サーバ ロード バランシングの設定

このマニュアルでは、Cisco IOS Server Load Balancing（IOS SLB）機能の設定方法について説明します。この章の IOS SLB コマンドの詳細な説明については、『*Cisco IOS IP Application Services Command Reference*』の「Server Load Balancing Commands」の章を参照してください。この章に記載されている他のコマンドのマニュアルを探すには、コマンド リファレンス マスター インデックスを使用するか、オンラインで検索してください。

SLB 機能は、IP サーバのロード バランシングを実現する Cisco IOS ベースのソリューションです。

IOS SLB 機能の使用方法

1. ネットワーク管理者は、IOS SLB 機能を使用して*仮想*サーバを定義します。仮想サーバとは、*サーバ ファーム*と呼ばれるネットワーク サーバのクラスタ内にある*実*サーバのグループです。この環境では、クライアントが仮想サーバの IP アドレスに接続するように設定されます。
2. 仮想サーバの IP アドレスは、各実サーバのループバック アドレスまたはセカンダリ IP アドレスとして設定されます。
3. クライアントが仮想サーバへの接続を開始すると、設定されているロード バランシング アルゴリズムに基づいて、接続する実サーバを IOS SLB 機能が選択します。

IOS SLB 機能には、次のように、多様なネットワーク デバイスおよびサービスに適したロード バランシングが用意されています。

- Hypertext Transfer Protocol（HTTP; ハイパーテキスト転送プロトコル）、Telnet、File Transfer Protocol（FTP; ファイル転送プロトコル）などのアプリケーション サーバ
- ファイアウォール
- Authentication, Authorization, and Accounting（AAA; 認証、認可、アカウンティング）、サーバ、Web キャッシュなどのサービス ノード

さらに、IOS SLB Exchange Director では、その他にも次のサービス ノードに適した高度なロード バランシング ルーティング機能を使用できます。

- mobile Service Exchange Framework（mSEF）コンポーネント：
  - Cisco Content Services Gateway（CSG）

    Supervisor Engine 32（SUP32-MSFC2A）とともに実行している場合、CSG Release 3.1(3)C7(1) 以降が必要です。
  - Cisco Gateway General Packet Radio Service（GPRS）Support Node（GGSN）
  - Cisco Service Selection Gateway（SSG）
  - Cisco Home Agent

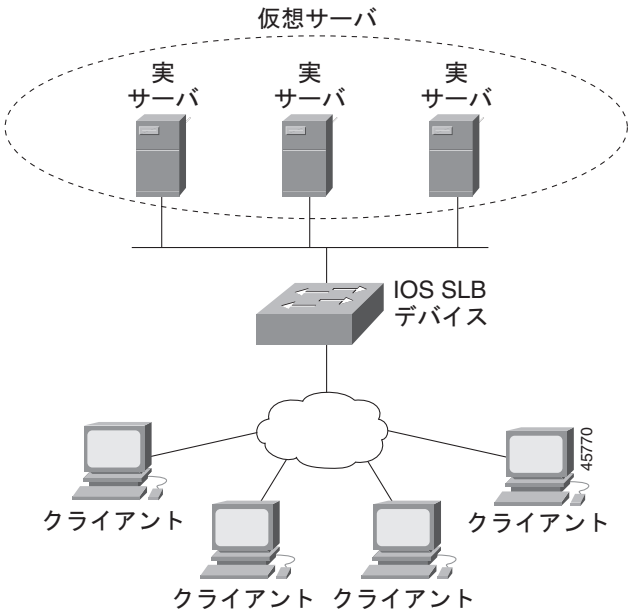
- モバイル、Public Wireless LAN（PWLAN; パブリック ワイヤレス LAN）、およびサービス プロバイダー ネットワーク用のその他のコンポーネント：
  - Wireless Application Protocol（WAP; ワイヤレス アプリケーション プロトコル）ゲートウェイ
  - プロトコル最適化ゲートウェイ
  - 他社製 GGSN および Home Agent
  - 他の RADIUS 対応フロー ゲートウェイ。これらのゲートウェイは、ゲートウェイを介してユーザに送信されるルートの RADIUS 認可要求およびアカウンティング要求を受信するプロキシまたはルーティング ノードです。Exchange Director は RADIUS およびデータ フローを同じゲートウェイにバインドし、ユーザのネットワーク アクティビティの完全で一貫したビューをゲートウェイが受信できるようにします。

また、Exchange Director には次の機能もあります。

- Cisco Catalyst 6500 シリーズ スイッチおよび Cisco 7600 シリーズ ルータの mSEF 内部の単一シャーシ フェールオーバー用に強化されたフェールオーバー機能。Route Processor Redundancy Plus（RPR+）とともに使用すると、冗長ルート プロセッサの IOS SLB ステートフル バックアップで、これらのプラットフォーム向けのフル IOS SLB ステートフル フェールオーバー機能が実現します。
- フローが永続的になるため、負荷が分散された IP フローの高度なリターン ルーティングが実現します。

図 1 に、単純な IOS SLB ネットワークを示します。

図 1　　Cisco IOS SLB の論理構成図



機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。この章に記載されている機能の詳細、および各機能がサポー

トされているリリースのリストについては、「IOS SLB の機能情報」（P.194）を参照してください。

プラットフォーム サポートとシスコ ソフトウェア イメージ サポートに関する情報を入手するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

この章の構成

Cisco IOS SLB に関する制約事項

一般的な制約事項

- *同じローカルエリア ネットワーク（LAN）または virtual LAN（VLAN）上にあるクライアントと実サーバ間のフローのロード バランシングはサポートされません。同じインターフェイス上のロード バランシング デバイスには、ロード バランシング対象のパケットを入出力できません。*
- 複数のユーザ セッションから同時に IOS SLB を設定することはできません。
- 実サーバの IP アドレスを含むすべてのサーバ ファームが **nat server** コマンドを使用して設定されている場合を除き、実サーバの IP アドレスと同じサブネット上に IOS SLB 仮想 IP アドレスを設定しないでください。
- スタンドアロン モードで動作します。また、現在、MultiNode Load Balancing（MNLB）Services Manager として動作していません。異なるサービス用であっても、同じ仮想 IP アドレスで設定されている IOS SLB および MNLB はサポートされません。IOS SLB を使用する場合でも、MNLB 環境で外部サービス マネージャ（LocalDirector など）による既存の MNLB フォワーディング エージェントを使用できます（MNLB は Cisco Application Services Architecture（CASA）とも呼ばれます）。
- バックアップ機能用の複数の IOS SLB インスタンスに関するサーバのロード バランシング統計情報の調整はサポートされません。
- FTP およびファイアウォール ロード バランシングは、dispatched モードでのみサポートされます。
- Dynamic Host Configuration Protocol（DHCP）のロード バランシングはサポートされません。
- Internet Protocol version 6（IPv6）はサポートされません。
- dispatched モードで動作している場合は、実サーバをレイヤ 2 隣接、タグスイッチ型、または GRE トンネル経由にする必要があります。

  サーバ NAT を使用して directed モードで実行している場合、実サーバは IOS SLB に対してレイヤ 2 隣接にする必要はありません。この機能によって、IOS SLB スイッチから数レイヤ 3 ホップ離れたところにサーバを配置できるため、ネットワーク設計が柔軟になります。

- マルチキャスト グループのメンバとして directed モードで実行されている場合、IOS SLB はマルチキャスト フローを受信できますが、マルチキャスト フローの送信はできません。dispatched モードで実行される場合、これは制限ではありません。
- TCP および UDP 仮想サーバに対してのみ、クライアント Network Address Translation（NAT; ネットワーク アドレス変換）とサーバ ポート変換をサポートします。
- IOS インターフェイス IP アドレスのいずれかと同じ仮想 IP アドレスへのストリームのバランスを取る場合（ループバックやイーサネットなど）は、IOS SLB が、そのアドレスへのすべての UDP パケットをトレースルート パケットとして扱い、「ホスト到達不能」ICMP パケットを使用して応答します。この問題は、IOS が対象 UDP ポートをリスンしている場合でも発生します。この問題を回避するには、仮想サーバをホスト（address/32）ではなくネットワーク（address/31）として設定します。
- IOS SLB 仮想サーバで設定した仮想 IP アドレスは、SNMP などの UDP ベースのルータ管理アプリケーションに使用しないでください。使用すると、CPU の使用率が高くなる可能性があります（これは、宛先ポート番号 0 で設定した UDP 仮想サーバの問題ではありません）。
- DFP エージェントには 3 秒以上の hello メッセージが必要です。そのため、DFP マネージャがタイムアウトを指定した場合、3 秒以上のタイムアウトを設定する必要があります。
- IOS SLB と Web Cache Communication Protocol（WCCP）の両方が Cisco Catalyst 6500 シリーズ スイッチ上に設定されており、WCCP Input Redirection が IOS SLB を使用して設定されている場合は、ルータとキャッシュ間でレイヤ 2 WCCP フォワーディングを使用する必要があります。この場合、WCCP および IOS SLB の両方がハードウェアで実行され、適切な順で処理されます。Generic Routing Encapsulation（GRE）フォワーディングを使用する場合、IOS SLB は WCCP よりも優先されます。また、MSFC で GRE フォワーディングが実行されるため、リダイレクトはありません。WCCP フォワーディング方式（レイヤ 2 または GRE）は、スイッチではなくキャッシュ エンジンで設定します。
- IOS SLB と Cisco Service Selection Gateway（SSG）は、同じデバイスに設定しないでください。
- 「サンドイッチ」設定（つまり、CSG、SSG、またはファイアウォールのファームの両側に IOS SLB が必要な設定）で、フローを 2 つの IOS SLB インスタンス（仮想サーバまたはファイアウォール ファーム）経由で転送しなければならない場合は、それらの IOS SLB インスタンスが別の Virtual Private Network（VPN; バーチャル プライベート ネットワーク）Routing and Forwarding（VRF）に存在している必要があります。
- サーバ ファーム、仮想サーバ、またはファイアウォール ファームのコンフィギュレーション モードで **access** コマンドを使用してアクセス インターフェイスを設定しない場合、VRF インターフェイスなど、デバイスのすべての使用可能なインターフェイスのサーバ ファーム、仮想サーバ、またはファイアウォール ファームについて、ワイルドカードがインストールされます。IOS SLB が VRF インターフェイスで必要ない場合、**access** コマンドを使用して、指定したインターフェイスにのみワイルドカードを制限します。
- VRF 認識 IOS SLB は VRF 間で動作しません。つまり、サーバ ファーム インターフェイスとクライアント トラフィック インターフェイスで同じ VRF を使用する必要があります。

スタティック NAT に関する制約事項

- クライアント NAT サーバ ファームと併用できません。つまり、実サーバでサーバ NAT に仮想 IP アドレスが使用されており、サーバ ファームがそれと同じ仮想 IP アドレスに関連付けられている場合は、クライアント NAT を使用するようにサーバ ファームを設定することができません。
- 各実サーバは 1 つの仮想サーバにのみ関連付ける必要があります。これは、IOS SLB が接続を適切に作成するためです。
- 0 ポートの仮想サーバが必要です。
- 仮想サービス FTP はサポートされません。
- パケット単位サーバ ロード バランシングを使用したスタティック NAT では、フラグメント化されたパケットが負荷分散されません。

