MPLS-TE 用の RSVP の実装

このモジュールでは、Cisco ASR 9000 シリーズ アグリゲーション サービス ルータでの MPLS トラフィック エンジニアリング（MPLS-TE）用のリソース予約プロトコル（RSVP）を実装する方法について説明します。

マルチプロトコル ラベル スイッチング（MPLS）は、Internet Engineering Task Force（IETF）が推進する標準ベースのソリューションで、インターネットおよびIPバックボーンをベストエフォート型ネットワークからビジネスクラスのトランスポート メディアに変換します。

リソース予約プロトコル（RSVP）は、システムによるネットワークからのリソース予約要求を可能にするシグナリング プロトコルです。 RSVP は、他のシステムからのプロトコル メッセージを処理し、ローカル クライアントからのリソース要求を処理して、プロトコル メッセージを生成します。 結果として、リソースは、ローカルおよびリモート クライアントの代わりにデータ フローに予約されます。 RSVP は、これらのリソース予約を作成、保守および削除します。

RSVP は、ネットワークへの Quality of Service（QoS）アクセスを制御する安全な方法を提供します。

MPLS トラフィック エンジニアリング（MPLS-TE）は、RSVP を使用して、ラベル スイッチ パス（LSP）をシグナリングします。

MPLS-TE 用 RSVP の実装機能の履歴

リリース	変更箇所
Release 3.7.2	この機能が導入されました。
Release 3.9.0	RSVP MIB 機能が追加されました。

MPLS-TE 用 RSVP の実装の前提条件

これらの前提条件は、MPLS-TE 用 RSVP の実装に必要です。

- You must be in a user group associated with a task group that includes the proper task IDs. The command reference guides include the task IDs required for each command. If you suspect user group assignment is preventing you from using a command, contact your AAA administrator for assistance.
- コンポジット ミニイメージおよび MPLS パッケージ、またはフル イメージのいずれかをインストールする必要があります。

MPLS-TE および用 RSVP の実装に関する情報

MPLS RSVP を実装するには、次の概念を理解する必要があります。

関連トピック

RSVP 認証の実装方法，（27 ページ）

MPLS-TE 用 RSVP の概要

RSVP は、インターネット アプリケーションによる MPLS-TE LSPのシグナリングを可能にするネットワーク制御プロトコルです。 RSVP 実装は、IETF RFC 2205、および RFC 3209に準拠します。

RSVP は、MPLS-TE が設定されるインターフェイスで自動的にイネーブルにされます。 非ゼロ帯域幅の MPLS-TE LSP では、RSVP 帯域幅は、インターフェイスで設定する必要があります。 すべての MPLS-TE LSP がゼロ帯域幅の場合、RSVP を設定する必要はありません。 O-UNI では、RSVP を設定する必要はありません。

RFC 2961 で定義されている RSVP リフレッシュ削減には、信頼できるメッセージおよびサマリー リフレッシュ メッセージのサポートが含まれます。 信頼できるメッセージは、メッセージが損失されるとすぐに再転送されます。 各サマリー リフレッシュ メッセージには、複数の状態をリフレッシュする情報が含まれるので、状態のリフレッシュに必要なメッセージングの量が大幅に削減されます。 2 つのルータ間でリフレッシュ削減を使用する場合、両方のルータでイネーブルにする必要があります。 リフレッシュ削減は、デフォルトでイネーブルです。

RSVP のメッセージ レート制限では、RSVP メッセージがインターフェイスで送信されるレートに最大しきい値を設定できます。 メッセージ レート制限は、デフォルトでディセーブルです。

RSVP を実装するプロセスは再起動が可能です。 ソフトウェア アップグレード、RSVP またはその任意のコラボレータのプロセス配置やプロセス障害は、データ プレーンのノンストップ フォワーディング（NSF）を保証します。

RSVP は、RFC 3473 に準拠するグレースフル リスタートをサポートします。 これは、ノードが設定済み再起動時間内でネイバーのコントロール プレーンとの通信を再確立するときに適用する手順を実行します。

RSVP はルーティング プロトコルではないため注意してください。 RSVP は、ルーティング プロトコルと機能し、ルーティングプロトコルにより計算されるルータで同等のダイナミック アクセス リストをインストールします。 このため、既存のネットワークで RSVP を実装する場合、新しいルーティング プロトコルに移行する必要はありません。

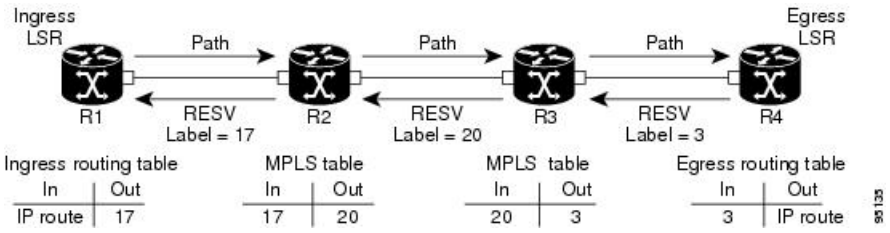
関連トピック

RSVP パケット ドロップの設定, （20 ページ）
RSVP パケットの DSCP の設定：例, （49 ページ）
RSVP 設定の確認, （22 ページ）

LSP 設定

LSP設定は、LSPヘッド ノードがパス メッセージをテール ノードに送信するときに開始されます（「RSVP オペレーション」の図を参照）。

図 *1*：*RSVP* オペレーション



パス メッセージは、各ノードのパスでリソースを予約して、各ノードのパス ソフト ステートを作成します。 テール ノードがパス メッセージを受信すると、ラベル付きの予約（RESV）メッセージを直前のノードに戻します。 予約メッセージが直前のノードに到着すると、予約されたリソースがロックされ、転送エントリが、テールエンド ノードから送信される MPLS ラベルでプログラムされます。 新しいMPLS ラベルが割り当てられ、次のノードアップストリームに送信されます。

予約メッセージがヘッド ノードに到着すると、ラベルがプログラムされ、MPLS データがパスに送信されます。

ハイ アベイラビリティ

RSVP は、ノンストップ フォワーディングを保証しますが、次の制約があります。

- 1:1 冗長ペアの 1 つの RP の障害耐性。
- ヒットレス ソフトウェア アップグレード。

RSVP ハイアベイラビリティ（HA）設計は、基礎となるアーキテクチャの制約に従います。つまり、プロセスで障害が発生しても、他のプロセスのオペレーションに影響を与えることはありません。 RSVP またはその任意のコラボレータのプロセス障害でも、トラフィックが損失せず、確立された LSP がダウンになることはありません。 RSVP が再起動すると、そのネイバーからシグナリング状態を回復します。 特別な設定や手動による介入は必要ありません。 RSVP グレースフル リスタートを設定できます。これは、障害後にネイバーから RSVP 状態を回復する標準メカニズムを提供します。

グレースフル リスタート

RSVP グレースフル リスタートは、ハイアベイラビリティ（HA）を保証するコントロールプレーン メカニズムを提供します。これにより、Cisco IOS XR ソフトウェアを実行するシステムでノンストップ フォワーディング サービスを提供しながら、障害状況を検出および回復できます。

RSVP グレースフル リスタートは、次の障害による MPLS トラフィックの悪影響を最小限に抑えるメカニズムを提供します。

- 通信チャネルがデータ チャネルと別々の場合での 2 つのノード間での通信チャネルの損失。これは、制御チャネル障害と呼ばれます。
- ノードのコントロールプレーンに障害が発生したが、ノードのデータ転送は維持されている状態の障害。 これは、ノード障害と呼ばれます。

RSVP グレースフル リスタートの手順については、RFC 3473『*Generalized MPLS Signaling, RSVP-TE Extensions*』の「障害処理」の項を参照してください。RSVP グレースフル リスタートを使用する主なメリットの 1 つは、ノンストップ フォワーディングおよび既存のラベルを維持しながら、コントロール プレーンを回復できることです。

グレースフル リスタート：標準およびインターフェイスベース

RSVP グレースフル リスタートを設定する場合、Cisco IOS XR ソフトウェアは、ノード ID アドレス ベースの Hello メッセージ（つまり、Hello Request および Hello Ack メッセージ）を送信および予測します。 RSVP グレースフル リスタート Hello セッションは、隣接ルータがノード ID ベースの Hello Ack メッセージに応答しない場合、確立されません。

隣接ルータでグレースフル リスタート Hello セッションを確立できるように、隣接ルータから送信されるインターフェイス アドレス ベースの Hello メッセージに応答（Hello Ack メッセージを送信）するように、グレースフル リスタートを設定することもできます。ただし、隣接ルータが、ノード ID ベースの Hello Ack メッセージに応答しない場合、RSVP グレースフル リスタート Hello セッションは確立されません。

Cisco IOS XR ソフトウェアは、グレースフル リスタートを設定する次の 2 つのコマンドを提供します。

- **signalling hello graceful-restart**
- **signalling hello graceful-restart interface-based**

（注） デフォルトでは、グレースフル リスタートはディセーブルになっています。 インターフェイス ベースのグレースフル リスタートをイネーブルにするには、最初に、標準グレースフル リスタートをイネーブルにする必要があります。 インターフェイス ベースのグレースフル リスタートを個別にイネーブルにすることはできません。

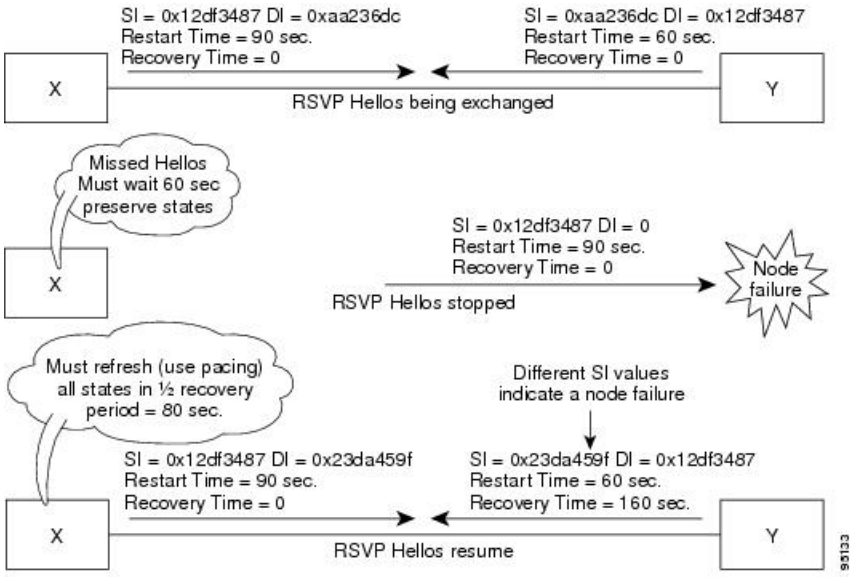
関連トピック

グレースフル リスタートのイネーブル化, （16 ページ）
グレースフル リスタートのイネーブル化：例, （47 ページ）
インターフェイスベースのグレースフル リスタートのイネーブル化：例, （48 ページ）

