隔（ミリ秒単位）です。
- **min_rx** *rx_interval* は、BFD パケット間の最小受信間隔（ミリ秒単位）です。
- **multiplier** *value* はホールドダウンを計算するために使用する乗数値です。
- 検出時間（X）を決定するには、次の計算を使用できます。
 検出時間（X） = **interval** *tx_interval* * **multiplier** 値
 検出時間（X）の推奨値は、VPC-SI の場合は 3 秒、VPC-DI の場合は 7 秒です。

2. CP および UP でコンテキストごとに BFD ループバックを設定します。

```
configure
context monitor_ctx_name
  monitor-protocols
    monitor-group monitor_group_name protocol bfd
      session-ctx session_ctx_name local-addr { ipv4_address |
ipv6_address } remote-address { ipv4_address | ipv6_address }
    #exit
```

注：

- *Monitor_ctx_name* は、BFD モニタリングを設定するコンテキストの名前です。これは、Sx が設定されているコンテキストと同じである必要があります。
- *Monitor_group_name* は、BFD モニタリングパラメータを指定するグループの名前です。複数のモニターグループを設定できます。
- *Session_ctx_name* は、BFD モニタリングが実行されるローカルインターフェイスを含むコンテキストの名前です。これは、Sx が設定されているコンテキストと同じである必要があります。

- **local-addr** { *ipv4_address* | *ipv6_address* } は、指定されたコンテキストのローカルインターフェイスに対応する IPv4 または IPv6 アドレスです。
- **remote-addr** { *ipv4_address* | *ipv6_address* } は、BFD モニタリングが実行されるリモートピアに対応する IPv4 または IPv6 アドレスです。
 - このモニターグループが CP で設定されている場合、リモートアドレスは UP グループのリモートアドレスになります。
 - このモニターグループが UP で設定されている場合、リモートアドレスは CP グループのリモートアドレスになります。

3. CP の特定の UP グループ内で BFD ループバック（リモート IP）を設定します。

```

configure
  user-plane-group up_group_name
    peer-node-id { ipv4_address | ipv6_address } monitor-group-name
    monitor_group_name
  #exit

```

注：

- *up_group_name* は、サポートされる N+2 UP リカバリのデータ UP を含む UP グループの名前です。
 - これをデフォルトグループにすることはできません。
 - このグループには、IMS/VoLTE をサポートするための UP を含めないでください。
- { *ipv4_address* | *ipv6_address* } は、UP グループに含めるアクティブ UP 上の Sx インターフェイスの IPv4 または IPv6 アドレスです。グループ内で複数のピアノードを設定できます。Sx インターフェイスは、BFD のモニタリングに使用されるインターフェイスとは異なることに注意してください。
- *monitor_group_name* は、UP が関連付けられるモニタリンググループの名前です。

モニタリングおよびトラブルシューティング

コマンドの表示

```
show sx peers { full address peer_ip_address | wide }
```

```
show sx peers full address peer_ip_address
```

指定したピアのモニター関連情報（VPN コンテキスト名、グループ名、状態など）を表示します。

show sx peers wide

「モニター状態」が表示されます。デフォルトの状態は、アップの場合は「U」、ダウンの場合は「D」、該当なしの場合は「N」です。

show sx-service statistics all

SNMP

次の SNMP トラップを使用して、N+2 UP リカバリの正常性をモニターできます。

- StarBFDSessUp (starentTraps 1276)
- StarBFDSessDown (starentTraps 1277)
- StarSxPathFailure (starentTraps 1382) : このトラップが更新され、新しい原因コード [bfd-failure(8)] が追加されました。
- StarSxPathFailureClear (starentTraps 1383)

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。