バックアップ サーバ ファームに関する制約事項

- プライマリ サーバ ファームとバックアップ サーバ ファームの両方に同じ実サーバを定義する方法はサポートされません。
- プライマリ サーバ ファームとバックアップ サーバ ファームの両方に同じ NAT 設定（なし、クライアント、サーバ、または両方）が必要です。さらに、NAT を指定する場合、両方のサーバ ファームは同じ NAT プールを使用する必要があります。
- HTTP リダイレクト ロード バランシングはサポートされません。プライマリ サーバ ファームでリダイレクト仮想サーバを指定している場合、そのプライマリをバックアップとして定義できません。また、そのプライマリ用のバックアップを定義できません。

ファイアウォール ロード バランシングに関する制約事項

- ロード バランシング デバイスごとに 1 つずつのファイアウォール ファームに制限されません。
- 各ファイアウォールは固有の MAC アドレスを持つ必要があります。また、各デバイスに対してレイヤ 2 隣接にする必要があります。ファイアウォールはデバイス上の個々のインターフェイスに接続することも、すべてのファイアウォールが 1 つの VLAN を共有し、1 つのインターフェイスを使用して接続することもできます。
- それぞれのファイアウォール ロード バランシング デバイスとファイアウォール間に、イーサネット インターフェイスが必要です。
- IOS SLB は、それぞれのファイアウォール ロード バランシング デバイス上で、それぞれのレイヤ 2 ファイアウォールを 1 つのレイヤ 3（IP）インターフェイスに接続するように要求します。
- 設定したファイアウォールの IP アドレスと同じサブネット上にある宛先 IP アドレスを使用するフローの負荷は分散されません（たとえば、ファイアウォール コンソール セッションのフローや、ファイアウォール LAN 上のその他のフローです）。
- 次の IOS SLB 機能はサポートされません。
  - NAT
  - ポートバインド サーバ
  - SynGuard
  - TCP セッションの再割り当て
  - 透過的 Web キャッシュ ロード バランシング

GPRS Tunneling Protocol（GTP; GPRS トンネリング プロトコル）Cause Code Inspection がイネーブルになっていない GPRS ロード バランシングに関する制約事項

- 複数のサーバ ファームに 1 つの実サーバが定義されている場合、各サーバ ファームは異なる仮想サーバに関連付ける必要があります。
- dispatched または directed サーバ NAT モードでだけ動作します。
- スティッキ接続がイネーブルの場合にだけ、ステートフル バックアップがサポートされます。
- ネットワークから送信された PDP コンテキスト要求の負荷は分散できません。
- 次の IOS SLB 機能はサポートされません。
  - バインド ID（バインド ID を使用すれば、1 台の物理サーバを複数の仮想サーバにバインドして、サーバごとに加重を報告させることができます）
  - Client-Assigned ロード バランシング
  - スロー スタート
  - 加重最小接続ロード バランシング アルゴリズム

GTP Cause Code Inspection がイネーブルになっている GPRS ロード バランシングに関する制約事項

- 複数のサーバ ファームに 1 つの実サーバが定義されている場合、各サーバ ファームは異なる仮想サーバに関連付ける必要があります。
- directed サーバ NAT モードでだけ動作します。
- ネットワークから送信された PDP コンテキスト要求の負荷は分散できません。
- 受信シグナリングおよび発信シグナリングは IOS SLB を介して送信される必要があります。
- SGSN または GGSN からピアにエコーを送信する必要があります。
- 次の IOS SLB 機能はサポートされません。
  - バインド ID
  - Client-Assigned ロード バランシング
  - スロー スタート

GTP v2 に関する制約事項

- クライアント NAT をサポートしません。
- IOS SLB は、Packet data network GateWay（PGW）と Serving GateWay（SGW）向けの GTP v2 制御パケットを負荷分散することができます。PGW ロードバランシング デバイスと SGW ロード バランシング デバイスが同じスーパーバイザ エンジン内に設定されている場合は、デバイスごとに別々の仮想サーバを設定する必要があります。
- IOS SLB は、次の GTP v2 メッセージのみをチェックして処理します。
  - GTP_CREATE_SESSION_REQ
  - GTP_ECHO_REQ
  - GTP_SLB_NOTIFICATION

  その他のメッセージはすべてドロップされます。
- IOS SLB は、次の GTP_SLB 通知メッセージをサポートします。
  - GTP_SLB_NOTIF_REASSIGN_REAL
  - GTP_SLB_NOTIF_PDP_DELETION.
  - GTP_SLB_NOTIF_PDP_STATUS

VPN サーバ ロード バランシングに関する制約事項

- Internet Control Message Protocol（ICMP; インターネット制御メッセージ プロトコル）およびワイルドカード（0-protocol）仮想サーバはサポートされません。

RADIUS ロード バランシング加速データ プレーン フォワーディングに関する制約事項

- ルート マップ アルゴリズムが必要です。
- 最適な結果を得るには、冗長 CSG が必要です。
- 加入者のアドレスの範囲による負荷分散のスタティック プロビジョニングが必要です。
- 簡易な IP Access Control List（ACL; アクセス コントロール リスト）だけがサポートされます。
- VSA 関連付けが使用されている場合は、IOS SLB が、関連付け情報をアクティブな RADIUS ロード バランシング デバイスにだけ保存し、バックアップ RADIUS ロード バランシング デバイスには保存しません。バックアップ RADIUS ロード バランシング デバイスは、アクティブな RADIUS ロード バランシング デバイスから VSA 関連付け情報を受信しません。

- すべての Accounting-Request メッセージおよび Access-Accept メッセージには、RADIUS 割り当ての Framed-ip-address アトリビュートを含める必要があります。また、各加入者フローの発信元 IP アドレスは、Access-Accept メッセージの Framed-ip-address アトリビュートの値と一致する必要があります。
- RADIUS アカウンティングを RADIUS クライアント（一般的に Network Access Server（NAS））でイネーブルにする必要があります。
- SLB サーバ ファーム コンフィギュレーション モードで **predictor route-map** コマンドを指定する場合、SLB サーバ ファーム コンフィギュレーション モードまたは実サーバ コンフィギュレーション モードで他のコマンドは使用できません。

VSA 関連付けに関する制約事項

- VSA 関連付けの結果、パフォーマンスが低下することがあります。
- IOS SLB は関連付け情報をアクティブな RADIUS ロード バランシング デバイスにだけ維持します。バックアップ RADIUS ロード バランシング デバイスには維持しません。バックアップ RADIUS ロード バランシング デバイスは、アクティブな RADIUS ロード バランシング デバイスから VSA 関連付け情報を受信しません。
- Cisco VSA は、RADIUS Accounting-Start パケットに注入されます。その他の RADIUS メッセージまたはパケット（interim RADIUS Accounting ON または OFF メッセージや、RADIUS Accounting-Stop パケットなど）には注入されません。
- **radius inject acct** コマンドおよび **radius inject auth** コマンドは、同じ仮想サーバに設定できません。

GPRS 用の RADIUS ロード バランシングに関する制約事項

- 加重ラウンド ロビン アルゴリズムが必要です。
- フラグメント化された RADIUS パケットはサポートされません。
- すべての Accounting-Request メッセージおよび Access-Accept メッセージには、RADIUS 割り当ての Framed-ip-address アトリビュートを含める必要があります。また、各加入者フローの発信元 IP アドレスは、Access-Accept メッセージの Framed-ip-address アトリビュートの値と一致する必要があります。
- RADIUS アカウンティングを RADIUS クライアント（一般的に Network Access Server（NAS））でイネーブルにする必要があります。

CDMA2000 用の RADIUS ロード バランシングに関する制約事項

- 加重ラウンド ロビン アルゴリズムが必要です。
- フラグメント化された RADIUS パケットはサポートされません。
- モバイル ネットワークのすべての加入者には、モバイル ワイヤレス ネットワーク内でルーティング可能な、固有の IP アドレスを割り当てる必要があります（つまり、重複する IP アドレスがない状態）。
- User-Name アトリビュートは 1 人の加入者、または、多くても極少数の加入者に対応付ける必要があります。そうしなかった場合は、予想外に大きな負荷が 1 つの SSG にかかる可能性があります。
- 簡易 IP ネットワークの場合、さらに次の制約事項が適用されます。
  - PDSN は、すべての RADIUS Access-Request パケットおよび Accounting-Start パケットに User-Name アトリビュートを含める必要があります。加入者の User-Name アトリビュートの値は、すべてのパケットで同じにする必要があります（ただし、MSID ベースのアクセスを提供する Cisco PDSN は除きます）。

  - PDSN は、すべての RADIUS Accounting-Start パケットおよび Accounting-Stop パケットに Framed-ip-address アトリビュートおよび NAS-ip-address を含める必要があります。Framed-ip-address アトリビュートの値は、SSG サービスの RADIUS ロード バランシングによってルーティングされる加入者データ パケットの発信元 IP アドレスと同じにする必要があります。
  - PDSN は、すべての Accounting-Request に NAS-ip-address を含める必要があります。BSC/PCF ハンドオフの場合、Accounting-Stop には、**1** の値を指定した 3GPP2-Session-Continue VSA を含めることで、加入者の RADIUS ロード バランシング スティッキ接続 データベース オブジェクトの破壊を回避します。
- Mobile IP ネットワークの場合、さらに次の制約事項が適用されます。
  - 加入者セッションの場合は、PDSN と HA が、User-Name アトリビュートを含む RADIUS Access-Request パケットと Accounting-Start パケットを送信する必要があります。すべての PDSN パケットおよび HA RADIUS パケットの User-Name アトリビュート値は、そのセッションで同じにする必要があります。
  - 加入者セッションの場合は、PDSN と HA が、SSG サービス用の RADIUS ロード バランシングによってルーティングされる加入者データ パケット内の発信元 IP アドレスと同じ Framed-ip-address アトリビュートを含む RADIUS Accounting-Request パケットを送信する必要があります。PDSN および HA から送信されるすべての RADIUS Accounting-Requests には、NAS-ip-address アトリビュートも含める必要があります。
  - PDSN は、すべての Accounting-Requests に 3GPP2-Correlation-Identifier アトリビュートを含める必要があります。

Home Agent Director に関する制約事項

- Registration Request（RRQ）には、負荷分散対象の Network Access Identifier（NAI）を含める必要があります。
- RRQ には、負荷分散対象の 0.0.0.0 と 255.255.255.255 のどちらかのホーム エージェント IP アドレスを含める必要があります。
- ファースト スイッチングのために、パケットに含まれる RRQ の NAI は 96 バイト長を超えることはできません。NAI の深さが 96 バイトを超えている場合は、IOS SLB がプロセス レベルでパケットを管理します。
- dispatched または directed サーバ NAT モードでだけ動作します。
- 次の IOS SLB 機能はサポートされません。
  - バインド ID
  - Client-Assigned ロード バランシング
  - スロー スタート
  - ステートフル バックアップ
  - スティッキ接続
  - 加重最小接続ロード バランシング アルゴリズム

HTTP プローブに関する制約事項

- HTTP プローブは、HTTP over Secure Socket Layer（HTTPS）をサポートしません。つまり、HTTP プローブを SSL サーバに送信できません。