グレースフル リスタート：図

次の図は、RSVP グレースフル リスタートでノード障害状況がどのように処理されるかを示します。

図 *2*：***RSVP*** でのノード障害



RSVP グレースフル リスタートでは、RSVP hello メッセージを使用する必要があります。 Hello メッセージは、RSVP ネイバー間で使用されます。 各ネイバーは、hello 要求オブジェクトを含む hello メッセージを自律して発行できます。 hello 拡張をサポートするレシーバは、hello 確認（ACK）オブジェクトを含む hello メッセージで応答します。 つまり、hello メッセージには、hello Request

または hello ACK オブジェクトのいずれかが含まれます。 これらの 2 つのオブジェクトのフォーマットは同じです。

Restart Cap オブジェクトは、ノードの再起動機能を示します。 これは、送信ノードが状態回復をサポートする場合、hello メッセージで送信されます。 Restart Cap オブジェクトには次の 2 つのフィールドがあります。

再起動時間

Hello メッセージが失われてから RSVP hello セッションを再確立するまでの時間。 ユーザは、再起動時間を手動で設定できます。

回復時間

hello メッセージの再確立後に受信者が状態を再同期するまで送信側が待機する時間。 この値は、障害が発生する前に存在した状態の数に基づいて計算およびアドバタイズされます。

グレースフル リスタートでは、hello メッセージは、64 の IP Time to Live（TTL）で送信されます。これは、hello メッセージの宛先が数ホップ離れることがあるためです。 グレースフル リスタートがイネーブルで、RSVP ステートがネイバーと共有される場合、hello メッセージ（Restart Cap オブジェクトを含む）は RSVP ネイバーに送信されます。

Restart Cap オブジェクトは、RSVP ステートがネイバーと共有される場合、その RSVP ネイバーに送信されます。 ネイバーが Restart Cap オブジェクトを含む hello メッセージに応答する場合、ネイバーは、グレースフル リスタート可能とみなれます。 ネイバーが hello メッセージに応答しない場合、または Restart Cap オブジェクトを含まない hello メッセージに応答した場合、RSVP は、そのネイバーへの hello の送信をバックオフします。 グレースフル リスタートがディセーブルの場合、hello メッセージ（Request または ACK）は送信されません。 hello Request メッセージが不明ネイバーから受信された場合、hello ACK は返されません。

ACL ベース プレフィックス フィルタリング

RSVP は、拡張アクセス リスト（ACL）の設定を提供して、RSVP ルータ アラート（RA）パケットで通常の処理を転送、ドロップまたは実行します。 プレフィックス フィルタリングは、コア アクセス ルータで使用されます。これにより、RA パケット（送信元/宛先アドレスで指定）を、アクセス ポイント間のコアを介してシームレスに転送できます（または、このノードでドロップできます）。 RA パケットには RSVP フローの送信元および宛先アドレスが含まれるので、RSVP は、プレフィックス フィルタリングを RA パケットのみに適用します。

（注） プレフィックス フィルタリングで転送される RA パケットは、RSVP バンドル メッセージとして送信しないでください。バンドル メッセージは、ホップバイホップであり、RA は含まれません。 メッセージを受信するノードは、プレフィックス フィルタリングを RA パケットのみに適用するので、バンドル メッセージは転送されません。

各着信 RSVP RA パケットに対して、RSVP は IP ヘッダーを検査して、送信元/宛先 IP アドレスと拡張 ACL で設定されたプレフィックスとの一致を試行します。 予測される結果は、次のとおりです。

- ACL が存在しない場合、パケットは、通常の RSVP パケットのように処理されます。
- ACL 一致により明示的に許可された場合（パケットの宛先がローカルでない場合）、パケットが転送されます。 IP TTL は、すべての転送パケットで減少します。
- ACL 一致により明示的に拒否された場合、パケットがドロップされます。

明示的な許可または明示的な拒否がない場合、ACL インフラストラクチャは、暗黙的な（デフォルト）拒否を返します。 RSVP は、パケットをドロップするように設定できます。 デフォルトでは、ACL 一致により暗黙的な（デフォルト）拒否が返された場合、RSVP によりパケットが処理されます。

関連トピック

プレフィックス フィルタリング用の ACL 設定, （18 ページ）
ACL ベース プレフィックス フィルタリングの設定：例, （48 ページ）

RSVP MIB

『*RFC 2206, RSVP Management Information Base Using SMIv2*』は、RSVP に関するすべての SNMP MIB オブジェクトを定義します。 RSVP MIB を実装することで、これらの機能を実行できます。

- 新しいフローが作成または削除されるときにトリガーされる 2 つのトラップ（NetFlow および LostFlow）を指定します。
- SNMP を使用して RSVP に属するオブジェクトにアクセスできます。

関連トピック

RSVP トラップの有効化, （25 ページ）
RSVP トラップのイネーブル化：例, （49 ページ）

RSVP 認証の実装に関する情報

RSVP 認証を実装する前に、キーチェーンを設定する必要があります。 キーチェーンの名前は、キーチェーン設定で使用される名前と同じにする必要があります。 キーチェーンの設定の詳細については、『*Cisco ASR 9000 Series Aggregation Services Router System Security Configuration Guide*』を参照してください。

（注） RSVP認証は、キー付きハッシュメッセージ認証コード（HMAC）タイプのアルゴリズムだけをサポートしています。

Cisco IOS XR ソフトウェアで RSVP 認証を実装するには、次の概念を理解する必要があります。

RSVP 認証機能

RSVP 認証では次タスクのみ実行できます。

- 自身とネイバーだけが認識している秘密キーを使用して、ネイバーとの安全な関係を設定する。
- RSVP 認証をグローバル、インターフェイスまたはネイバー コンフィギュレーション モードで設定する。
- キー ID、着信インターフェイス、送信元アドレスおよび宛先アドレスに基づいて関連付けられる有効なセキュリティ関係があるかチェックすることで、着信インターフェイスを認証する。
- メッセージ ダイジェスト付きインテグリティ オブジェクトを発信メッセージに追加する。
- インテグリティ オブジェクトでシーケンス番号を使用して、リプレイ アタックを検出する。

RSVP 認証設計

ネットワーク管理者は、RSVP 要求を開始するシステムのセットを制御するセキュリティ ドメインを確立できる機能が必要です。

RSVP 認証機能を使用すると、RSVP ネットワークのネイバーは、安全なハッシュを使用して、すべての RSVP シグナリング メッセージにデジタル署名できます。これにより、RSVP メッセージの受信側は、送信側の IP アドレスだけに頼ることなく、メッセージの送信側を確認できます。

署名は、RFC 2747 で定義されている RSVP メッセージの RSVP インテグリティ オブジェクトで RSVP ホップごとに実行されます。 この方式では、偽造やメッセージ改ざんに対する保護が提供されます。 ただし、受信側で、受信した RSVP メッセージ内のデジタル署名を確認するためには、送信側で使用されたセキュリティ キーを取得する必要があります。

ネットワーク管理者は、共有ネットワークの各 RSVP ネイバーで共有のキーを手動で設定します。

次に、グローバル、インターフェイスまたはネイバー コンフィギュレーション モードの選択方法を示します。

- グローバル コンフィギュレーション モードは、ルータが単一のセキュリティ ドメインに属する場合に最適です（たとえば、プロバイダー コア ルータのセットの一部などです）。 単一の共有キー セットは、すべての RSVP メッセージの認証に使用されます。
- インターフェイスまたはネイバー コンフィギュレーション モードは、ルータが複数のセキュリティ ドメインに属する場合に最適です。 たとえば、プロバイダー ルータが、プロバイダー エッジ（PE）に隣接する場合や、PE がエッジ デバイスに隣接する場合です。 異なるキーを使用できますが、共有はできません。

グローバル コンフィギュレーション モードは、インターフェイスおよびネイバー インターフェイスモードのデフォルトを設定します。これらのモードは、明示的に設定されていない限り、次のように、グローバル コンフィギュレーション モードからパラメータを継承します。

- ウィンドウ サイズは、1 に設定されます。
- 制限は 1800 に設定されます。
- **key-source key-chain** コマンドは、none またはディセーブルに設定されます。

関連トピック

RSVP 認証用インターフェイスのライフタイムの設定, （35 ページ）
すべてのモードを使用した RSVP 認証：例, （51 ページ）

グローバル、インターフェイス、およびネイバー認証モード

キー、ウィンドウ サイズおよびライフタイムを含むすべての認証パラメータに対してグローバル デフォルトを設定できます。これらのデフォルトは、各ネイバーまたはインターフェイスで認証を設定するときに継承されます。ただし、これらのパラメータはネイバーまたはインターフェイスで個別で設定できますが、この場合はグローバル値（設定値またはデフォルト値）は継承されません。

（注） RSVP では、パラメータが複数のレベル（インターフェイス単位、ネイバー単位、またはグローバル）で設定される場合に使用される認証パラメータを選択するときに、次のルールが適用されます。RSVPは、ネイバー、インターフェイス、グローバルに順にパラメータを使用します。

グローバル キーを使用すると、設定が簡単になり、複数のネイバーおよび複数のインターフェイスからメッセージを受信するときにキーのミスマッチを防ぐことができます。ただし、グローバル キーは、セキュリティに関して最適ではありません。

インターフェイス キーは、2 つの RSVP ネイバー間で特定のインターフェイスのセキュリティを確保するときに使用されます。RSVP メッセージの多くは IP ルートなので、インターフェイス キーが適さない状況が多くあります。インターフェイスのすべてのキーが同じではない場合、次の理由から、キーのミスマッチが発生する可能性があります。

- RSVP グレースフル リスタートがイネーブルの場合、RSVP hello メッセージは、ローカル ルータ ID の送信元 IP アドレスおよび隣接ルータID の宛先 IP アドレスで送信されます。複数のルートが 2 つのネイバー間に存在できるので、RSVP hello メッセージは、異なるインターフェイスを経由することがあります。
- RSVP 高速再ルーティング（FRR）がアクティブの場合、RSVP Path および Resv メッセージは、複数のインターフェイスを経由できます。
- Generalized Multiprotocol Label Switching（GMPLS）オプティカル トンネルが設定されている場合、RSVP メッセージは、送信元および宛先 IP アドレスとしてルータ ID を使用して交換

されます。 複数の制御チャネルが 2 つのネイバー間に存在できるので、RSVP メッセージは、異なるインターフェイスを経由することがあります。

ネイバー ベース キーは、RSVP 認証手順をサポートするネイバーとサポートしないネイバーが混在するネットワークでの使用に適しています。 ネイバー ベース キーが特定のネイバーに設定されている場合、すべてのネイバーのアドレスおよびルータ ID を RSVP 認証に対し設定することを推奨します。

関連トピック

グローバル コンフィギュレーション モードでの RSVP 認証のライフタイムの設定, （29 ページ）
RSVP 認証グローバル コンフィギュレーション モード：例, （50 ページ）
インターフェイス モードでの RSVP 認証キーチェーンの指定, （33 ページ）
すべてのモードを使用した RSVP 認証：例, （51 ページ）