UDP プローブに関する制約事項

- UDP プローブは、フラグメント化された Response パケットをサポートしません。
- UDP プローブは、プローブ パケットに特定の発信元ポート値を必要とするホストをサポートしません。UDP プローブによって、各プローブ用に一時的なポートが選択されます。
- ペイロードから生成された Message Digest Algorithm Version 5（MD5）チェックサムがあるプロトコルおよびアプリケーションは、適切なチェックサムを取得するために、「スニファ」によってキャプチャする必要があります。
- Cisco IOS Multiprotocol Label Switching（MPLS）の場合：
  - Supervisor Engine 720 環境では、クライアントが MPLS クラウド経由で IOS SLB に接続できます。
  - MPLS クライアント インターフェイスは、トンネル エンジニアリングを使用して設定する必要があります。その他の MPLS 設定はサポートされません。
  - MPLS クライアント インターフェイスは、IP パケットとしてパケットを受信する必要があります。
  - MPLS クライアント インターフェイスは、Penultimate Hop Popping（PHP）ルータの背後に配置する必要があります。
- Cisco Catalyst 6500 シリーズ スイッチと Cisco 7600 シリーズ ルータの場合：
  - Native Cisco IOS のみをサポートします（c6sup イメージ）。Native Cisco IOS には、MSFC と Policy Feature Card（PFC; ポリシー フィーチャ カード）が必要です。同じ Catalyst 6500 スイッチ上で冗長 MSFC を実行している場合は、2 つの MSFC 間のステートフル バックアップはサポートされませんが、2 つの MSFC 間のステートレス バックアップはサポートされます。

    MSFC という用語は、特に区別されている場合を除き、MSFC1、MSFC2、または MSFC3 を指します。

    PFC という用語は、特に区別されている場合を除き、PFC1、PFC2、または PFC3 を指します。
  - Multilayer Switching（MLS; マルチレイヤ スイッチング）フロー モードは、フルフロー モードまたはインターフェイス フルフロー モードで動作する必要があります。IOS SLB は、固有に使用するフロー モードを自動的に設定します。MLS フローの設定方法については、『*Catalyst 6000 Family IOS Software Configuration Guide*』を参照してください。
  - dispatched モードで実行する場合、実サーバは、PFC によって実行されるハードウェア データ パケットのアクセラレーションを使用して、IOS SLB に対してレイヤ 2 隣接にする必要があります（つまり、追加のルータを超えません）。同じサーバ ファーム内のすべての実サーバは、同じ VLAN 上にある必要があります。実サーバでループバック アドレスを設定する必要があります。
  - ファイアウォール ファームのすべての実サーバは同じ VLAN 上にある必要があります。異なるファイアウォール ファームにある実サーバは、異なる VLAN に配置できます。
  - directed モードには、ハードウェア データ パケット アクセラレーション機能がありません（ハードウェア データ パケット アクセラレーションは PFC によって実行され、directed モードでは、パケットが PFC ではなく MSFC によって管理されます）。
  - Cisco Supervisor Engine 2 では、ファイアウォール ロード バランシングが必要な「サンドイッチ」設定がサポートされません。これは、このような設定には VRF が必要なためです。VRF は Supervisor Engine 2 に対してサポートされていません。

ASN Release 6 ロード バランシングに関する制約事項

- dispatched または directed サーバ NAT モードでだけ動作します。directed モードでは、IOS SLB が、Mobile Station Pre-Attachment 要求の宛先 IP アドレスを、選択された Access Service Network（ASN）ゲートウェイの実サーバの IP アドレスに変更します。
- DFP が必要です。
- 次の機能はサポートされません。
  - クライアント NAT
  - 加重最小接続アルゴリズム（Mobile Station Pre-Attachment 要求用）
- ベース ステーションが Pre-Attachment ACKnowledgement パケット、つまり、ACK パケットを直接 ASN ゲートウェイに送信して、IOS SLB をバイパスするように設定されている場合は、実サーバを停止することなくセッションがタイムアウトできるようにする必要があります。そのために、**no faildetect inband** コマンドの実サーバ コンフィギュレーション モードを設定します。
- ステートフル バックアップとスティッキ接続の場合：
  - ASN スティッキ接続は Cisco Broadband Wireless Gateway（BWG）Release 2.0 以降でのみサポートされます。
  - Cisco BWG 上で ASN を実行している場合は、**gw port** コマンドを仮想サーバ コンフィギュレーション モードで設定することを推奨します。
  - Cisco BWG と、ASN にロード バランシングを提供している IOS SLB 間の通信ポートとして、ポート番号の 2231 を使用しないでください。
  - Cisco BWG 上で ASN を実行していない場合は、**sticky** コマンドを仮想サーバ コンフィギュレーション モードで使用してスティッキ オブジェクトを削除する必要があります。これは、通知ポート上での delete 通知と NAI アップデート通知が想定されていないためです。
  - Cisco BWG から IOS SLB に ASN に関する通知を送信できるようにするには、Cisco BWG 上で **wimax agw slb port** コマンドをグローバル コンフィギュレーション モードで設定します。

（注） Cisco BWG コマンドについては、『*Cisco Broadband Wireless Gateway Command Reference*』に記載されています。

  - MSID が登録されている場合に、Cisco BWG から IOS SLB に NAI アップデート通知を送信できるようにするには、Cisco BWG 上で **wimax agw slb notify nai-updates** コマンドをグローバル コンフィギュレーション モードで設定します。
  - MSID が登録されていないか、削除されている場合に、Cisco BWG から IOS SLB に delete 通知を送信できるようにするには、Cisco BWG 上で **wimax agw slb notify session-deletion** コマンドをグローバル コンフィギュレーション モードで設定します。

Cisco IOS SLB に関する情報

IOS SLB を設定するには、次の概念を理解する必要があります。

- 「IOS SLB の利点」（P.11）
- 「Cisco IOS SLB 機能」（P.12）：ここでは、IOS SLB の一般的な機能について説明します。
- 「Exchange Director 機能」（P.31）：ここでは、mobile Service Exchange Framework（mSEF）用の Exchange Director が提供する独自の機能について説明します。

（注） 一部の IOS SLB 機能はプラットフォーム固有であり、この機能に関するマニュアルには記載されていません。このような機能については、該当するプラットフォームのマニュアルを参照してください。

IOS SLB の利点

IOS SLB は Cisco IOS と同じソフトウェア コード ベースを共有しており、Cisco IOS ソフトウェアのすべてのソフトウェア機能セットを備えています。

Cisco Catalyst 6500 シリーズ スイッチ上で IOS SLB を dispatched モードで実行すると、ハードウェア アクセラレーションによってパケットが非常に高速に転送されます。

IOS SLB は、分散環境でサーバと接続を積極的に管理するためのテクニックを駆使して、コンテンツとアプリケーションの継続的なハイ アベイラビリティを保証します。また、ユーザ要求をサーバのクラスタ全体で分散することによって、応答性とシステム容量を最適化し、大規模サイト、中規模サイト、および小規模サイトのインターネット、データベース、およびアプリケーション サービスの提供コストを削減します。

さらに、スケーラビリティ、可用性、およびメンテナンス容易性を向上します。

- 新しい物理（実）サーバの追加や、既存のサーバの削除または障害はいつでも発生する可能性がありますが、仮想サーバの可用性には影響はなく、ユーザが意識することはありません。
- IOS SLB のスロー スタート機能を使用すれば、新しいサーバの負荷を段階的に上げることによって、短期間に多くの新しい接続をサーバに割り当てることで発生する障害を阻止できます。
- IOS SLB は、フラグメント化されたパケットおよび IP オプションが指定されたパケットをサポートして、制御が及ばないクライアントやネットワークの変動からくるサーバへの危険性を和らげます。
- IOS SLB ファイアウォール ロード バランシングを使用すると、インターネット サイトへのアクセスを拡張できます。既存の接続に影響を与えることなくファイアウォールを追加できるため、サイトを拡張してもユーザに影響がありません。

DFP を使用すると、別のロード バランシング システムに負荷を分散できます。IOS SLB は DFP マネージャとして動作することでホスト サーバからの負荷を受け入れ、DFP エージェントとして動作することで負荷を DFP マネージャに送出します。この機能は独立してイネーブルにされるため、どちらか一方、または両方を同時に実装できます。

IOS SLB は、サーバ アプリケーションの管理を容易にします。クライアントが認識するのは仮想サーバのみで、実サーバの変更に管理は必要ありません。

IOS SLB は、実サーバのアドレスを外部ネットワークに公表することがないため、実サーバのセキュリティが向上します。ユーザが知るのは仮想 IP アドレスだけです。IP アドレスおよびポート番号（TCP または UDP）に基づいて、不必要なフローをフィルタできます。また、ファイアウォールの必要性はなくなりませんが、IOS SLB によって一部のサービス拒絶攻撃から保護できます。

支社の場合、IOS SLB を使用して、複数サイトのロード バランシング、およびサイト全体で障害が発生した場合の障害回復が可能です。また、ロード バランシングの処理を分散できます。

Cisco IOS SLB 機能

Cisco IOS SLB には次のようなサブ機能が含まれています。

ルーティング機能

IOS SLB には次のルーティング機能があります。

サーバ ロード バランシングのアルゴリズム

IOS SLB には次のロード バランシング アルゴリズムがあります。

仮想サーバに到達する新規の各接続要求について、実サーバを選択する基礎としてこれらのアルゴリズムのいずれかを指定できます。

アルゴリズムごとに、終了状態の接続が、実サーバに割り当てられた接続数に照らしてカウントされます。その結果、他のアルゴリズムよりも最小接続アルゴリズムが影響を受けます。これは、最小接続アルゴリズムが接続数に左右されるためです。IOS SLB は、接続が割り当てられるたびに、1 つの実サーバあたりの接続数、およびアルゴリズムのメトリクスを調整します。

加重ラウンド ロビン アルゴリズム

加重ラウンド ロビン アルゴリズムでは、循環形式で、サーバ ファームから仮想サーバへの新しい接続に使用される実サーバを選択するように指定します。実サーバごとに加重 *n* が割り当てられます。この加重は、仮想サーバに関連付けられた他の実サーバと比較した場合の接続の管理能力を表します。つまり、*n* 回、新しい接続がその実サーバに割り当てられてから、サーバ ファームの次の実サーバが選択されます。

たとえば、サーバ ファームが ServerA（*n* = 3）、ServerB（*n* = 1）、および ServerC（*n* = 2）という実サーバで構成されているとします。仮想サーバに対する最初の 3 つの接続は ServerA に割り当てられ、4 番目の接続は ServerB、5 番目と 6 番目の接続は ServerC に割り当てられます。

（注） ラウンド ロビン アルゴリズムを使用するように IOS SLB デバイスを設定するには、*n*=1 の荷重をサーバ ファーム内のすべてのサーバに割り当てます。

GTP Cause Code Inspection がイネーブルになっていない GPRS ロード バランシングには、加重ラウンド ロビン アルゴリズムが必要です。加重最小接続を使用するサーバ ファームを GTP Cause Code Inspection がイネーブルになっていない GPRS ロード バランシングを提供する仮想サーバにバインドすることはできますが、その仮想サーバを稼動させることはできません。これを実行しようとすると、IOS SLB からエラー メッセージが発行されます。

Home Agent Director には、加重ラウンド ロビン アルゴリズムが必要です。加重最小接続を使用するサーバ ファームを Home Agent Director 仮想サーバにバインドすることはできますが、その仮想サーバを稼動させることはできません。これを実行しようとすると、IOS SLB からエラー メッセージが発行されます。