セキュリティ アソシエーション

セキュリティ アソシエーション（SA）は、リプレイ アタック、スプーフィングおよびパケット破壊を防止するために、ピアとの安全な通信に必要な情報のコレクションとして定義されます。

次の表は、セキュリティ アソシエーションを定義するメイン パラメータを示します。

表 *1*：セキュリティ アソシエーションのメイン パラメータ

パラメータ	説明
src	送信元の IP アドレス。
dst	最終宛先の IP アドレス。
interface	SA のインターフェイス。
direction	SA の送信または受信タイプ。
Lifetime	未使用のセキュリティ アソシエーション データの収集に使用される有効期限タイマーの値。
Sequence Number	送信または受信（direction のタイプ）された最後のシーケンス番号。
key-source	設定可能パラメータのキーのソース。
keyID	最後に使用されたキー番号（key-source から返されます）。

パラメータ	説明
digest	最後に使用されたアルゴリズム（key-source から返されます）。
Window Size	設定可能なパラメータの許容範囲を指定します。 このパラメータは、direction パラメータが受信タイプの場合に適用可能です。
Window	受信または受け入れられた最後の *window size* 値のシーケンス番号を指定します。 このパラメータは、direction パラメータが受信タイプの場合に適用可能です。

SA は、認証を要求するメッセージを送受信するときに動的に作成されます。 ネイバー、送信元および宛先アドレスは、メッセージが着信か発信かに基づいて、IPヘッダーまたはHOPオブジェクトなどの RSVP オブジェクトから取得されます。

SA が作成されると、有効期限タイマーが作成されます。 SA がメッセージを認証すると、最近使用されたことを示すマークが付けられます。 ライフタイム タイマーは、SA が使用されているかどうかを定期的にチェックします。 使用されている場合、フラグが宣言され、再びマークが付けられない限り、次の期間までクリーンアップされます。

次の表に、メッセージ タイプに基づいた SA の送信元および宛先アドレス キーのタイプを検出する方法を示します。

表 *2*：各種メッセージの送信元および宛先アドレスの位置

メッセージ タイプ	送信元アドレスの位置	宛先アドレスの位置
Path	HOP オブジェクト	SESSION オブジェクト
PathTear	HOP オブジェクト	SESSION オブジェクト
PathError	HOP オブジェクト	IP ヘッダー
Resv	HOP オブジェクト	IP ヘッダー
ResvTear	HOP オブジェクト	IP ヘッダー
ResvError	HOP オブジェクト	IP ヘッダー
ResvConfirm	IP ヘッダー	CONFIRM オブジェクト
Ack	IP ヘッダー	IP ヘッダー
Srefresh	IP ヘッダー	IP ヘッダー

メッセージ タイプ	送信元アドレスの位置	宛先アドレスの位置
Hello	IP ヘッダー	IP ヘッダー
Bundle	—	—

関連トピック

RSVP ネイバー認証用キーチェーンの指定, （39 ページ）
RSVP ネイバー認証：例, （51 ページ）
RSVP ネイバー認証のライフタイムの設定, （40 ページ）
RSVP 認証グローバル コンフィギュレーション モード：例, （50 ページ）

Key-source Key-chain

key-source key-chain は、使用するキーを指定するときに使用されます。

特定の ID を含むキーのリストを設定し、さまざまなライフタイムを指定します。これにより、サービスを中断することなく、事前に定義されたインターバルでキーが自動的変更されます。ロールオーバーは、信頼できない送信元が現在のキーを取得、推論または予想した場合に発生する問題を最小化することで、ネットワーク セキュリティを向上します。

RSVP は、次のキー ID タイプを使用して、ロールオーバーを処理します。

- TX の場合、最新の適切なキー ID を使用します。
- RX の場合、インテグリティ オブジェクトで受信されるキー ID を使用します。

キーチェーン管理の実装の詳細については、『*Cisco ASR 9000 Series Router System Security Configuration Guide Cisco ASR 9000 Series Router*』を参照してください。

関連トピック

グローバル コンフィギュレーション モードでキーチェーンを使用した RSVP 認証のイネーブル化, （27 ページ）
RSVP 認証グローバル コンフィギュレーション モード：例, （50 ページ）
RSVP ネイバー認証用キーチェーンの指定, （39 ページ）
RSVP ネイバー認証：例, （51 ページ）

ウィンドウサイズおよびシーケンス外のメッセージに関するガイドライン

次のガイドラインは、ウィンドウ サイズおよびシーケンス外のメッセージに必要です。

- デフォルトのウィンドウ サイズは、1 に設定されます。 単一のメッセージがシーケンス外で受信された場合、RSVP は、これを拒否し、メッセージを表示します。
- RSVP メッセージがバースト モードで送信された場合（たとえば、トンネル最適化など）、一部のメッセージが、一定時間だけシーケンス外になることがあります。
- ウィンドウ サイズは、**window-size** コマンドを使用して増加できます。 ウィンドウ サイズが増加すると、重複するシーケンス番号をチェックして、リプレイ アタックを検出できます。

関連トピック

グローバル コンフィギュレーション モードでの RSVP 認証のウィンドウ サイズの設定, （31 ページ）
RSVP 認証用インターフェイスのウィンドウ サイズの設定, （36 ページ）
RSVP ネイバー認証用ウィンドウ サイズの設定, （42 ページ）
すべてのモードを使用した RSVP 認証：例, （51 ページ）
インターフェイスの RSVP 認証：例, （50 ページ）

シーケンス外に関する警告事項

次に、シーケンス外に関する警告を示します。

- RSVP メッセージが、最大伝送単位（MTU）値が異なる複数のインターフェイス タイプを経由する場合、断片化される場合、一部のメッセージがシーケンス外になることがあります。
- IP オプションがいくつかあるパケットは、並べ替えられることがあります。
- QoS 設定を変更すると、パケットが一時的に並べ替えられることがあります。
- QoS ポリシーは、パケットの並べ替えを安定した状態にします。

すべてのシーケンス外メッセージがドロップされるため、送信側は、これらを再転送する必要があります。 RSVP 状態タイムアウトは一般的に長いため、transient ステートのシーケンス外メッセージでは、ステート タイムアウトは発生しません。

RSVP の実装方法

RSVP は、いくつかのルータでの調整が必要で、LSP を設定するため RSVP メッセージの交換を確立します。 クライアント アプリケーションによっては、RSVP で、いくつかの基本設定が必要になります（次のトピックを参照）。

トラフィック エンジニアリング トンネル帯域幅の設定

トラフィック エンジニアリング トンネル帯域幅を設定するには、最初に、TE トンネルを設定し、インターフェイスごとに予約帯域幅を設定する必要があります（データ チャネルまたは制御チャネルの帯域幅を設定する必要はありません）。

Cisco IOS XR ソフトウェアは、先行標準と IETF の 2 つの MPLS DS-TE モードをサポートします。

（注） 先行標準 DS-TE では、データ チャネルまたは制御チャネルの帯域幅を設定する必要はありません。 このアプリケーションでは、その他に特別な RSVP 設定は必要ありません。 RSVP 帯域幅が、特定のインターフェイスで指定されていない場合、LSP設定でゼロ帯域幅を指定できます（RSVP インターフェイス コンフィギュレーション モードまたは MPLS-TE コンフィギュレーション モードで設定されている場合）。

関連トピック

先行標準 DS-TE トンネルの設定
RDM を使用した IETF DS-TE トンネルの設定
MAM を使用した IETF DS-TE トンネルの設定

DiffServ-TE 帯域幅の確認

次のタスクを実行して、DiffServ-TE 帯域幅を確認します。

RSVP グローバルおよびサブプールで、予約可能な帯域幅は、ノードの TE トンネルを収容するために、インターフェイスごとに設定されます。 すべての設定可能な帯域幅プールから使用できる帯域幅が、IGP を使用してアドバタイズされます。 RSVP は、適切な帯域幅プール要件により TE トンネルをシグナリングします。

手順の概要

1. **configure**
2. **rsvp**
3. **interface** *type interface-path-id*
4. **bandwidth** *total-bandwidth max-flow* **sub-pool** *sub-pool-bw*
5. 次のいずれかのコマンドを使用します。
   - **end**
   - **commit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure** 例： `RP/0/RSP0/CPU0:router# configure`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**rsvp** 例： `RP/0/RSP0/CPU0:router(config)# rsvp`	RSVP コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type interface-path-id* 例： `RP/0/RSP0/CPU0:router(config-rsvp)# interface pos 0/2/0/0`	RSVP プロトコルのインターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**bandwidth** *total-bandwidth max-flow* **sub-pool** *sub-pool-bw* 例： `RP/0/RSP0/CPU0:router(config-rsvp-if)# bandwidth 1000 100 sub-pool 150`	このインターフェイスで、フローおよびサブプール帯域幅の予約可能な帯域幅および最大 RSVP 帯域幅を設定します。

ステップ 5	次のいずれかのコマンドを使用します。
	• **end**
	• **commit**
	
	例：
	`RP/0/RSP0/CPU0:router(config-rsvp-if)# end`
	または
	`RP/0/RSP0/CPU0:router(config-rsvp-if)# commit`
		設定変更を保存します。
		• **end** コマンドを実行すると、変更をコミットするように要求されます。
		`Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:`
		◦ **yes** と入力すると、実行コンフィギュレーションファイルに変更が保存され、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。
		◦ **no** と入力すると、コンフィギュレーションセッションが終了して、ルータが EXEC モードに戻ります。変更はコミットされません。
		◦ **cancel** と入力すると、現在のコンフィギュレーション セッションが継続します。コンフィギュレーショ

	コマンドまたはアクション	目的
		ンセッションは終了せず、設定変更もコミットされません。 • 実行コンフィギュレーション ファイルに変更を保存し、コンフィギュレーション セッションを継続するには、**commit** コマンドを使用します。

関連トピック

差別化サービス トラフィック エンジニアリング
帯域幅設定（MAM）：例, （45 ページ）
帯域幅設定（RDM）：例, （46 ページ）

グレースフル リスタートのイネーブル化

次のタスクを実行して、ノード ID およびインターフェイス ベース hello の両方を使用して実装するために、グレースフル リスタートをイネーブルにします。

RSVP グレースフル リスタートによって、ノンストップ フォワーディング サービスが維持されると同時に、障害状態の検出および回復を可能にするハイ アベイラビリティを確保するためにコントロール プレーン メカニズムが提供されています。

手順の概要

1. **configure**
2. **rsvp**
3. **signalling graceful-restart**
4. **signalling graceful-restart interface-based**
5. 次のいずれかのコマンドを使用します。
   - **end**
   - **commit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure** 例： `RP/0/RSP0/CPU0:router:router# configure`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**rsvp** 例： `RP/0/RSP0/CPU0:router(config)# rsvp`	RSVP コンフィギュレーション モードを開始します。
ステップ 3	**signalling graceful-restart** 例： `RP/0/RSP0/CPU0:router(config-rsvp)# signalling graceful-restart`	ノードでグレースフル リスタート プロセスをイネーブルにします。
ステップ 4	**signalling graceful-restart interface-based** 例： `RP/0/RSP0/CPU0:router(config-rsvp)# signalling graceful-restart interface-based`	ノードでインターフェイス ベース グレースフル リスタート プロセスをイネーブルにします。