RADIUS ロード バランシングには、加重ラウンド ロビン アルゴリズムが必要です。

RADIUS ロード バランシング加速データ プレーン フォワーディングは、加重ラウンド ロビン アルゴリズムをサポート*しません*。

加重最小接続アルゴリズム

加重最小接続アルゴリズムは、サーバ ファームから選択された次の実サーバがアクティブ接続の最も少ないサーバになるように指定します。このアルゴリズムでも、各実サーバに加重が割り当てられます。加重が割り当てられると、最も接続数が少ないサーバは、各サーバのアクティブな接続数、および各サーバの相対的な容量に基づいて決まります。ある実サーバの容量を算出するには、そのサーバに割り当てられた加重を、仮想サーバに関連付けられたすべての実サーバに割り当てられた加重の合計で割ります。つまり、$n_1/(n_1+n_2+n_3...)$ です。

たとえば、サーバ ファームが ServerA（*n* = 3）、ServerB（*n* = 1）、および ServerC（*n* = 2）という実サーバで構成されているとします。ServerA には 3/(3+1+2) で算出される容量があります。つまり、仮想サーバ上のすべてのアクティブな接続の半分です。ServerB にはすべてのアクティブな接続の 1/6 の容量、ServerC にはすべてのアクティブな接続の 1/3 の容量があります。任意の時点で、仮想サーバに対する次の接続は、アクティブな接続数が、算出された容量から最も離れている実サーバに割り当てられます。

（注） サーバ ファーム内のすべてのサーバに *n*=1 の荷重を割り当てた場合は、IOS SLB デバイスが単純な最小接続アルゴリズムを使用するように設定されます。

GTP Cause Code Inspection がイネーブルになっていない GPRS ロード バランシングは、加重最小接続アルゴリズムをサポートしません。

GTP Cause Code Inspection がイネーブルになっている GPRS ロード バランシングは、加重最小接続アルゴリズムをサポートします。

ASN ロード バランシング（Mobile Station Pre-Attachment 要求用）、Home Agent Director、RADIUS ロード バランシング、および RADIUS ロード バランシング加速データ プレーン フォワーディングは、加重最小接続アルゴリズムをサポートしません。

ルート マップ アルゴリズム

ルート マップ アルゴリズムが有効なのは、IOS SLB RADIUS ロード バランシング加速データ プレーン フォワーディング（Turbo RADIUS ロード バランシングとも呼ばれます）だけです。Turbo RADIUS ロード バランシングは、Cisco Content Services Gateway（CSG）環境で Policy-Based Routing（PBR; ポリシーベース ルーティング）ルート マップを使用して加入者のデータプレーン トラフィックを管理する高性能ソリューションです。Turbo RADIUS ロード バランシングが RADIUS ペイロードを受信すると、そのペイロードを検査して、framed-IP アトリビュートを抽出し、ルート マップを IP アドレスに適用してから、加入者を管理する CSG を決定します。

ポリシーベース ルーティングの詳細については、『*Cisco IOS IP Routing Configuration Guide*』の「Policy-Based Routing」と「Configuring Policy-Based Routing」を参照してください。

（注） RADIUS ロード バランシング加速データ プレーン フォワーディングでは、ルート マップ アルゴリズムが必要です。

バインディング ID のサポート

バインド ID を使用すれば、1 台の物理サーバを複数の仮想サーバにバインドして、サーバごとに加重を報告させることができます。したがって、単一の実サーバは、自身の複数インスタンスとして表現され、それぞれに異なるバインド ID が割り当てられます。Dynamic Feedback Protocol（DFP; ダイナミック フィードバック プロトコル）は、バインド ID を使用して、特定の加重が指定された実サーバのインスタンスを識別します。DFP を使用している場合にのみ、バインド ID 機能を使用します。

GPRS ロード バランシングおよび Home Agent Director は、バインド ID をサポートしません。

Client-Assigned ロード バランシング

Client-Assigned ロード バランシングでは、仮想サーバを使用する権限を持つクライアント IP サブネットのリストを指定することで、仮想サーバに対するアクセスを制限できます。この機能を使用すると、仮想 IP アドレスに接続する 1 セットのクライアント IP サブネット（内部サブネットなど）を、1 つのサーバ ファームまたはファイアウォール ファームに割り当て、別のクライアント セット（外部クライアントなど）を別のサーバ ファームまたはファイアウォール ファームに割り当てることができます。

GPRS ロード バランシングおよび Home Agent Director は、Client-Assigned ロード バランシングをサポートしません。

接続のレート制限

IOS SLB を使用すると、サーバ ファームの 1 つの実サーバに許可する最大接続レートを指定できます。詳細については、実サーバ コンフィギュレーション モードの **rate** コマンドに関する説明を参照してください。

コンテンツ フロー モニタのサポート

IOS SLB は Cisco Content Flow Monitor（CFM）をサポートします。CFM は、CiscoWorks2000 製品ファミリ内の Web ベース ステータス モニタリング アプリケーションです。CFM を使用すると、Cisco サーバ ロード バランシング デバイスを管理できます。CFM は Windows NT および Solaris ワークステーション上で動作します。CFM には Web ブラウザを使用してアクセスします。

TCP 接続コンテキストの遅延削除

IP パケットの順序異常が原因で、IOS SLB が、TCP 接続の終了（finish [FIN] または reset [RST]）後に、接続用の他のパケットが続いているのを検出する場合があります。一般的に、この問題は TCP 接続パケットがたどるパスが複数あるときに発生します。接続が終了した後に到着するパケットを適切にリダイレクトするために、IOS SLB が、指定された期間、TCP 接続情報（つまり、コンテキスト）を保持します。接続の終了後にコンテキストを保持する期間は、設定可能な遅延タイマーで制御されます。

ファイアウォール ロード バランシング

名前が示すように、ファイアウォール ロード バランシングには次のような機能があります。

- IOS SLB でファイアウォールへのフローのバランスを取ることができます。
- ファイアウォール グループ（ファイアウォール ファームと呼ばれる）の両側にあるロード バランシング デバイスを使用して、各フローのトラフィックが同じファイアウォールに送信されるように保証することによって、セキュリティ ポリシーを保護します。

各ロード バランシング デバイスに複数のファイアウォール ファームを設定できます。

- レイヤ 3 ファイアウォール : IP アドレス指定可能インターフェイスを備えています。ファイアウォール ロード バランシング デバイスとサブネットが隣接しており、MAC アドレスが一意の場合に、IOS SLB ファイアウォール ロード バランシングでサポートされます。デバイスはユーザ パケットの IP アドレスを変更しません。選択したファイアウォールにパケットを送信するために、デバイスは使用するインターフェイスを決定し、それに従ってレイヤ 2 ヘッダーを変更します。この種類のルーティングは、IOS SLB が使用する標準の dispatched ルーティングです。
- レイヤ 2 ファイアウォール : IP アドレスがありません。IOS SLB ファイアウォール ロード バランシングに対して透過的です。IOS SLB は、レイヤ 2 ファイアウォールを IP アドレス指定可能インターフェイス間に配置することによってサポートします。

ロード バランシング デバイス（たとえば、1 つの LAN）上の 1 つのレイヤ 3 インターフェイスから離れた場所に複数のレイヤ 3 ファイアウォールを配置することができますが、各インターフェイスから離れた場所に配置できるレイヤ 2 ファイアウォールは 1 台だけです。

ロード バランシング デバイスを設定する場合、そのデバイスの IP アドレスを使用してレイヤ 3 を設定し、ファイアウォールの「外側」にあるデバイスのインターフェイスの IP アドレスを使用して レイヤ 2 を設定します。

ファイアウォール ファーム内のファイアウォール全体について、フローの負荷を分散するために、IOS SLB ファイアウォール ロード バランシングは各受信フローについてルート検索を実行し、発信元および宛先の IP アドレス（さらに、オプションで発信元および宛先の TCP または User Datagram Protocol（UDP）のポート番号）を確認します。ファイアウォール ロード バランシングは、ハッシュ アルゴリズムをルート検索の結果に適用して、接続要求の管理に最適なファイアウォールを選択します。

（注） IOS SLB ファイアウォール ロード バランシングでは、受信パケットを確認し、ルート検索を実行する*必要があります*。Cisco Catalyst 6500 シリーズ スイッチでは、さらにいくつかのパケットを検査する必要があります。ファイアウォール ロード バランシングは、内側（保護されている側）のルーティング性能に影響するため、全体設計の中で考慮する必要があります。

複数のファイアウォールが設置されたネットワークの可用性と回復力を最大化するには、いずれかのファイアウォールにだけ 1 つのルートを設定するのではなく、ファイアウォールごとに均等加重ルートを設定します。

IOS SLB ファイアウォール ロード バランシングには、次の機能があります。

- ファイアウォール ファームの両側から開始される接続の負荷は分散されます。
- ファイアウォール セット（つまり、ファイアウォール ファーム）の中で負荷は分散されます。
- 接続のすべてのパケットは、同じファイアウォールを介して送信されます。以降の接続は、同じファイアウォールに割り当てられるように、「スティッキ」にすることができます。
- source-IP、destination-IP、および source-destination-IP のスティッキ接続がサポートされます。
- ファイアウォールの障害を検出し、回復するために、プローブが使用されます。
- 冗長機能が用意されています。Hot Standby Router Protocol（HSRP; ホット スタンバイ ルータ プロトコル）、ステートレス バックアップ、およびステートフル バックアップのすべてがサポートされます。
- 複数のインターフェイスの種類およびルーティング プロトコルがサポートされているため、外側（インターネット側）のロード バランシング デバイスはアクセス ルータとして動作できます。
- プロキシ ファイアウォールがサポートされます。

GTP IMSI スティッキ データベース

IOS SLB は、特定の International Mobile Subscriber ID（IMSI）用の GGSN を選択して、同じ IMSI から、選択された GGSN に、以降のすべての Packet Data Protocol（PDP）作成要求を転送することができます。

この機能をイネーブルにするために、IOS SLB は、各 IMSI をセッション データベースだけでなく、対応する実サーバにマップする GTP IMSI スティッキ データベースを使用します。

1. その IMSI で最初の GTP PDP 作成要求が処理されると、IOS SLB によってスティッキ データベース オブジェクトが作成されます。
2. また、実サーバから削除を示す通知を受信した場合、または非アクティブな状態の結果として、スティッキ オブジェクトが削除されます。
3. GGSN で 1 つの IMSI に属する最後の PDP が削除されると、GGSN から IOS SLB にスティッキ オブジェクトを削除するように通知されます。

Home Agent Director

ホーム エージェントは、モバイル ノードのアンカー ポイントです。モバイル ノードのフローを現在の外部エージェント（接続ポイント）にルーティングします。

Home Agent Director は、ホーム エージェント セット（サーバ ファームの実サーバとして設定されます）の中で、Mobile IP Registration Request（RRQ）のロード バランシングを実行します。Home Agent Director には次の特徴があります。

- dispatched モードまたは directed サーバ NAT モードで実行できますが、directed クライアント NAT モードでは実行できません。dispatched モードの場合、ホーム エージェントは IOS SLB デバイスに対して レイヤ 2 隣接にする必要があります。
- ステートフル バックアップをサポートしません。詳細については、「ステートフル バックアップ」（P.30）を参照してください。
- 仮想 Home Agent Director の IP アドレス宛ての RRQ を、加重ラウンド ロビン ロード バランシング アルゴリズムを使用して、実際のホーム エージェントの 1 つに配信します。このアルゴリズムの詳細については、「加重ラウンド ロビン アルゴリズム」（P.13）を参照してください。
- 容量に基づいて RRQ を割り当てるには、DFP が必要です。

Mobile IP、ホーム エージェントの詳細と関連するトピックについては、『*Cisco IOS IP Mobility Configuration Guide*』を参照してください。

インターフェイス認識

一部の環境では、仮想サーバ、ファイアウォール ファーム、接続、およびセッションにパケットをマッピングするときに、IOS SLB で入力インターフェイスを考慮する必要があります。IOS SLB では、この機能はインターフェイス認識と呼ばれます。インターフェイス認識を設定すると、設定したアクセス インターフェイスに到達したトラフィックのみが処理されます（アクセス インターフェイスは任意のレイヤ 3 インターフェイスです）。

このような「サンドイッチ」環境では、CSG、SSG、またはファイアウォールのファームの両側に IOS SLB が必要です。たとえば、ファームの一方で RADIUS ロード バランシングを実行し、もう一方でファイアウォール ロード バランシングを実行できます。また、ファイアウォール ファームの両側でファイアウォール ロード バランシングを実行することもできます。

最大接続

IOS SLB では、サーバおよびファイアウォール ロード バランシングの最大接続数を設定できます。

- サーバ ロード バランシングの場合、実サーバに割り当てるアクティブな接続数に制限を設定できます。実サーバの接続の最大数に達すると、以降のすべての接続要求は、接続数が指定した制限値に低下するまで、他のサーバへと自動的に切り替えられます。
- ファイアウォール ロード バランシングの場合、ファイアウォール ファームに割り当てるアクティブな TCP または UDP の数に制限を設定できます。ファイアウォール ファームの接続の最大数に達すると、接続数が指定した制限値に低下するまで、新規の接続はドロップされます。

複数ファイアウォール ファームのサポート

各ロード バランシング デバイスに複数のファイアウォール ファームを設定できます。

ネットワーク アドレス変換

Cisco IOS Network Address Translation（NAT; ネットワーク アドレス変換）（RFC 1631）を使用すると、未登録の「プライベート」IP アドレスをグローバルに登録された IP アドレスに変換してインターネットに接続できます。この機能の一部として、ネットワーク全体について 1 つのアドレスだけを外部に通知するように Cisco IOS NAT を設定できます。この設定には追加のセキュリティおよびネットワーク プライバシーが用意されており、そのアドレスの外部から内部ネットワーク全体を効率的に隠蔽できます。NAT には、セキュリティおよびアドレス保存の二重機能性があり、一般的にリモート アクセス環境で実装されます。

ここでは、次の内容について説明します。

- 「セッション リダイレクション」（P.18）
- 「dispatched モード」（P.18）
- 「directed モード」（P.18）
- 「サーバ NAT」（P.19）
- 「クライアント NAT」（P.19）
- 「スタティック NAT」（P.19）
- 「サーバ ポート変換」（P.21）

セッション リダイレクション

セッション リダイレクション NAT は、パケットを実サーバにリダイレクトします。IOS SLB は、dispatched モードまたは directed モードという 2 つのセッション リダイレクション モードのいずれかで動作します。

（注） dispatched モードと directed モードの両方で、IOS SLB が接続を追跡する必要があります。そのため、ロード バランシング デバイスをバイパスするクライアントに対して、実サーバからの代替ネットワーク パスがないように、ネットワークを設計する必要があります。

dispatched モード

dispatched NAT モードでは、仮想サーバ アドレスが実サーバに認識されます。実サーバのそれぞれで、仮想サーバ IP アドレスをループバック アドレスまたはセカンダリ IP アドレス として設定する必要があります。パケットは、Media Access Control（MAC; メディア アクセス制御）レイヤの実サーバにリダイレクトされます。dispatched モードでは仮想サーバ IP アドレスが変更されないため、実サーバを IOS SLB に対してレイヤ 2 隣接にする必要があります。そうしなかった場合は、仲介ルータが、選択された実サーバにルーティングできない可能性があります。

Cisco Catalyst 6500 シリーズ スイッチの場合は、通常、ハードウェア データ パケット アクセラレーションを備えた dispatched モードの方が directed モードよりもパフォーマンスが向上します。

ループバック アドレスの設定の詳細については、『*Cisco IOS Interface Configuration Guide*』の「Configuring Virtual Interfaces」の章を参照してください。

（注） 一部の UDP アプリケーションは、ループバック インターフェイスからの要求に応答できません。このような場合、directed モードを使用する必要があります。

directed モード

directed NAT モードでは、どの実サーバにも認識されない IP アドレスを仮想サーバに割り当てることができます。IOS SLB は、仮想サーバの IP アドレスを実サーバの IP アドレスに変換する NAT を使用して、クライアントと実サーバ間で交換されるパケットを変換します。

IOS SLB は次の種類の NAT をサポートします。

- 「サーバ NAT」（P.19）
- 「クライアント NAT」（P.19）
- 「スタティック NAT」（P.19）
- 「サーバ ポート変換」（P.21）

（注） 同じ接続にサーバ NAT とクライアント NAT の両方を使用できます。

IOS SLB は、directed で FTP またはファイアウォール ロード バランシングをサポートしません。そのため、FTP およびファイアウォール ロード バランシングでは NAT を使用できません。

IOS SLB は、TCP 仮想サーバと UDP 仮想サーバに対して、クライアント NAT しかサポートしません。

IOS SLB は、Encapsulation Security Payload（ESP; 暗号ペイロード）仮想サーバまたは Generic Routing Encapsulation（GRE; 総称ルーティング カプセル化）仮想サーバに対して、サーバ NAT（サーバ ポート変換以外）しかサポートしません。

サーバ NAT

サーバ NAT には、仮想サーバの IP アドレスを実サーバの IP アドレスに置換する処理（およびその逆の処理）があります。サーバ NAT には次のような利点があります。

- ロード バランシング デバイスから多数のホップを経た位置にサーバを配置できます。
- 仲介ルータは、トンネリングなしでサーバにルーティングできます。
- 実サーバ側にループバックおよびセカンダリ インターフェイスは必要ありません。
- 実サーバを IOS SLB に対してレイヤ 2 隣接にする必要はありません。
- 実サーバは、同じ IOS SLB デバイス上の仮想サーバに対して接続を開始できます。

クライアント NAT

ネットワークで複数のロード バランシング デバイスを使用している場合、クライアント IP アドレスを、デバイスのいずれかに関連付けられている IP アドレスで置換することで、発信フローが適切なデバイスにルーティングされます。また、クライアント NAT の場合、多数のクライアントが同じ一時ポートを使用できるため、一時クライアント ポートを変更する必要があります。複数のロード バランシング デバイスを使用しない場合でも、負荷が分散された接続のパケットがデバイス中をルーティングされないようにするには、クライアント NAT が便利です。

スタティック NAT

スタティック NAT の場合、スタティック NAT コマンドを設定すると、アドレス変換は NAT 変換テーブルに登録され、スタティック NAT コマンドを削除するまで変換テーブルに保存されます。

スタティック NAT を使用すれば、一部のユーザは NAT を使用し、同じイーサネット インターフェイス上の他のユーザは、引き続き固有の IP アドレスを使用できます。このオプションによって、実サーバからの応答と、実サーバが開始した接続要求とを区別することで、実サーバのデフォルトの NAT 動作を設定できます。

たとえば、サーバ NAT を使用すると、実サーバに対する Domain Name System（DNS; ドメイン ネーム システム）の受信要求パケットおよび発信応答パケットをリダイレクトできます。また、スタティック NAT を使用すると、実サーバからの接続要求を処理できます。

（注） DNS にはスタティック NAT が必要ありませんが、実サーバ IP アドレスが外部から隠蔽されるため、使用することを推奨します。

IOS SLB は次のスタティック NAT オプションをサポートします。各オプションは **ip slb static** コマンドを使用して設定します。

- Static NAT with dropped connections : 既存の接続に対応するパケットではない場合、パケットがドロップされるように実サーバを設定します。通常、このオプションは、スタティック NAT コンフィギュレーション モードの **real** コマンドで、サブネット マスクまたはポート番号オプションとともに使用されます。その結果、指定したサブネットまたはポートに対する接続が構築され、実サーバからのその他の接続はすべてドロップされます。
- Static NAT with a specified address : アドレス変換時に、ユーザが指定した仮想 IP アドレスを使用するように実サーバが設定されます。
- Static NAT with per-packet server load balancing : IOS SLB が実サーバから発信されたパケットの接続状態を維持しないように、実サーバが設定されます。つまり、IOS SLB はサーバ NAT を使用して、実サーバから発信されたパケットをリダイレクトします。パケット別のサーバ ロード バランシングは、DNS ロード バランシングの場合に特に便利です。IOS SLB は、パケット別のサーバ ロード バランシング環境の障害を検出するために DNS プローブを使用します。

（注） パケット単位サーバ ロード バランシングを使用したスタティック NAT では、フラグメント化されたパケットが負荷分散されません。

- Static NAT with sticky connections：実サーバから発信されたパケットがスティッキ オブジェクトに一致しない場合、IOS SLB がそのパケットの接続状態を維持しないように、実サーバが設定されます。
  - IOS SLB は一致するスティッキ オブジェクトを検出すると、接続を構築します。
  - IOS SLB は一致するスティッキ オブジェクトを検出しない場合、接続を構築せずにパケットを転送します。

IOS SLB で実サーバからのパケットを扱う場合、次のロジックを使用します。

ステップ 1 パケットは実サーバと一致しますか。

- 「いいえ」の場合、IOS SLB はそのパケットを処理しません。
- 「はい」の場合、処理を続行します。

ステップ 2 パケットは既存の接続と一致しますか。

- 「はい」の場合、IOS SLB は、接続コントロール ブロックに従って、NAT を使用してパケットをリダイレクトします。
- 「いいえ」の場合、処理を続行します。

ステップ 3 スタティック NAT を使用するように実サーバは設定されていますか。

- 「いいえ」の場合は、IOS SLB がそのパケットを通常どおり管理します。この機能は、スタティック NAT パススルーとも呼ばれます。
- 「はい」の場合、処理を続行します。

ステップ 4 既存の接続に対応するパケットではない場合、パケットがドロップされるように実サーバは設定されていますか。

- 「はい」の場合、IOS SLB はパケットをドロップします。
- 「いいえ」の場合、処理を続行します。

ステップ 5 実サーバは、パケット別のサーバ ロード バランシング用に設定されていますか。

- 「はい」の場合、IOS SLB は NAT を使用してパケットをリダイレクトします。
- 「いいえ」の場合、処理を続行します。

ステップ 6 スティッキ接続の接続状態を維持するように実サーバは設定されていますか。

- 「いいえ」の場合、IOS SLB は接続を構築します。
- 「はい」の場合、IOS SLB は一致するスティッキ オブジェクトを検索します。処理を続行します。

ステップ 7 IOS SLB は一致するスティッキ オブジェクトを検索できますか。

- 「いいえ」の場合、IOS SLB はパケットをドロップします。
- 「はい」の場合、IOS SLB は接続を構築します。

サーバ ポート変換

サーバ ポート変換は、Port Address Translation（PAT; ポート アドレス変換）とも呼ばれます。サーバ NAT の形式の 1 つであり、仮想サーバの IP アドレスではなく仮想サーバのポートの変換が行われます。仮想サーバのポート変換には、仮想サーバの IP アドレスの変換は必要ありませんが、2 種類の変換を併用することもできます。