ステップ 5	次のいずれかのコマンドを使用します。
	• **end**
	• **commit**
	
	例：
	`RP/0/RSP0/CPU0:router(config-rsvp)# end`
	または
	`RP/0/RSP0/CPU0:router(config-rsvp)# commit`
		設定変更を保存します。
		• **end** コマンドを実行すると、変更をコミットするように要求されます。
		`Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:`
		◦ **yes** と入力すると、実行コンフィギュレーション ファイルに変更が保存され、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。
		◦ **no** と入力すると、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。変更はコミットされません。
		◦ **cancel** と入力すると、現在のコンフィギュレーション セッションが継続します。コンフィギュレーショ

	コマンドまたはアクション	目的
		ン セッションは終了せず、設定変更もコミットされません。 • 実行コンフィギュレーション ファイルに変更を保存し、コンフィギュレーション セッションを継続するには、**commit** コマンドを使用します。

関連トピック

グレースフル リスタート：標準およびインターフェイスベース，（4 ページ）
グレースフル リスタートのイネーブル化：例，（47 ページ）
インターフェイスベースのグレースフル リスタートのイネーブル化：例，（48 ページ）

ACL ベース プレフィックス フィルタリングの設定

RSVP プレフィックス フィルタリングがどのように関連付けられるかを示す 2 つの手順が提供されます。

• プレフィックス フィルタリング用の ACL 設定，（18 ページ）
• RSVP パケット ドロップの設定，（20 ページ）

プレフィックス フィルタリング用の ACL 設定

次のタスクを実行して、パケット フィルタリングに使用される送信元および宛先プレフィックスを識別する拡張アクセス リスト ACL を設定します。

（注） 拡張 ACL は、拡張 ACL コンフィギュレーション コマンドを使用して個別に設定する必要があります。

手順の概要

1. **configure**
2. **rsvp**
3. **signalling prefix-filtering access-list**
4. 次のいずれかのコマンドを使用します。
   - **end**
   - **commit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure** 例： `RP/0/RSP0/CPU0:router# configure`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**rsvp** 例： `RP/0/RSP0/CPU0:router(config)# rsvp`	RSVP コンフィギュレーション モードを開始します。
ステップ 3	**signalling prefix-filtering access-list** 例： `RP/0/RSP0/CPU0:router(config-rsvp)# signalling prefix-filtering access-list banks`	拡張アクセス リスト名を文字列として入力します。
ステップ 4	次のいずれかのコマンドを使用します。 • **end** • **commit** 例： `RP/0/RSP0/CPU0:router(config-rsvp)# end`	設定変更を保存します。 • **end** コマンドを実行すると、変更をコミットするように要求されます。 `Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:` ◦ **yes** と入力すると、実行コンフィギュレーション ファイルに変更が保存され、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。

	コマンドまたはアクション	目的
	または `RP/0/RSP0/CPU0:router(config-rsvp)# commit`	◦ **no** と入力すると、コンフィギュレーションセッションが終了して、ルータが EXEC モードに戻ります。変更はコミットされません。 ◦ **cancel** と入力すると、現在のコンフィギュレーションセッションが継続します。コンフィギュレーションセッションは終了せず、設定変更もコミットされません。 • 実行コンフィギュレーション ファイルに変更を保存し、コンフィギュレーションセッションを継続するには、**commit** コマンドを使用します。

関連トピック

ACL ベース プレフィックス フィルタリング, （6 ページ）
ACL ベース プレフィックス フィルタリングの設定：例, （48 ページ）

RSVP パケット ドロップの設定

次のタスクを実行して、ACL 一致により暗黙的（デフォルト）拒否が返されたときに RA パケットをドロップするように RSVP を設定します。

デフォルトの動作は、ACL 一致により暗黙的（デフォルト）拒否が返されると、RA パケットで通常の RSVP 処理を実行します。

手順の概要

1. **configure**
2. **rsvp**
3. **signalling prefix-filtering default-deny-action**
4. 次のいずれかのコマンドを使用します。
   - **end**
   - **commit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure** 例： `RP/0/RSP0/CPU0:router# configure`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**rsvp** 例： `RP/0/RSP0/CPU0:router(config)# rsvp`	RSVP コンフィギュレーション モードを開始します。
ステップ 3	**signalling prefix-filtering default-deny-action** 例： `RP/0/RSP0/CPU0:router(config-rsvp)# signalling prefix-filtering default-deny-action`	RA メッセージをドロップします。

ステップ 4	次のいずれかのコマンドを使用します。
	• **end**
	• **commit**
	
	例：
	`RP/0/RSP0/CPU0:router(config-rsvp)# end`
	または
	`RP/0/RSP0/CPU0:router(config-rsvp)# commit`
		設定変更を保存します。
		• **end** コマンドを実行すると、変更をコミットするように要求されます。
		`Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:`
		◦ **yes** と入力すると、実行コンフィギュレーション ファイルに変更が保存され、コンフィギュレーションセッションが終了して、ルータが EXEC モードに戻ります。
		◦ **no** と入力すると、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。変更はコミットされません。
		◦ **cancel** と入力すると、現在のコンフィギュレーションセッションが継続します。コンフィギュレーションセッションは終了せず、設定変更もコミットされません。

	コマンドまたはアクション	目的
		• 実行コンフィギュレーションファイルに変更を保存し、コンフィギュレーションセッションを継続するには、**commit** コマンドを使用します。

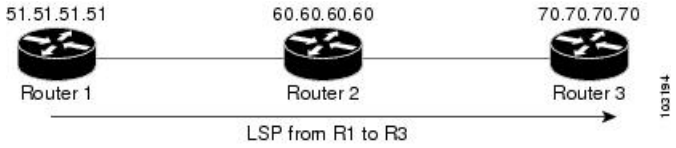
関連トピック

MPLS-TE 用 RSVP の概要 , （2 ページ）
RSVP パケットの DSCP の設定：例, （49 ページ）

RSVP 設定の確認

次の図は、トポロジを示します。

図 *3*：トポロジの例



次の手順を実行して、RSVP 設定を確認します。

手順の概要

1. **show rsvp session**
2. **show rsvp counters messages summary**
3. **show rsvp counters events**
4. **show rsvp interface** *type interface-path-id* [**detail**]
5. **show rsvp graceful-restart**
6. **show rsvp graceful-restart** [**neighbors** *ip-address* | **detail**]
7. **show rsvp interface**
8. **show rsvp neighbor**

手順の詳細

ステップ 1 **show rsvp session**

LSP のパスのすべてのルータが、セッションごとに少なくとも 1 つのパス ステート ブロック（PSB）および 1 つの予約ステート ブロック（RSB）で設定されていることを確認します。

例：

```
RP/0/RSP0/CPU0:router# show rsvp session

Type Destination Add DPort Proto/ExtTunID PSBs RSBs Reqs
 ---- --------------- ----- --------------- ----- ----- ----- LSP4
 172.16.70.70 6 10.51.51.51 1 1 0
```

この例では、出力は、入力（ヘッド）ルータ 10.51.51.51 から出力（テール）ルータ 172.16.70.70 への LSP を示します。 トンネル ID（宛先ポートとも呼ばれます）は 6 です。

例：

```
If no states can be found for a session that should be up, verify the
      application (for example, MPLS-TE ) to see if
      everything is in order. If a session has one PSB but no RSB, this indicates
      that either the Path message is not making it to the egress (tail) router or
      the reservation message is not making it back to the router R1 in question.
```

ダウンストリーム ルータ R2 に移動して、セッション情報を表示します。

例：

```
If R2 has no PSB, either the path message is not making it to the
      router or the path message is being rejected (for example, due to lack of
      resources). If R2 has a PSB but no RSB, go to the next downstream router R3
      to investigate. If R2 has a PSB and an RSB, this means the reservation is
      not making it from R2 to R1 or is being rejected.
```

ステップ 2 **show rsvp counters messages summary**

RSVP メッセージが転送および受信されるかどうかを確認します。

例：

```
RP/0/RSP0/CPU0:router# show rsvp counters messages summary

All RSVP Interfaces Recv Xmit Recv Xmit Path 0 25
      Resv 30 0 PathError 0 0 ResvError 0 1 PathTear 0 30 ResvTear 12 0
      ResvConfirm 0 0 Ack 24 37 Bundle 0 Hello 0 5099 SRefresh 8974 9012
      OutOfOrder 0 Retransmit 20 Rate Limited 0
```

ステップ 3 **show rsvp counters events**

失効している RSVP ステートの数を確認します。 RSVP はソフトステート メカニズムを使用するので、障害によっては、ネイバーからのリフレッシュが欠落し RSVP ステートが失効します。

例：

```
RP/0/RSP0/CPU0:router# show rsvp counters events

mgmtEthernet0/0/0/0 tunnel6 Expired Path states 0 Expired
      Path states 0 Expired Resv states 0 Expired Resv states 0 NACKs received 0
      NACKs received 0 POS0/3/0/0                              POS0/3/0/1 Expired
      Path states 0 Expired Path states 0 Expired Resv states 0 Expired Resv
      states 0 NACKs received 0 NACKs received 0 POS0/3/0/2
                                  POS0/3/0/3 Expired Path states 0 Expired Path
      states 0 Expired Resv states 0 Expired Resv states 1 NACKs received 0 NACKs
```

```
      received 1
```

ステップ 4 **show rsvp interface** *type interface-path-id* [**detail**]

リフレッシュ削減が特定のインターフェイスで機能しているか確認します。

例：

```
RP/0/RSP0/CPU0:router# show rsvp interface pos0/3/0/3 detail

INTERFACE: POS0/3/0/3 (ifh=0x4000D00). BW
      (bits/sec): Max=1000M. MaxFlow=1000M. Allocated=1K (0%). MaxSub=0.
      Signalling: No DSCP marking. No rate limiting. States in: 1. Max missed
      msgs: 4. Expiry timer: Running (every 30s). Refresh interval: 45s. Normal
      Refresh timer: Not running. Summary refresh timer: Running. Refresh
      reduction local: Enabled. Summary Refresh: Enabled (4096 bytes max).
      Reliable summary refresh: Disabled. Ack hold: 400 ms, Ack max size: 4096
      bytes. Retransmit: 900ms. Neighbor information: Neighbor-IP Nbor-MsgIds
      States-out Refresh-Reduction Expiry(min::sec) -------------- --------------
      ---------- ------------------ ---------------- 64.64.64.65 1 1 Enabled
      14::45
```

ステップ 5 **show rsvp graceful-restart**

グレースフル リスタートがローカルでイネーブルにされているか確認します。

例：

```
RP/0/RSP0/CPU0:router# show rsvp graceful-restart

Graceful restart: enabled Number of global
      neighbors: 1 Local MPLS router id: 10.51.51.51 Restart time: 60 seconds
      Recovery time: 0 seconds Recovery timer: Not running Hello interval: 5000
      milliseconds Maximum Hello miss-count: 3
```