IOS SLB は、TCP および UDP の場合にだけ、サーバ ポート変換をサポートします。

ポートバインド サーバ

ポートバインド サーバを使用すると、1 つの仮想サーバの IP アドレスで、HTTP などのサービス用の実サーバ セットと、Telnet などのサービス用の実サーバ セットを表現できます。仮想サーバを定義するときに、そのサーバで管理する TCP ポートまたは UDP ポートを指定する必要があります。ただし、サーバ ファームで NAT を設定する場合、ポートバインド サーバを設定することもできます。

仮想サーバ定義で指定されていないポートの仮想サーバ アドレス宛てのパケットは、リダイレクトされません。

IOS SLB は、ポートバインド サーバと非ポートバインド サーバの両方をサポートしますが、ポートバインド サーバの使用が推奨されます。

IOS SLB ファイアウォール ロード バランシングは、ポートバインド サーバをサポートしません。

ルート ヘルス インジェクション

（**inservice** コマンドを使用して）仮想サーバをサービスに登録すると、デフォルトで、仮想サーバの IP アドレスがアドバタイズされます（ルーティング テーブルに追加されます）。Web サイトの仮想 IP アドレスに適切なホスト ルートが存在する場合は、そのホスト ルートをアドバタイズできますが、その IP アドレスを使用できるという保証はありません。ただし、IP アドレスを使用できると IOS SLB で検証された場合にだけ、ホスト ルートをアドバタイズするように、**advertise** コマンドで IOS SLB を設定できます。IP アドレスを使用できなくなると、IOS SLB はアドバタイズメントを撤回します。この機能はルート ヘルス インジェクションと呼ばれます。

スティッキ接続

オプションの **sticky** コマンドを使用すると、同じクライアントからの発信を、サーバ ファーム内の同じロード バランシング サーバに強制的に接続できます。

クライアント トランザクションには、複数の連続する接続が必要なことがあります。つまり、同じクライアントの IP アドレスまたはサブネットからの新しい接続を、同じ実サーバに割り当てる必要があります。このような接続は、ファイアウォール ロード バランシングの場合に特に重要です。場合によってファイアウォールは、特定の攻撃を検出するために複数の接続をプロファイルする必要があるためです。

- IOS SLB は、source-IP スティッキ接続をサポートします。
- ファイアウォール ロード バランシングは、source-IP、destination-IP、および source-destination-IP のスティッキ接続をサポートします。
- RADIUS ロード バランシングは、calling-station-IP、framed-IP、および username のスティッキ接続をサポートします。

ファイアウォール ロード バランシングの場合、同じクライアント - サーバ ペア間の接続は、同じファイアウォールに割り当てられます。次の条件をすべて満たす場合、新しい接続はスティッキ接続と見なされます。

- 実サーバの状態は OPERATIONAL または MAXCONNS_THROTTLED です。
- 仮想サーバまたはファイアウォール ファームにスティッキ タイマーが定義されています。

同じサーバまたはファイアウォールに対するこの新しい接続のバインディングは、最後のスティッキ接続が終了した後も、ユーザが定義した期間、継続されます。

「サンドイッチ」ファイアウォール ロード バランシングに必要な、クライアント - サーバ アドレスのスティッキ動作を実現するには、ファイアウォール ファームの両側でスティッキを有効にする必要があります。この設定では、クライアント - サーバ スティッキの関連付けは、クライアント - サーバ アドレス ペア間に最初の接続が開かれたときに作成されます。この最初の接続が確立した後に、IOS SLB はファームの一方にあるファイアウォール ロード バランシング デバイスにスティッキの関連付けを維持し、両方のファイアウォール ロード バランシング デバイスによってクライアントまたはサーバの IP アドレスから開始された接続に、スティッキの関連付けを適用します。

クライアント サブネット スティッキは、**sticky** コマンドをサブネット マスク付きで指定した場合にイネーブルになります。サブネット スティッキは、ある接続から次の接続でクライアントの IP アドレスが変わる場合に便利です。たとえば、クライアント接続は IOS SLB に到達する前に、スティッキ管理機能がない NAT またはプロキシ ファイアウォールのセットを経由する可能性があります。このような場合、サーバに対処できるロジックがないと、クライアント トランザクションは失敗します。こうしたファイアウォールが同じサブネット セットのアドレスを割り当てるときに発生する可能性がある問題には、IOS SLB のスティッキ サブネット マスクであれば対応できます。

スティッキ接続は、複数の仮想サーバまたはファイアウォール ファームによって管理されるサービスのカップリングも許可します。このオプションによって、関連サービスの接続要求に同じ実サーバを使用できます。たとえば、通常 Web サーバ（HTTP）は TCP ポート 80 を使用し、HTTPS はポート 443 を使用します。HTTP 仮想サーバおよび HTTPS 仮想サーバをカップリングすると、同じクライアントの IP アドレスまたはサブネットからの ポート 80 および 443 に対する接続は、同じ実サーバに割り当てられます。

同じスティッキ グループに属する仮想サーバは、バディ仮想サーバとも呼ばれます。

Home Agent Director はスティッキ接続をサポートしません。

TCP セッションの再割り当て

IOS SLB は、クライアントが新しい接続を開こうとして実サーバに送信される各 TCP SYNchronize Sequence Number（SYN）を追跡します。複数の連続する SYN に応答がない場合、または SYN が RST で応答される場合、TCP セッションは新しい実サーバに再割り当てされます。SYN の試行回数は、設定可能な再割り当てしきい値で制御されます。

IOS SLB ファイアウォール ロード バランシングは、TCP セッションの再割り当てをサポートしません。

透過的 Web キャッシュ ロード バランシング

IOS SLB は、透過的 Web キャッシュのクラスタ全体で HTTP フローの負荷を分散できます。この機能をセットアップするには、透過的 Web キャッシュで処理するサブネット IP アドレス、または何らかの共通するサブセットを仮想サーバとして設定します。透過的 Web キャッシュ ロード バランシングに使用する仮想サーバは、サブネット IP アドレスの代理で ping に応答しません。また、トレースルートに影響がありません。

必要なページがキャッシュに含まれない場合など、状況によっては、Web キャッシュからインターネットへの独自の接続を開始する必要があります。このような接続は、同じ Web キャッシュ セットに対して負荷を分散しないでください。このような要件に対処するために、IOS SLB では **client exclude** ステートメントを設定できます。このステートメントで、Web キャッシュから開始された接続はロード バランシング スキームから除外されます。

IOS SLB ファイアウォール ロード バランシングは、透過的 Web キャッシュ ロード バランシングをサポートしません。

セキュリティ機能

IOS SLB には次のセキュリティ機能があります。

代替 IP アドレス

IOS SLB を使用すると、代替 IP アドレスを使用して、ロード バランシング デバイスに Telnet を使用できます。そのためには、次のいずれかの方式を使用します。

- いずれかのインターフェイス IP アドレスを使用して、ロード バランシング デバイスに Telnet を実行します。
- セカンダリ IP アドレスを定義して、ロード バランシング デバイスに Telnet を実行します。

この機能は、LocalDirector（LD）Alias コマンドで提供される機能と似ています。

サーバ ファームおよびファイアウォール ファームに対する攻撃の回避

IOS SLB は、サイトを攻撃から守るためにサイトのファイアウォールに依存しています。一般的に、IOS SLB は、スイッチやルータと同程度に直接攻撃の影響を受けます。ただし、高度にセキュアなサイトであれば、次の手順でセキュリティを強化できます。

- クライアントが実サーバに直接接続しないように、プライベート ネットワークの実サーバを設定します。この設定によって、クライアントは常に IOS SLB を経由して実サーバに接続するようになります。
- IOS SLB デバイスのインターフェイスを宛先に指定した外部ネットワークからのフローを拒否するように、アクセス ルータまたは IOS SLB デバイスの入力アクセス リストを設定します。つまり、予期しないアドレスからの *すべての*直接フローを拒否します。
- ファイアウォール サブネットの実 IP アドレスまたは存在しない IP アドレスに対してフローを送信しようとする攻撃から保護するには、プライベート ネットワークでファイアウォールを設定します。
- ファイアウォール宛ての予期しない*すべての*フロー（特に、外部ネットワークから発信されたフロー）を拒否するようにファイアウォールを設定します。

スロー スタート

過負荷を防止するために、スロー スタートは、起動直後の実サーバに向けられる新しい接続の数を制御します。加重最小接続ロード バランシングを使用する環境では、起動した直後の実サーバには接続がないため、新しい接続が多数割り当てられ、過負荷になる可能性があります。

GPRS ロード バランシングおよび Home Agent Director は、スロー スタートをサポートしません。

SynGuard

SynGuard は、仮想サーバによって管理される TCP start-of-connection パケット（SYN）のレートを制限して、SYN フラッド サービス拒否攻撃と呼ばれるネットワーク上の問題を阻止します。ユーザが大量の SYN をサーバに送信することもあり、それによってサーバの過負荷やクラッシュが発生し、他のユーザへのサービスが停止する可能性があります。SynGuard によって、IOS SLB または実サーバを停止させる攻撃などを回避します。SynGuard は、仮想サーバによって管理される SYN 数を一定間隔でモニタして、その数が、設定された SYN しきい値を超えないようにします。しきい値に達すると、新しい SYN はドロップされます。

IOS SLB ファイアウォール ロード バランシングおよび Home Agent Director は、SynGuard をサポートしません。

サーバ障害の検出機能および回復機能

IOS SLB には、次のサーバ障害検出機能と回復機能があります。

- 「自動サーバ障害検出」（P.24）
- 「自動アンフェイル」（P.25）
- 「バックアップ サーバ ファーム」（P.25）
- 「Dynamic Feedback Protocol（DFP）Agent Subsystem のサポート」（P.25）
- 「Cisco IOS SLB 用の DFP」（P.25）
- 「GGSN-IOS SLB メッセージング」（P.26）
- 「仮想サーバの INOP_REAL 状態」（P.26）
- 「プローブ」（P.27）

自動サーバ障害検出

IOS SLB は、実サーバに対して失敗した各 Transmission Control Protocol（TCP; トランスミッション制御プロトコル）接続試行を自動的に検出し、そのサーバの障害カウンタを増加します（同じクライアントからの失敗した TCP 接続がカウント済みの場合、障害カウンタは増加しません）。サーバの障害カウンタが設定可能な障害しきい値を超えると、そのサーバはアウト オブ サービスと見なされ、アクティブな実サーバのリストから削除されます。

RADIUS ロード バランシングの場合、RADIUS 要求に対して実サーバから応答がないと、IOS SLB は自動サーバ障害検出を実行します。

全ポート仮想サーバ（つまり、GTP ポートを除くすべてのポート宛てのフローを受け入れる仮想サーバ）を設定した場合、アプリケーション ポートが存在しないサーバにフローを渡すことができます。サーバがこのようなフローを拒否すると、IOS SLB はそのサーバを無効と見なし、ロード バランシングから除外することがあります。この状況は、RADIUS ロード バランシング環境の応答が遅い AAA サーバの場合にも発生する可能性があります。この状況を回避するには、自動サーバ障害検出をディセーブルにします。