ステップ 6 **show rsvp graceful-restart** [**neighbors** *ip-address* | **detail**]

グレースフルリスタートがネイバーでイネーブルにされているか確認します。次に、ネイバー192.168.60.60 が hello メッセージに応答しない例を示します。

例：

```
RP/0/RSP0/CPU0:router# show rsvp graceful-restart neighbors 192.168.60.60

Neighbor App State Recovery Reason
      Since LostCnt --------------- ----- ------ -------- ------------
      -------------------- -------- 192.168.60.60 MPLS INIT DONE N/A 12/06/2003
      19:01:49 0
RP/0/RSP0/CPU0:router# show rsvp graceful-restart neighbors detail

Neighbor: 192.168.60.60 Source: 10.51.51.51
      (MPLS) Hello instance for application MPLS Hello State: INIT (for 3d23h)
      Number of times communications with neighbor lost: 0 Reason: N/A Recovery
      State: DONE Number of Interface neighbors: 1 address: 10.64.64.65 Restart
      time: 0 seconds Recovery time: 0 seconds Restart timer: Not running Recovery
      timer: Not running Hello interval: 5000 milliseconds Maximum allowed missed
      Hello messages: 3
```

ステップ 7 **show rsvp interface**

使用できる RSVP 帯域幅を確認します。

例：

```
RP/0/RSP0/CPU0:router# show rsvp interface

Interface MaxBW MaxFlow Allocated MaxSub -----------
      -------- -------- --------------- -------- Et0/0/0/0 0 0 0 ( 0%) 0 PO0/3/0/0
      1000M 1000M 0 ( 0%) 0 PO0/3/0/1 1000M 1000M 0 ( 0%) 0 PO0/3/0/2 1000M 1000M
      0 ( 0%) 0 PO0/3/0/3 1000M 1000M 1K ( 0%) 0
```

ステップ 8 **show rsvp neighbor**
RSVP ネイバーを確認します。

例：

```
RP/0/RSP0/CPU0:router# show rsvp neighbor detail
Global Neighbor: 40.40.40.40 Interface Neighbor: 1.1.1.1
      Interface: POS0/0/0/0 Refresh Reduction: "Enabled" or "Disabled". Remote
      epoch: 0xXXXXXXXX Out of order messages: 0 Retransmitted messages: 0
      Interface Neighbor: 2.2.2.2 Interface: POS0/1/0/0 Refresh Reduction:
      "Enabled" or "Disabled". Remote epoch: 0xXXXXXXXX Out of order messages: 0
      Retransmitted messages: 0
```

関連トピック

MPLS-TE 用 RSVP の概要 , （2 ページ）

RSVP トラップの有効化

RSVP MIB トラップ以外、MIB をアクティブにするために必要な作業はありません。 この MIB 機能は、RSVP が有効になると自動的にイネーブルになりますが、RSVP トラップはイネーブルにする必要があります。

次のタスクを実行して、すべての RSVP MIB トラップ、NewFlow トラップおよび LostFlow トラップをイネーブルにします。

手順の概要

1. **configure**
2. **snmp-server traps rsvp lost-flow**
3. **snmp-server traps rsvp new-flow**
4. **snmp-server traps rsvp all**
5. Use one of these commands:
   - **end**
   - **commit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure** 例： `RP/0/RSP0/CPU0:router# configure`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**snmp-server traps rsvp lost-flow** 例： `RP/0/RSP0/CPU0:router(config)# snmp-server traps rsvp lost-flow`	RSVP 通知を送信して、RSVP LostFlow トラップをイネーブルにします。
ステップ 3	**snmp-server traps rsvp new-flow** 例： `RP/0/RSP0/CPU0:router(config)# snmp-server traps rsvp new-flow`	RSVP 通知を送信して、RSVP NewFlow トラップをイネーブルにします。
ステップ 4	**snmp-server traps rsvp all** 例： `RP/0/RSP0/CPU0:router(config)# snmp-server traps rsvp all`	RSVP 通知を送信して、すべての RSVP MIB トラップをイネーブルにします。

ステップ 5	Use one of these commands:
	• **end**
	• **commit**
	
	例：
	`RP/0/RSP0/CPU0:router(config)# end`
	or
	`RP/0/RSP0/CPU0:router(config)# commit`
		Saves configuration changes.
		• When you issue the **end** command, the system prompts you to commit changes:
		`Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:`
		◦ Entering yes saves configuration changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode.
		◦ Entering no exits the configuration session and returns the router to EXEC mode without committing the configuration changes.
		◦ Entering cancel leaves the router in the current configuration session without exiting or committing the configuration changes.

	コマンドまたはアクション	目的
		• Use the **commit** command to save the configuration changes to the running configuration file and remain within the configuration session.

関連トピック

RSVP MIB, （7 ページ）
RSVP トラップのイネーブル化：例, （49 ページ）

RSVP 認証の実装方法

RSVP 認証モードには、グローバル、インターフェイスおよびネイバーの 3 種類があります。 次のトピックでは、各モードで RSVP 認証を実装する方法について説明します。

グローバル コンフィギュレーション モード RSVP 認証の設定

ここでは、グローバル コンフィギュレーション モードで RSVP 認証を設定する手順について説明します。

グローバル コンフィギュレーション モードでキーチェーンを使用した RSVP 認証のイネーブル化

次のタスクを実行して、グローバルコンフィギュレーションモードでキーチェーンを指定することによる暗号認証の RSVP 認証をイネーブルにします。

（注） このタスクを完了をする前に、キーチェーンを設定する必要があります（『*Cisco ASR 9000 Series Aggregation Services Router System Security Configuration Guide* 』を参照）。

手順の概要

1. **configure**
2. **rsvp authentication**
3. **key-source key-chain** *key-chain-name*
4. 次のいずれかのコマンドを使用します。
   - **end**
   - **commit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure** 例： `RP/0/RSP0/CPU0:router# configure`	グローバル コンフィギュレーション モードを開始します。

ステップ 2	**rsvp authentication**
	
	例：
	`RP/0/RSP0/CPU0:router(config)# rsvp authentication`
	`RP/0/RSP0/CPU0:router(config-rsvp-auth)#`
		RSVP 認証コンフィギュレーション モードを開始します。

ステップ 3	**key-source key-chain** *key-chain-name* 例： `RP/0/RSP0/CPU0:router(config-rsvp-auth)# key-source key-chain mpls-keys`	RSVP シグナリング メッセージを認証するキー情報のソースを指定します。 ***key-chain-name*** キーチェーンの名前。 最大文字数は 32 です。

ステップ 4	次のいずれかのコマンドを使用します。
	• **end**
	• **commit**
	
	例：
	`RP/0/RSP0/CPU0:router(config-rsvp-auth)# end`
		設定変更を保存します。
		• **end** コマンドを実行すると、変更をコミットするように要求されます。
		`Uncommitted changes found, commit them before exiting(yes/no/cancel)?`
		`[cancel]:`
		◦ **yes** と入力すると、実行コンフィギュレーション ファイルに変更が保存され、コンフィギュレーショ

	コマンドまたはアクション	目的
	または `RP/0/RSP0/CPU0:router(config-rsvp-auth)# commit`	ン セッションが終了して、ルータが EXEC モードに戻ります。 ◦ **no** と入力すると、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。変更はコミットされません。 ◦ **cancel** と入力すると、現在のコンフィギュレーションセッションが継続します。コンフィギュレーション セッションは終了せず、設定変更もコミットされません。 • 実行コンフィギュレーションファイルに変更を保存し、コンフィギュレーション セッションを継続するには、**commit** コマンドを使用します。

関連トピック

Key-source Key-chain, （12 ページ）
RSVP 認証グローバル コンフィギュレーション モード：例, （50 ページ）

グローバル コンフィギュレーション モードでの RSVP 認証のライフタイムの設定

次のタスクを実行して、グローバル コンフィギュレーション モードの RSVP 認証のライフタイム値を設定します。

手順の概要

1. **configure**
2. **rsvp authentication**
3. **life-time** *seconds*
4. 次のいずれかのコマンドを使用します。
   - **end**
   - **commit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure** 例： `RP/0/RSP0/CPU0:router# configure`	グローバル コンフィギュレーション モードを開始します。

ステップ 2	**rsvp authentication**
	
	例：
	
	`RP/0/RSP0/CPU0:router(config)# rsvp authentication`
	`RP/0/RSP0/CPU0:router(config-rsvp-auth)#`
		RSVP 認証コンフィギュレーション モードを開始します。

ステップ 3	**life-time** *seconds* 例： `RP/0/RSP0/CPU0:router(config-rsvp-auth)# life-time 2000`	信頼できる他の RSVP ネイバーとのセキュリティ アソシエーションを RSVP が保持する期間を制御します。 ***seconds*** 信頼できる他の RSVP ネイバーとのアイドルなセキュリティ アソシエーションを RSVP が保持する期間（秒単位）。 指定できる値の範囲は 30 ～ 86400 です。 デフォルト値は 1800 です。

ステップ 4	次のいずれかのコマンドを使用します。
	
	• **end**
	• **commit**
	
	例：
	
	`RP/0/RSP0/CPU0:router(config-rsvp-auth)# end`
	または
	
	`RP/0/RSP0/CPU0:router(config-rsvp-auth)# commit`
		設定変更を保存します。
		
		• **end** コマンドを実行すると、変更をコミットするように要求されます。
		
		`Uncommitted changes found, commit them before exiting(yes/no/cancel)?`
		`[cancel]:`
		
		◦ **yes** と入力すると、実行コンフィギュレーション ファイルに変更が保存され、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。
		
		◦ **no** と入力すると、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。変更はコミットされません。
		
		◦ **cancel** と入力すると、現在のコンフィギュレーション セッションが継続します。コンフィギュレーション セッションは終了せず、設定変更もコミットされません。

	コマンドまたはアクション	目的
		• 実行コンフィギュレーションファイルに変更を保存し、コンフィギュレーション セッションを継続するには、**commit** コマンドを使用します。

関連トピック

グローバル、インターフェイス、およびネイバー認証モード, （9 ページ）
RSVP 認証グローバル コンフィギュレーション モード：例, （50 ページ）

グローバル コンフィギュレーション モードでの RSVP 認証のウィンドウ サイズの設定

次のタスクを実行して、グローバル コンフィギュレーション モードの RSVP 認証のウィンドウ サイズを設定します。

手順の概要

1. **configure**
2. **rsvp authentication**
3. **window-size** *N*
4. 次のいずれかのコマンドを使用します。
   - **end**
   - **commit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure** 例： `RP/0/RSP0/CPU0:router# configure`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**rsvp authentication** 例： `RP/0/RSP0/CPU0:router(config)# rsvp authentication`	RSVP 認証コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
	`RP/0/RSP0/CPU0:router(config-rsvp-auth)#`	
ステップ 3	**window-size** *N* 例： `RP/0/RSP0/CPU0:router(config-rsvp-auth)# window-size 33`	受信できるシーケンス外の RSVP 認証済みメッセージの最大数を指定します。 ***N*** シーケンス外のメッセージを制限するウィンドウのサイズ。 範囲は 1 ～ 64 です。 デフォルト値は 1 であり、この場合すべてのシーケンス外メッセージがドロップされます。

ステップ 4	次のいずれかのコマンドを使用します。
	• **end**
	• **commit**
	
	例：
	`RP/0/RSP0/CPU0:router(config-rsvp-auth)# end`
	または
	`RP/0/RSP0/CPU0:router(config-rsvp-auth)# commit`
		設定変更を保存します。
		• **end** コマンドを実行すると、変更をコミットするように要求されます。
		`Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:`
		◦ **yes** と入力すると、実行コンフィギュレーション ファイルに変更が保存され、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。
		◦ **no** と入力すると、コンフィギュレーションセッションが終了して、ルータが EXEC モードに戻ります。変更はコミットされません。
		◦ **cancel** と入力すると、現在のコンフィギュレーションセッションが継続します。コンフィギュレーションセッションは終了せず、設定変更もコミットされません。
		• 実行コンフィギュレーション ファイルに変更を保存し、コンフィギュレーション セッションを継続するには、**commit** コマンドを使用します。

関連トピック

ウィンドウ サイズおよびシーケンス外のメッセージに関するガイドライン, （12 ページ）
すべてのモードを使用した RSVP 認証：例, （51 ページ）
インターフェイスの RSVP 認証：例, （50 ページ）

RSVP 認証用インターフェイスの設定

次のタスクでは、RSVP 認証のインターフェイスを設定する方法について説明します。

インターフェイス モードでの RSVP 認証キーチェーンの指定

次のタスクを実行して、インターフェイス モードで RSVP 認証キーチェーンを指定します。

最初にキーチェーンを指定する必要があります（『*Cisco ASR 9000 Series Aggregation Services Router System Security Configuration Guide* 』を参照）。

手順の概要

1. **configure**
2. **rsvp interface** *type interface-path-id*
3. **authentication**
4. **key-source key-chain** *key-chain-name*
5. 次のいずれかのコマンドを使用します。
   - **end**
   - **commit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure** 例： `RP/0/RSP0/CPU0:router# configure`	グローバル コンフィギュレーション モードを開始します。

ステップ 2	**rsvp interface** *type interface-path-id*
	
	例：
	`RP/0/RSP0/CPU0:router(config)# rsvp interface POS 0/2/1/0`
	`RP/0/RSP0/CPU0:router(config-rsvp-if)#`
		RSVP インターフェイス コンフィギュレーション モードを開始します。

ステップ 3	**authentication**
	
	例：
	`RP/0/RSP0/CPU0:router(config-rsvp-if)# authentication`
	`RP/0/RSP0/CPU0:router(config-rsvp-if-auth)#`
		RSVP 認証コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	**key-source key-chain** *key-chain-name* 例： `RP/0/RSP0/CPU0:router(config-rsvp-if-auth)# key-source key-chain mpls-keys`	RSVP シグナリング メッセージを認証するキー情報のソースを指定します。 ***key-chain-name*** キーチェーンの名前。 最大文字数は 32 です。

ステップ 5	次のいずれかのコマンドを使用します。
	• **end**
	• **commit**
	
	例：
	`RP/0/RSP0/CPU0:router(config-rsvp-if-auth)# end`
	または
	`RP/0/RSP0/CPU0:router(config-rsvp-if-auth)# commit`
		設定変更を保存します。
		• **end** コマンドを実行すると、変更をコミットするように要求されます。
		`Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:`
		◦ **yes** と入力すると、実行コンフィギュレーション ファイルに変更が保存され、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。
		◦ **no** と入力すると、コンフィギュレーションセッションが終了して、ルータが EXEC モードに戻ります。変更はコミットされません。
		◦ **cancel** と入力すると、現在のコンフィギュレーションセッションが継続します。コンフィギュレーションセッションは終了せず、設定変更もコミットされません。
		• 実行コンフィギュレーション ファイルに変更を保存し、コンフィギュレーション セッションを継続するには、**commit** コマンドを使用します。

関連トピック

グローバル、インターフェイス、およびネイバー認証モード, （9 ページ）
すべてのモードを使用した RSVP 認証：例, （51 ページ）

RSVP 認証用インターフェイスのライフタイムの設定

次のタスクを実行して、インターフェイスのセキュリティ アソシエーションのライフタイムを設定します。

手順の概要

1. **configure**
2. **rsvp interface** *type interface-path-id*
3. **authentication**
4. **life-time** *seconds*
5. 次のいずれかのコマンドを使用します。
   - **end**
   - **commit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure** 例： `RP/0/RSP0/CPU0:router# configure`	グローバル コンフィギュレーション モードを開始します。

ステップ 2	**rsvp interface** *type interface-path-id*
	例：
	`RP/0/RSP0/CPU0:router(config)# rsvp interface POS 0/2/1/0`
	`RP/0/RSP0/CPU0:router(config-rsvp-if)#`
		RSVP インターフェイス コンフィギュレーション モードを開始します。

ステップ 3	**authentication**
	例：
	`RP/0/RSP0/CPU0:router(config-rsvp-if)# authentication`
	`RP/0/RSP0/CPU0:router(config-rsvp-if-auth)#`
		RSVP認証コンフィギュレーション モードを開始します。

ステップ 4	**life-time** *seconds* 例： `RP/0/RSP0/CPU0:router(config-rsvp-if-auth)#`	信頼できる他の RSVP ネイバーとのセキュリティ アソシエーションを RSVP が保持する期間を制御します。

	コマンドまたはアクション	目的
	`life-time 2000`	***seconds*** 信頼できる他のRSVPネイバーとのアイドルなセキュリティ アソシエーションを RSVP が保持する期間（秒単位）。 指定できる値の範囲は 30 ～ 86400 です。 デフォルト値は 1800 です。

ステップ 5	次のいずれかのコマンドを使用します。
	• **end**
	• **commit**
	例：
	`RP/0/RSP0/CPU0:router(config-rsvp-if-auth)# end`
	または
	`RP/0/RSP0/CPU0:router(config-rsvp-if-auth)# commit`
		設定変更を保存します。
		• **end** コマンドを実行すると、変更をコミットするように要求されます。
		`Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:`
		◦ **yes** と入力すると、実行コンフィギュレーション ファイルに変更が保存され、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。
		◦ **no** と入力すると、コンフィギュレーションセッションが終了して、ルータが EXEC モードに戻ります。変更はコミットされません。
		◦ **cancel** と入力すると、現在のコンフィギュレーション セッションが継続します。コンフィギュレーション セッションは終了せず、設定変更もコミットされません。
		• 実行コンフィギュレーション ファイルに変更を保存し、コンフィギュレーション セッションを継続するには、**commit** コマンドを使用します。

関連トピック

RSVP 認証設計, （8 ページ）
すべてのモードを使用した RSVP 認証：例, （51 ページ）

RSVP 認証用インターフェイスのウィンドウ サイズの設定

次のタスクを実行して、RSVP 認証のインターフェイスのウィンドウ サイズを設定して、受信したシーケンス番号の有効性をチェックします。

手順の概要

1. **configure**
2. **rsvp interface** *type interface-path-d*
3. **authentication**
4. **window-size** *N*
5. 次のいずれかのコマンドを使用します。
   - **end**
   - **commit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure** 例： `RP/0/RSP0/CPU0:router# configure`	グローバル コンフィギュレーション モードを開始します。

ステップ 2	**rsvp interface** *type interface-path-d*
	
	例：
	`RP/0/RSP0/CPU0:router(config)# rsvp interface POS 0/2/1/0`
	`RP/0/RSP0/CPU0:router(config-rsvp-if)#`
		RSVP インターフェイス コンフィギュレーション モードを開始します。

ステップ 3	**authentication**
	
	例：
	`RP/0/RSP0/CPU0:router(config-rsvp-if)# authentication`
	`RP/0/RSP0/CPU0:router(config-rsvp-if-auth)#`
		RSVP インターフェイス認証コンフィギュレーション モードを開始します。

ステップ 4	**window-size** *N* 例： `RP/0/RSP0/CPU0:router(config-rsvp-if-auth)# window-size 33`	受信できるシーケンス外の RSVP 認証済みメッセージの最大数を指定します。 ***N*** シーケンス外のメッセージを制限するウィンドウのサイズ。 範囲は 1 ～ 64 です。 デフォルト値は 1 であり、この場合すべてのシーケンス外メッセージがドロップされます。

	コマンドまたはアクション	目的

ステップ 5	次のいずれかのコマンドを使用します。
	• **end**
	• **commit**
	
	例：
	`RP/0/RSP0/CPU0:router(config-rsvp-if-auth)# end`
	または
	`RP/0/RSP0/CPU0:router(config-rsvp-if-auth)# commit`
		設定変更を保存します。
		• **end** コマンドを実行すると、変更をコミットするように要求されます。
		`Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:`
		◦ **yes** と入力すると、実行コンフィギュレーション ファイルに変更が保存され、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。
		◦ **no** と入力すると、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。変更はコミットされません。
		◦ **cancel** と入力すると、現在のコンフィギュレーション セッションが継続します。コンフィギュレーション セッションは終了せず、設定変更もコミットされません。
		• 実行コンフィギュレーション ファイルに変更を保存し、コンフィギュレーション セッションを継続するには、**commit** コマンドを使用します。

関連トピック

ウィンドウ サイズおよびシーケンス外のメッセージに関するガイドライン，（12 ページ）
すべてのモードを使用した RSVP 認証：例，（51 ページ）
インターフェイスの RSVP 認証：例，（50 ページ）

RSVP ネイバー認証の設定

次のタスクでは、RSVP ネイバー認証を設定する方法について説明します。

• RSVP ネイバー認証用キーチェーンの指定，（39 ページ）
• RSVP ネイバー認証のライフタイムの設定，（40 ページ）
• RSVP ネイバー認証用ウィンドウ サイズの設定，（42 ページ）

RSVP ネイバー認証用キーチェーンの指定

次のタスクを実行して、キーチェーン RSVP ネイバー認証を指定します。

最初にキーチェーンを指定する必要があります（『*Cisco ASR 9000 Series Aggregation Services Router System Security Configuration Guide* 』を参照）。

手順の概要

1. **configure**
2. **rsvp neighbor** *IP-address* **authentication**
3. **key-source key-chain** *key-chain-name*
4. 次のいずれかのコマンドを使用します。
   - **end**
   - **commit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure** 例： `RP/0/RSP0/CPU0:router# configure`	グローバル コンフィギュレーション モードを開始します。

ステップ 2	**rsvp neighbor** *IP-address* **authentication**
	
	例：
	`RP/0/RSP0/CPU0:router(config)# rsvp neighbor 1.1.1.1 authentication`
	`RP/0/RSP0/CPU0:router(config-rsvp-nbor-auth)#`
		ネイバー認証コンフィギュレーション モードを開始します。 **rsvp neighbor** コマンドを使用して、ネイバーの RSVP 暗号認証をアクティブにします。
		IP address
		ネイバーの IP アドレス。 特定のネイバーの単一 IP アドレスです。通常は、ネイバーの物理インターフェイスまたは論理（ループバック）インターフェイスのいずれかです。
		authentication
		RSVP 認証パラメータを設定します。