（注） **no faildetect inband** コマンドを使用して自動サーバ障害検出をディセーブルにした場合は、1 つ以上のプローブを設定することを強く推奨します。

no faildetect inband コマンドを指定した場合は、指定された **faildetect numconns** コマンドが無視されます。

自動アンフェイル

実サーバに障害が発生し、アクティブなサーバのリストから削除されると、設定可能な再試行タイマーに指定された期間、新しい接続は割り当てられません。タイマーの期限が切れると、そのサーバには新しい仮想サーバ接続を受ける資格ができ、IOS SLB から次の適格性確認の接続がサーバに送信されます。その接続が成功すると、失敗したサーバはアクティブな実サーバのリストに戻されます。接続に失敗すると、サーバはアウト オブ サービスのままで、再試行タイマーがリセットされます。失敗した接続は少なくとも 1 回は再試行されているはずです。実行されていない場合、次の適格性確認の接続もその失敗したサーバに送信されます。

バックアップ サーバ ファーム

バックアップ サーバ ファームは、プライマリ サーバ ファームに定義されている実サーバで新しい接続を受け入れることができないときに使用できるサーバ ファームです。バックアップ サーバ ファームを設定する場合、次の注意事項を考慮する必要があります。

- サーバ ファームは、同時にプライマリとバックアップの両方として動作できます。
- 同じ実サーバを、同時にプライマリとバックアップの両方に定義することはできません。
- プライマリとバックアップのどちらも、同じ NAT 設定（なし、クライアント、サーバ、または両方）にする必要があります。さらに、NAT を指定する場合、両方のサーバ ファームは同じ NAT プールを使用する必要があります。

Dynamic Feedback Protocol（DFP）Agent Subsystem のサポート

IOS SLB は DFP Agent Subsystem 機能（グローバル ロード バランシングとも呼ばれます）をサポートします。そのため、IOS SLB 以外のクライアント サブシステムも DFP エージェントとして実行できます。DFP Agent Subsystem を利用すると、複数のクライアント サブシステムの複数の DFP エージェントを同時に使用できます。

DFP Agent Subsystem の詳細については、Cisco IOS Release 12.2(18)SXD の *DFP Agent Subsystem* 機能に関するマニュアルを参照してください。

Cisco IOS SLB 用の DFP

IOS SLB DFP がサポートされている場合は、ロード バランシング環境内の DFP マネージャが DFP エージェントとの TCP 接続を開始することができます。接続後は、DFP エージェントによって 1 つまたは複数の実サーバからステータス情報が収集され、情報は相対的な加重に変換され、DFT マネージャに加重がレポートされます。実サーバのロード バランシング処理時に、DFP マネージャで加重が考慮されます。ユーザが定義した間隔での報告に加えて、実サーバのステータスが急に変化した場合に DFP エージェントが初期レポートを送信します。

DFP によって算出される加重は、サーバ ファーム コンフィギュレーション モードで **weight** コマンドを使用してユーザが定義したスタティックな加重よりも優先されます。ネットワークから DFP を外すと、IOS SLB はスタティックな加重に戻されます。

IOS SLB は、DFP マネージャ、別の DFP マネージャ用の DFP エージェント、または同時に両方の役割として定義できます。両方の役割を設定する場合、IOS SLB から他の DFP マネージャへ定期的なレポートが送信されます。その DFP マネージャでは、新しい各接続要求について最適なサーバ ファームを選択するためにレポートの情報が使用されます。次に、IOS SLB では、選択したサーバ ファーム内で最適な実サーバを選択するために同じ情報が使用されます。

また、DFP は、複数のクライアント サブシステム（IOS SLB と GPRS など）の複数の DFP エージェントの同時使用もサポートしています。

詳細については、次のセクションを参照してください。

- 「DFP および GPRS ロード バランシング」（P.26）

- 「DFP および Home Agent Director」（P.26）

DFP および GPRS ロード バランシング

GPRS ロード バランシングの場合、DFP マネージャとして IOS SLB を定義し、サーバ ファームの各 GGSN に DFP エージェントを定義できます。定義後は、DFP エージェントから GGSN の加重をレポートできます。DFP エージェントは、CPU 使用率、プロセッサ メモリ、および GGSN ごとにアクティブにすることができる Packet Data Protocol（PDP）コンテキスト（モバイル セッション）の最大数に基づいて、各 GGSN の加重を計算します。第一近似として、DFP では、既存の PDP コンテキスト数を、最大許容 PDP コンテキスト数で割った値が算出されます。

（既存の PDP コンテキスト数）/（最大 PDP コンテキスト数）

最大 PDP コンテキスト数は、**gprs maximum-pdp-context-allowed** コマンドを使用して指定します。デフォルト値は、10,000 PDP コンテキストです。デフォルト値を受け入れると、GGSN の加重が非常に低く算出されることがあります。

（既存の PDP コンテキスト）/10000 = 低い GGSN 加重

gprs maximum-pdp-context-allowed コマンドを使用して、最大 PDP コンテキスト数を指定した場合は、この計算を考慮してください。たとえば、GGSN として動作する Cisco 7200 シリーズ ルータは、多くの場合、45,000 PDP コンテキストの最大値で設定されます。

DFP および Home Agent Director

Home Agent Director を使用している場合は、DFP マネージャとして IOS SLB を定義し、サーバ ファームの各ホーム エージェント上で DFP エージェントを定義することができます。また、DFP エージェントからホーム エージェントの加重を報告させることができます。DFP エージェントは、CPU 使用率、プロセッサ メモリ、およびホーム エージェントごとにアクティブにすることができるバインディングの最大数に基づいて、各ホーム エージェントの加重を計算します

（バインディングの最大数 - 現在のバインディング数）/ バインディングの最大数 *（CPU 使用率 + メモリ使用率）/32 * 最大 DFP 加重 = 報告される加重

*バインディングの最大数*は 235,000 です。*最大 DFP 加重*は 24 です。

GGSN-IOS SLB メッセージング

特定の状態が発生した場合に、GGSN から IOS SLB に通知することができます。IOS SLB では通知によって適切な判断を下すことができます。結果として、GPRS ロード バランシングと障害検出が改善されます。

GGSN から送信される通知では、未使用の空間（将来的に使用するための予備）および次の Information Element（IE; 情報要素）のメッセージの種類とともに GTP を使用します。

- 通知の種類。通知条件を示します。たとえば、Call Admission Control（CAC; コール アドミッション制御）で現在の GGSN に障害が発生したときに、代替 GGSN にセッションを再割り当てするための IOS SLB に対する通知があります。
- 関連セッションの ID（セッション キー）。
- 通知の種類に固有のその他の IE。たとえば、再割り当てのための通知には、本来は SGSN に送信される予定だった作成応答が含まれます。この処理によって、通知によって再割り当ての最大数が設定した制限に達しても、IOS SLB からこの応答を SGSN にリレーできます。

GGSN-IOS SLB メッセージングは、dispatched モードと directed モードの両方でサポートされます。

仮想サーバの INOP_REAL 状態

仮想サーバに関連付けられているすべての実サーバが非アクティブの場合、次のアクションを実行するように、仮想サーバを設定できます。

- 仮想サーバを INOP_REAL 状態に設定します。
- 仮想サーバの状態遷移について SNMP トラップを生成します。
- 仮想サーバは ICMP 要求に対する応答を停止します。

詳細については、SLB サーバ ファームの仮想サーバ コンフィギュレーション モードの **inservice（サーバ ファームの仮想サーバ）**コマンドに関する説明を参照してください。

プローブ

プローブは、サーバ ファーム内の実サーバごとまたはファイアウォール ファーム内のファイアウォールごとのステータスを決定します。Cisco IOS SLB 機能は、DNS、HTTP、ping、TCP、カスタム UDP、および WSP プローブをサポートします。

- DNS プローブは実サーバに対してドメイン名解決要求を送信し、返される IP アドレスを確認します。
- HTTP プローブは実サーバに対する HTTP 接続を確立し、実サーバに対して HTTP 要求を送信し、その応答を確認します。HTTP プローブは、サーバ ロード バランシングで処理されたデバイス、およびファイアウォール ロード バランシングで処理されたファイアウォール（ファイアウォールのもう一方にあるデバイスでも）について、接続を確認できる簡単な方法です。

  HTTP プローブを使用すれば、サーバ ロード バランシングで処理されたアプリケーションをモニタすることもできます。頻繁にプローブを使用すると、アプリケーションに対する接続だけでなく、各アプリケーションの動作を確認できます。

  HTTP プローブは、HTTP over Secure Socket Layer（HTTPS）をサポートしません。つまり、HTTP プローブを SSL サーバに送信できません。
- ping プローブは実サーバに ping を送信します。HTTP プローブと同様に、ping プローブは、ロード バランシング処理されたデバイスとファイアウォールの接続を確認できる簡単な方法です。
- TCP プローブは TCP 接続の確立と削除を行います。TCP ポート 443（HTTPS）の障害を検出するには、TCP プローブを使用します。
- カスタム UDP プローブは、次のように多様なアプリケーションとプロトコルをサポートできます。
  - RADIUS Accounting/Authorization プローブ
  - GTP Echo プローブ
  - Connectionless WSP プローブ
  - CSG ユーザ データベース ロード バランシング用 XML-over-UDP プローブ
  - Mobile IP RRQ/RRP
- WSP プローブは、ワイヤレス コンテンツの要求をシミュレートし、取得したコンテンツを確認します。ポート 9201 のワイヤレス アプリケーション プロトコル（WAP）スタックの障害を検出するには、WSP プローブを使用します。

各サーバ ファーム、またはファイアウォール ファームの各ファイアウォールに、複数のプローブを設定できます。また、サポートされる種類のプローブを任意に組み合わせることができます。

経路選択済みプローブとしてプローブにフラグを付けることもできます。ただし、次の注意事項があります。

- 1 つのサーバ ファームにつき、同時に 1 インスタンスの経路選択済みプローブだけを実行できます。
- 経路選択済みプローブ宛ての発信パケットは、指定した IP アドレスに直接ルーティングされます。

IOS SLB プローブは SA Agent を使用します。SA Agent が使用できるメモリの量を指定するには、**rtr low-memory** コマンドを使用します。使用できる空きメモリの量が、**rtr low-memory** コマンドで指定された値を下回ると、SA Agent では、新しい動作を設定できません。詳細については、『*Cisco IOS IP SLAs Command Reference*』で **rtr low-memory** コマンドの説明を参照してください。

サーバ ロード バランシングのプローブ

プローブは、サーバ ファーム内の各実サーバのステータスを判断します。そのサーバ ファームに属するすべての仮想サーバに関連付けられたすべての実サーバが検査されます。

実サーバが 1 つのプローブで合格しなかった場合は、すべてのプローブで合格しません。実サーバが回復すると、サービスを復旧する前に、すべてのプローブがその回復を承認する必要があります。

(注) プローブがステートフル バックアップ用に設定され、フェールオーバーが発生した場合は、ステータスの変更（バックアップからアクティブへ）が新しいアクティブ IOS SLB デバイス内のプローブに正確に反映されます。ただし、（フェールオーバー前にアクティブ デバイスだった）新しいバックアップ IOS SLB デバイス内のプローブには、そのステータスがアクティブとして表示されます。

ファイアウォール ロード バランシングのプローブ

プローブはファイアウォールの障害を検出します。ファイアウォール ファームに関連付けられているすべてのファイアウォールが検査されます。

あるプローブに対してファイアウォールが失敗すると、すべてのプローブに失敗したことになります。ファイアウォールが回復したら、すべてのプローブがその回復を認識するまで、プローブをサービスに戻すことができません。