ステップ 3	**key-source key-chain** *key-chain-name* 例： `RP/0/RSP0/CPU0:router(config-rsvp-nbor-auth)#`	RSVP シグナリング メッセージを認証するキー情報のソースを指定します。 ***key-chain-name*** キーチェーンの名前。 最大文字数は 32 です。

	コマンドまたはアクション	目的
	key-source key-chain mpls-keys	

ステップ 4	次のいずれかのコマンドを使用します。
	• **end**
	• **commit**
	例：
	`RP/0/RSP0/CPU0:router(config-rsvp-nbor-auth)# end`
	または
	`RP/0/RSP0/CPU0:router(config-rsvp-nbor-auth)# commit`
		設定変更を保存します。
		• **end** コマンドを実行すると、変更をコミットするように要求されます。
		`Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:`
		◦ **yes** と入力すると、実行コンフィギュレーション ファイルに変更が保存され、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。
		◦ **no** と入力すると、コンフィギュレーションセッションが終了して、ルータが EXEC モードに戻ります。変更はコミットされません。
		◦ **cancel** と入力すると、現在のコンフィギュレーションセッションが継続します。コンフィギュレーションセッションは終了せず、設定変更もコミットされません。
		• 実行コンフィギュレーション ファイルに変更を保存し、コンフィギュレーション セッションを継続するには、**commit** コマンドを使用します。

関連トピック

Key-source Key-chain, （12 ページ）
セキュリティ アソシエーション, （10 ページ）
RSVP ネイバー認証：例, （51 ページ）

RSVP ネイバー認証のライフタイムの設定

次のタスクを実行して、RSVP ネイバー認証モードのセキュリティ アソシエーションのライフタイムを設定します。

手順の概要

1. **configure**
2. **rsvp neighbor** *IP-address* **authentication**
3. **life-time** *seconds*
4. 次のいずれかのコマンドを使用します。
   - **end**
   - **commit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure** 例： `RP/0/RSP0/CPU0:router# configure`	グローバル コンフィギュレーション モードを開始します。

ステップ 2	**rsvp neighbor** *IP-address* **authentication**
	
	例：
	`RP/0/RSP0/CPU0:router(config)# rsvp neighbor 1.1.1.1 authentication`
	`RP/0/RSP0/CPU0:router(config-rsvp-nbor-auth)#`
		RSVP ネイバー認証コンフィギュレーション モードを開始します。 **rsvp neighbor** コマンドを使用して、RSVP のネイバーを指定します。
		IP address
		ネイバーの IP アドレス。 特定のネイバーの単一 IP アドレスです。通常は、ネイバーの物理インターフェイスまたは論理（ループバック）インターフェイスのいずれかです。
		authentication
		RSVP 認証パラメータを設定します。

ステップ 3	**life-time** *seconds* 例： `RP/0/RSP0/CPU0:router(config-rsvp-nbor-auth)# life-time 2000`	信頼できる他の RSVP ネイバーとのセキュリティ アソシエーションを RSVP が保持する期間を制御します。 引数は次のものを指定します。 ***seconds*** 信頼できる他の RSVP ネイバーとのアイドルなセキュリティ アソシエーションを RSVP が保持する期間（秒単位）。 指定できる値の範囲は 30 ～ 86400 です。 デフォルト値は 1800 です。
ステップ 4	次のいずれかのコマンドを使用します。	設定変更を保存します。

	コマンドまたはアクション	目的

	• **end**
	• **commit**
	
	例：
	`RP/0/RSP0/CPU0:router(config-rsvp-nbor-auth)# end`
	または
	`RP/0/RSP0/CPU0:router(config-rsvp-nbor-auth)# commit`
		• **end** コマンドを実行すると、変更をコミットするように要求されます。
		`Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:`
		◦ **yes** と入力すると、実行コンフィギュレーション ファイルに変更が保存され、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。
		◦ **no** と入力すると、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。変更はコミットされません。
		◦ **cancel** と入力すると、現在のコンフィギュレーション セッションが継続します。コンフィギュレーション セッションは終了せず、設定変更もコミットされません。
		• 実行コンフィギュレーション ファイルに変更を保存し、コンフィギュレーション セッションを継続するには、**commit** コマンドを使用します。

関連トピック

セキュリティ アソシエーション，（10 ページ）
RSVP 認証グローバル コンフィギュレーション モード：例，（50 ページ）

RSVP ネイバー認証用ウィンドウ サイズの設定

次のタスクを実行して、RSVP ネイバー認証のウィンドウ サイズを設定して、受信したシーケンス番号の有効性をチェックします。

手順の概要

1. **configure**
2. **rsvp neighbor** *IP address* **authentication**
3. **window-size** *N*
4. 次のいずれかのコマンドを使用します。
   - **end**
   - **commit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure** 例： `RP/0/RSP0/CPU0:router# configure`	グローバルコンフィギュレーションモードを開始します。

ステップ 2	**rsvp neighbor** *IP address* **authentication**
	
	例：
	
	`RP/0/RSP0/CPU0:router(config)# rsvp neighbor 1.1.1.1 authentication`
	`RP/0/RSP0/CPU0:router(config-rsvp-nbor-auth)#`
		RSVP ネイバー認証コンフィギュレーションモードを開始します。 **rsvp neighbor** コマンドを使用して、RSVP のネイバーを指定します。
		
		IP address
		
		ネイバーの IP アドレス。 特定のネイバーの単一 IP アドレスです。通常は、ネイバーの物理インターフェイスまたは論理（ループバック）インターフェイスのいずれかです。
		
		authentication
		
		RSVP 認証パラメータを設定します。

ステップ 3	**window-size** *N* 例： `RP/0/RSP0/CPU0:router(config-rsvp-nbor-auth)# window-size 33`	受信されるシーケンス外の RSVP 認証済みメッセージの最大数を指定します。 ***N*** シーケンス外のメッセージを制限するウィンドウのサイズ。 範囲は 1 ～ 64 です。 デフォルト値は 1 であり、この場合すべてのシーケンス外メッセージがドロップされます。
ステップ 4	次のいずれかのコマンドを使用します。	設定変更を保存します。

	コマンドまたはアクション	目的

	• **end**
	• **commit**
	
	例：
	`RP/0/RSP0/CPU0:router(config-rsvp-nbor-auth)# end`
	または
	`RP/0/RSP0/CPU0:router(config-rsvp-nbor-auth)# commit`
		• **end** コマンドを実行すると、変更をコミットするように要求されます。
		`Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:`
		◦ **yes** と入力すると、実行コンフィギュレーション ファイルに変更が保存され、コンフィギュレーション セッションが終了して、ルータが EXEC モードに戻ります。
		◦ **no** と入力すると、コンフィギュレーションセッションが終了して、ルータが EXEC モードに戻ります。変更はコミットされません。
		◦ **cancel** と入力すると、現在のコンフィギュレーション セッションが継続します。コンフィギュレーション セッションは終了せず、設定変更もコミットされません。
		• 実行コンフィギュレーション ファイルに設定変更を保存し、コンフィギュレーション セッションを継続するには、**commit** コマンドを使用します。

関連トピック

ウィンドウ サイズおよびシーケンス外のメッセージに関するガイドライン, （12 ページ）
すべてのモードを使用した RSVP 認証：例, （51 ページ）
インターフェイスの RSVP 認証：例, （50 ページ）

RSVP 認証の詳細の確認

RSVP により確立される他の RSVP ネイバーとのセキュリティ アソシエーションを表示するには、**show rsvp authentication** コマンドを使用します。

RSVP 認証のセキュリティ アソシエーションの削除

RSVP 認証 SA を削除するには、**clear rsvp authentication** コマンドを使用します。 各 SA の RSVP カウンタを削除するには、**clear rsvp counters authentication** コマンドを使用します。

RSVP の設定例

サポートされている RSVP 機能の一部に関する RSVP の設定例を示します。

帯域幅設定（先行標準）：例

次に、先行標準DS-TEモードを使用したインターフェイスの帯域幅の設定例を示します。この例では、7500 の予約可能な帯域幅インターフェイスを設定し、1 つのフローの最大帯域幅を 1000 に指定して、2000 のサブプール帯域幅を追加します。

```
rsvp interface pos 0/3/0/0
 bandwidth 7500 1000 sub-pool 2000
```

帯域幅設定（MAM）：例

次に、MAMを使用したインターフェイスの帯域幅の設定例を示します。次に、POSインターフェイス 0/3/0/0 上のすべての RSVP 予約の合計を 7500 kbps に制限し、個々のフローの予約は 1000 kbps 以下とする例を示します。

```
rsvp interface pos 0/3/0/0
 bandwidth mam 7500 1000
```

関連トピック

DiffServ-TE 帯域幅の確認, （14 ページ）
差別化サービス トラフィック エンジニアリング

帯域幅設定（RDM）：例

次に、RDM を使用したインターフェイスの帯域幅の設定例を示します。次に、POS インターフェイス 0/3/0/0 上のすべての RSVP 予約の合計を 7500 kbps に制限し、個々のフローの予約は 1000 kbps 以下とする例を示します。

```
rsvp interface pos 0/3/0/0
 bandwidth rdm 7500 1000
```

関連トピック

DiffServ-TE 帯域幅の確認, （14 ページ）
差別化サービス トラフィック エンジニアリング

リフレッシュ削減および信頼性の高いメッセージング設定：例

RFC 2961 で定義されているリフレッシュ削減機能は、デフォルトでサポートされ、イネーブルです。次に、リフレッシュ削減機能の設定例を示します。リフレッシュ削減は、ネイバーでもサポートされている場合に限り、ネイバーで使用されます。

更新インターバルおよびリフレッシュ メッセージ数の設定：例

次に、POS 0/3/0/0 でのリフレッシュ インターバルを 30 秒に設定する例、およびノードがステートをクリーンアップする前に欠落できるリフレッシュ メッセージの数をデフォルト値の 4 から 6 に変更する例を示します。

```
rsvp interface pos 0/3/0/0
 signalling refresh interval 30
 signalling refresh missed 6
```

信頼性の高いメッセージング設定で使用される再送信時間：例

次に、再送信タイマーを 2 秒に設定する例を示します。不要な再転送を防止するには、インターフェイスで設定されている再転送時間値が、そのピアの ACK 保持時間より長くなければなりません。

```
rsvp interface pos 0/4/0/1
 signalling refresh reduction reliable retransmit-time 2000
```

確認応答時間の設定：例

次に、確認保持時間をデフォルト値の 400 ms から変更して ACK 送信を遅くする、または速くする例と、最大確認メッセージ サイズをデフォルト サイズの 4096 バイトから変更する例を示しま

す。 次に、確認保持時間をデフォルト値の 400 ms から変更する例と、ACK の送信を遅く、または速くする例を示します。 最大確認メッセージのデフォルト サイズは 4096 バイトです。

```
rsvp interface pos 0/4/0/1
 signalling refresh reduction reliable ack-hold-time 1000
rsvp interface pos 0/4/0/1
 signalling refresh reduction reliable ack-max-size 1000
```

（注） 不要な再転送を防ぐために、ピアのインターフェイスの再転送時間が、ACK 保持時間の 2 倍であることを確認してください。

サマリー リフレッシュ メッセージ サイズ設定：例

次に、サマリー リフレッシュ メッセージの最大サイズを 1500 バイトに設定する例を示します。

```
rsvp interface pos 0/4/0/1
 signalling refresh reduction summary max-size 1500
```

リフレッシュ削除のディセーブル化：例

ピア ノードでリフレッシュ削除がサポートされていない場合、またはその他の理由でインターフェイスのリフレッシュ削減をディセーブルにする場合、次のインターフェイスでリフレッシュ削減をディセーブルにする例を参照してください。

```
rsvp interface pos 0/4/0/1
 signalling refresh reduction disable
```

グレースフル リスタートの設定：例

RSVP グレースフル リスタートは、グローバルまたはインターフェイスごとに（リフレッシュ関連パラメータとして）設定されます。 次に、グレースフル リスタートをイネーブルにし、リスタート時間を設定して、hello メッセージ インターバルを変更する例を示します。

グレースフル リスタートのイネーブル化：例

次に、デフォルトで RSVP グレースフル リスタート機能をイネーブルにする例を示します。 ディセーブルの場合、次のコマンドを使用してイネーブルにします。

```
rsvp signalling graceful-restart
```

関連トピック

グレースフル リスタートのイネーブル化, （16 ページ）
グレースフル リスタート：標準およびインターフェイスベース, （4 ページ）

インターフェイスベースのグレースフル リスタートのイネーブル化：例

次に、インターフェイスで RSVP グレースフル リスタート機能をイネーブルにする例を示します。

```
signalling hello graceful-restart interface-based
```

関連トピック

グレースフル リスタートのイネーブル化，（16 ページ）
グレースフル リスタート：標準およびインターフェイスベース，（4 ページ）

再起動時間の変更：例

次に、ネイバー ノードに送信される hello メッセージでアドバタイズされる再起動時間を変更する例を示します。

```
rsvp signalling graceful-restart restart-time 200
```

hello インターバルの変更：例

次に、RSVP グレースフル リスタート hello メッセージがネイバーごとに送信されるインターバルを変更し、ネイバーがダウンと宣言される前に欠落する hello メッセージの数を変更する例を示します。

```
rsvp signalling hello graceful-restart refresh interval 4000
rsvp signalling hello graceful-restart refresh misses 4
```

ACL ベース プレフィックス フィルタリングの設定：例

次に、RSVP がローカル アドレスではない送信元アドレス 1.1.1.1 からルータ アラート（RA）パケットを受信する例を示します。 パケットは、IP TTL を減少して転送されます。 2.2.2.2 を宛先とするパケットがドロップされます。 その他のすべての RA パケットは、通常の RSVP パケットです。

```
show run ipv4 access-list
  ipv4 access-list rsvpacl
  10 permit ip host 1.1.1.1 any
  20 deny ip any host 2.2.2.2
  !
show run rsvp
  rsvp
  signalling prefix-filtering access-list rsvpacl
  !
```

関連トピック

プレフィックス フィルタリング用の ACL 設定，（18 ページ）
ACL ベース プレフィックス フィルタリング，（6 ページ）

RSVP パケットの DSCP の設定：例

次に、RSVP パケットの IP ヘッダーのディファレンシエーテッド サービス コード ポイント（DSCP）フィールドを設定する例を示します。

```
rsvp interface pos0/2/0/1
 signalling dscp 20
```

関連トピック

RSVP パケット ドロップの設定, （20 ページ）
MPLS-TE 用 RSVP の概要 , （2 ページ）

RSVP トラップのイネーブル化：例

次に、ルータがすべての RSVP トラップを送信できるように設定する例を示します。

```
configure
 snmp-server traps rsvp all
```

次に、ルータが RSVP LostFlow トラップを送信できるように設定する例を示します。

```
configure
 snmp-server traps rsvp lost-flow
```

次に、ルータが RSVP RSVP NewFlow トラップを送信できるように設定する例を示します。

```
configure
 snmp-server traps rsvp new-flow
```

関連トピック

RSVP トラップの有効化, （25 ページ）
RSVP MIB, （7 ページ）

RSVP 認証の設定例

次の設定例は、RSVP 認証に使用されます。

- RSVP 認証グローバル コンフィギュレーション モード：例, （50 ページ）
- インターフェイスの RSVP 認証：例, （50 ページ）
- RSVP ネイバー認証：例, （51 ページ）
- すべてのモードを使用した RSVP 認証：例, （51 ページ）

RSVP 認証グローバル コンフィギュレーション モード：例

次に、すべての RSVP メッセージの認証をイネーブルにし、SA のデフォルト ライフタイムを増加する例を示します。

```
rsvp
 authentication
  key-source key-chain default_keys
  life-time 3600
 !
!
```

（注） 指定されるキーチェーン（default_keys）が存在し、これに有効なキーが含まれている必要があります。そうでない場合、シグナリングは失敗します。

関連トピック

グローバル コンフィギュレーション モードでキーチェーンを使用した RSVP 認証のイネーブル化, （27 ページ）
Key-source Key-chain, （12 ページ）
グローバル コンフィギュレーション モードでの RSVP 認証のライフタイムの設定, （29 ページ）
グローバル、インターフェイス、およびネイバー認証モード, （9 ページ）
RSVP ネイバー認証のライフタイムの設定, （40 ページ）
セキュリティ アソシエーション, （10 ページ）

インターフェイスの RSVP 認証：例

次に、1 つだけのインターフェイスで送受信されるすべての RSVP メッセージの認証をイネーブルにして、SA のウィンドウ サイズを設定する例を示します。

```
rsvp
 interface GigabitEthernet0/6/0/0
  authentication
   window-size 64
  !
 !
```

（注） キーソース キーチェーン設定が指定されていないので、グローバル認証モード キーチェーンが使用および継承されます。 グローバル キーチェーンが存在し、これに有効なキーが含まれている必要があります。そうでない場合、シグナリングは失敗します。

関連トピック

グローバル コンフィギュレーション モードでの RSVP 認証のウィンドウ サイズの設定，（31 ページ）
RSVP 認証用インターフェイスのウィンドウ サイズの設定，（36 ページ）
RSVP ネイバー認証用ウィンドウ サイズの設定，（42 ページ）
ウィンドウ サイズおよびシーケンス外のメッセージに関するガイドライン，（12 ページ）

RSVP ネイバー認証：例

次に、特定の IP アドレスだけで送受信されるすべての RSVP メッセージの認証をイネーブルにする例を示します。

```
rsvp
 neighbor 10.0.0.1
  authentication
   key-source key-chain nbr_keys
  !
 !
!
```

関連トピック

RSVP ネイバー認証用キーチェーンの指定，（39 ページ）
Key-source Key-chain，（12 ページ）
セキュリティ アソシエーション，（10 ページ）

すべてのモードを使用した RSVP 認証：例

この設定例では、次の機能を実行する方法を示します。

- すべての RSVP メッセージを認証します。
- **key-source key-chain** コマンドを nbr_keys に設定して、10.0.0.1 間での RSVP メッセージを認証します。SA ライフタイムは 3600 に設定されます。デフォルトのウィンドウ サイズは 1 に設定されます。
- **key-source key-chain** コマンドを default_keys に設定して、10.0.0.1 間での RSVP メッセージを認証します。SA ライフタイムは 3600 に設定されます。ウィンドウ サイズは、GigabitEthernet0/6/0/0 を使用する場合は 64 に設定され、それ以外の場合はデフォルト値の 1 が使用されます。

```
rsvp
 interface GigabitEthernet0/6/0/0
  authentication
   window-size 64
  !
 !
 neighbor 10.0.0.1
  authentication
```

```
    key-source key-chain nbr_keys
   !
  !
  authentication
   key-source key-chain default_keys
   life-time 3600
  !
 !
```

（注） キーチェーンが存在しない場合、または有効なキーが含まれていない場合、シグナリングが失敗するので、設定エラーが発生します。 ただし、これはシグナリングを防止するためです。たとえば、上記の例の場合、nbr_keys に有効なキーが含まれていない場合、10.0.0.1 でのすべてのシグナリングが失敗します。

関連トピック

グローバル コンフィギュレーション モードでの RSVP 認証のウィンドウ サイズの設定，（31 ページ）
RSVP 認証用インターフェイスのウィンドウ サイズの設定，（36 ページ）
RSVP ネイバー認証用ウィンドウ サイズの設定，（42 ページ）
ウィンドウ サイズおよびシーケンス外のメッセージに関するガイドライン，（12 ページ）
インターフェイス モードでの RSVP 認証キーチェーンの指定，（33 ページ）
グローバル、インターフェイス、およびネイバー認証モード，（9 ページ）
RSVP 認証用インターフェイスのライフタイムの設定，（35 ページ）
RSVP 認証設計，（8 ページ）

その他の参考資料

次に、MPLS RSVP 実装に関連する参考資料を示します。

関連資料

関連項目	参照先
Cisco IOS XR MPLS RSVP コマンド	『*Cisco ASR 9000 Series Aggregation Services Router MPLS Command Reference*』の「*RSVP Infrastructure Commands on Cisco ASR 9000 Series Router*」モジュール
スタートアップ資料	『*Cisco ASR 9000 Series Aggregation Services Router Getting Started Guide*』
ユーザ グループとタスク ID に関する情報	『』の「*Configuring AAA Services on Cisco ASR 9000 Series Router*」モジュール

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	—

MIB

MIB	MIB のリンク
—	Cisco IOS XR softwareを使用して MIB を検出およびダウンロードするには、次の URL から Cisco MIB Locator を使用して、[Cisco Access Products] メニューでプラットフォームを選択します。 http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

RFC

RFC	タイトル
RFC 2205	『*Resource Reservation Protocol Version 1 Functional Specification*』
RFC 2206	『*RSVP Management Information Base using SMIv2*』
RFC 2747	『*RSVP Cryptographic Authentication*』
RFC 2961	『*RSVP Refresh Overhead Reduction Extensions*』
RFC 3209	『*RSVP-TE: Extensions to RSVP for LSP Tunnels*』
RFC 3473	『*Generalized MPLS Signaling, RSVP-TE Extensions*』
RFC 4090	『*Fast Reroute Extensions to RSVP-TE for LSP Tunnels*』

シスコのテクニカル サポート

説明	リンク
シスコのテクニカル サポート Web サイトには、数千ページに及ぶ検索可能な技術情報があります。製品、テクノロジー、ソリューション、技術的なヒント、およびツールへのリンクもあります。 Cisco.com に登録済みのユーザは、このページから詳細情報にアクセスできます。	http://www.cisco.com/techsupport