パスワードの問題を回避するには、HTTP プローブがステータス コード 401 を想定するように設定されていることを確認します。詳細については、**expect** コマンドの説明を参照してください。

デバイスの HTTP サーバを設定するには、**ip http server** コマンドを使用します。詳細については、『*Cisco IOS Configuration Fundamentals Command Reference*』で **ip http server** コマンドの説明を参照してください。

透過的 Web キャッシュ ロード バランシング環境では、仮想 IP アドレスは設定されないため、HTTP プローブは Web キャッシュの実 IP アドレスを使用します。

プロトコル サポート機能

IOS SLB には次のプロトコル サポート機能があります。

- 「プロトコル サポート」（P.28）
- 「AAA ロード バランシング」（P.29）
- 「オーディオおよびビデオのロード バランシング」（P.29）
- 「VPN サーバ ロード バランシング」（P.30）

プロトコル サポート

IOS SLB は次のプロトコルをサポートします。

- Access Service Network（ASN）
- Domain Name System（DNS; ドメイン ネーム システム）
- Encapsulation Security Payload（ESP; カプセル化セキュリティ ペイロード）
- File Transfer Protocol（FTP; ファイル転送プロトコル）
- Generic Routing Encapsulation（GRE）
- GPRS Tunneling Protocol v0（GTP v0; GPRS トンネリング プロトコル v0）
- GPRS Tunneling Protocol v1（GTP v1; GPRS トンネリング プロトコル v1）
- GPRS Tunneling Protocol v2（GTP v2; GPRS トンネリング プロトコル v2）

- Hypertext Transfer Protocol（HTTP; ハイパーテキスト転送プロトコル）
- Hypertext Transfer Protocol over Secure Socket Layer（HTTPS; HTTP over SSL）
- Internet Message Access Protocol（IMAP）
- Internet Key Exchange（IKE、旧称 ISAKMP）
- IP in IP Encapsulation（IPinIP）
- Mapping of Airline Traffic over IP, Type A（MATIP-A）
- Network News Transport Protocol（NNTP）
- Post Office Protocol, version 2（POP2）
- Post Office Protocol, version 3（POP3）
- RTSP 経由の RealAudio/RealVideo
- Remote Authentication Dial-In User Service（RADIUS）
- Simple Mail Transport Protocol（SMTP）
- Telnet
- Transmission Control Protocol（TCP; トランスミッション制御プロトコル）および標準の TCP プロトコル
- User Datagram Protocol（UDP; ユーザ データグラム プロトコル）および標準の UDP プロトコル
- X.25 over TCP（XOT）
- 次のようなワイヤレス アプリケーション プロトコル（WAP）
  - Connectionless Secure WSP
  - Connectionless WSP
  - Connection-Oriented Secure WSP
  - Connection-Oriented WSP

AAA ロード バランシング

IOS SLB には、RADIUS の Authentication, Authorization, and Accounting（AAA; 認証、認可、アカウンティング）サーバ用の RADIUS ロード バランシング機能があります。

また、次の RADIUS ロード バランシング機能があります。

- 使用可能な RADIUS サーバおよびプロキシ サーバに、RADIUS 要求を分散します。
- RADIUS 要求の再送信（未応答の要求の再送信など）を、元の要求と同じ RADIUS サーバまたはプロキシ サーバにルーティングします。
- セッションベースの自動障害検出機能があります。
- ステートレス バックアップとステートフル バックアップの両方をサポートします。

さらに IOS SLB は、従来およびモバイルのワイヤレス ネットワークの両方で、RADIUS の認可フローとアカウンティング フローをプロキシするデバイスの負荷を分散できます。詳細については、「RADIUS ロード バランシング」（P.36）を参照してください。

オーディオおよびビデオのロード バランシング

IOS SLB は、RealNetworks アプリケーションを実行しているサーバに対して、Real-Time Streaming Protocol（RTSP; リアルタイム トランスポート ストリーミング プロトコル）経由の RealAudio ストリームと RealVideo ストリームのバランスを取ることができます。

VPN サーバ ロード バランシング

IOS SLB は、次のような実行中のフローなど、バーチャル プライベート ネットワーク（VPN）フローの負荷を分散します。

- IP Security（IPSec; IP セキュリティ）フロー。IPSec フローは、UDP コントロール セッションと ESP トンネルから構成されます。
- Point-to-Point Tunneling Protocol（PPTP）フロー。PPTP フローは、TCP コントロール セッションと GRE トンネルから構成されます。

冗長機能

次のいずれかが発生した場合に、IOS SLB デバイスが単一障害点となり、サーバがバックボーンに対する接続を失う可能性があります。

- IOS SLB デバイスに障害が発生する。
- あるスイッチから distribution-layer スイッチへのリンクが解除状態になる。

このリスクを軽減するために、IOS SLB は HSRP に基づいて、次の冗長性の強化をサポートします。

- 「ステートレス バックアップ」（P.30）
- 「ステートフル バックアップ」（P.30）
- 「アクティブ スタンバイ」（P.31）

ステートレス バックアップ

ステートレス バックアップは、1 台のレイヤ 3 スイッチの可用性に依存せずに、イーサネット ネットワーク上のホストからの IP フローをルーティングすることによって、ネットワークの高可用性を実現します。Router Discovery Protocol（System-to-Intermediate System（IS-IS）Interdomain Routing Protocol（IDRP）など）をサポートしないホストで、新しいレイヤ 3 スイッチにシフトする機能がない場合は特に、ステートレス バックアップが有効です。

ステートフル バックアップ

ステートフル バックアップを使用すると、ロード バランシングの決定を段階的にバックアップするか、プライマリ スイッチとバックアップ スイッチ間で「状態を維持」できます。バックアップ スイッチは、HSRP がフェールオーバーを検出するまで、仮想サーバを休止状態にしたままにします。検出後、バックアップ（現在はプライマリ）スイッチは、仮想アドレスのアドバタイズとフローの処理を開始します。HSRP は、障害検出用のタイマーを設定するために使用することができます。

ステートフル バックアップは、IOS SLB に 1 対 1 のステートフルまたはアイドル バックアップ スキームを提供します。つまり、クライアント フローまたはサーバ フローを同時に処理できる IOS SLB は 1 インスタンスだけであり、アクティブな各 IOS SLB スイッチのバックアップ プラットフォームは 1 つだけです。

Home Agent Director はステートフル バックアップをサポートしません。

（注） プローブがステートフル バックアップ用に設定され、フェールオーバーが発生した場合は、ステータスの変更（バックアップからアクティブへ）が新しいアクティブ IOS SLB デバイス内のプローブに正確に反映されます。ただし、（フェールオーバー前にアクティブ デバイスだった）新しいバックアップ IOS SLB デバイス内のプローブには、そのステータスがアクティブとして表示されます。

アクティブ スタンバイ

アクティブ スタンバイによって、2 つの IOS SLB は同じ仮想 IP アドレスの負荷を分散すると同時に、相互にバックアップとして動作できます。負荷を分散できる仮想 IP アドレスがサイトに 1 つしかない場合、アクセス ルータでポリシーベース ルーティングを使用して、フローのサブセットを各 IOS SLB 宛てにします。

IOS SLB ファイアウォール ロード バランシングは、アクティブ スタンバイをサポートします。つまり、2 ペアのファイアウォール ロード バランシング デバイス（ファイアウォールの各サイドに 1 ペア）を設定できます。各ペアの各デバイスは、トラフィックを処理し、ペアのパートナーをバックアップします。

Exchange Director 機能

IOS SLB は、Cisco Catalyst 6500 シリーズ スイッチおよび Cisco 7600 シリーズ ルータ用の mobile Service Exchange Framework（mSEF）に対して、Exchange Director をサポートします。Exchange Director には次の機能があります。

ASN ロード バランシング

IOS SLB は、Access Service Network（ASN）ゲートウェイ セット全体のロード バランシングを実行できます。ゲートウェイ サーバ ファームは、ベース ステーションから 1 つの ASN ゲートウェイとして見えます。

Mobile Subscriber Station（MSS）がネットワークに入るときに、ベース ステーションが Mobile Station Pre-Attachment 要求を IOS SLB の仮想 IP アドレスに送信します。IOS SLB は ASN ゲートウェイを選択し、要求をそのゲートウェイに転送します。ゲートウェイは Mobile Station Pre-Attachment 応答でベース ステーションに直接応答します。そのように設定されていれば、ベース ステーションが IOS SLB に Mobile Station Pre-Attachment ACK を返し、その ACK は選択されたゲートウェイに転送されます。以降のすべてのトランザクションは、ベース ステーションとゲートウェイ間で送信されます。

ASN ゲートウェイに対してスティッキ接続がイネーブルになっている場合は、IOS SLB が、加入者に関するロード バランシングを決定したら、同じ加入者からの以降の要求をすべて同じ Cisco BWG に転送します。スティッキ情報がスタンバイ IOS SLB に複製されます。

IOS SLB は、Mobile Station ID（MSID; モバイル ステーション ID）を使用して、MSS ごとに 1 つずつのスティッキ エントリを持つスティッキ データベースを生成します。このスティッキ データベースを使用すれば、IOS SLB で選択された実サーバの MSID に関する永続的セッション トラッキングを実行することができます。MSS から仮想 IP アドレスに送信された最初のパケットによって、セッション オブジェクトとスティッキ オブジェクトが作成されます。セッション ルックアップが失敗した場合は、MSS からの以降のパケットは MSID を使用してスティッキ データベース内の実サーバを検索します。スティッキ オブジェクトが存在するかぎり、特定の MSS に属しているすべてのパケットが同じ BWG に対して負荷分散されます。

スティッキ MSID エントリをバックアップ IOS SLB に複製することによって、冗長性がサポートされています。冗長性は、シャーシ内（ステートフル スイッチオーバー）環境とシャーシ間（HSRP）環境の両方で動作します。セッションは、スタンバイ IOS SLB に複製する必要はありません。

GPRS ロード バランシング

GPRS は、European Telecommunications Standards Institute（ETSI）Global System for Mobile Communication（GSM）フェーズ 2+ 標準に基づくパケット ネットワーク インフラストラクチャです。GSM モバイル ユーザからのパケット データを Packet Data Network（PDN）に転送するために使用されます。Cisco Gateway GPRS Support Node（GGSN; ゲートウェイ GPRS サポート ノード）は、GTP を使用して Serving GPRS Support Node（SGSN）とインターフェイスします。トランスポートには UDP が使用されます。IOS SLB には GPRS ロード バランシング機能があり、GGSN 用に信頼性と可用性を向上しました。

IOS SLB と GGSN で共有するネットワークを設定する場合、次の注意事項を考慮してください。

- レイヤ 2 情報が適切で明確になるように、スタティック ルータ（**ip route** コマンドを使用します）および実サーバの IP アドレス（**real** コマンドを使用します）を指定します。
- 次のいずれかの方式を使用して、サブネットを慎重に選択します。
  - 仮想テンプレート アドレス サブネットの重複を回避します。
  - 実サーバ上のインターフェイスではなく、実サーバに対するネクストホップのアドレスを指定します。
- IOS SLB は、特定の IMSI から作成されたすべての PDP コンテキストを同じ GGSN に割り当てます。
- IOS SLB は、GTP version 0（GTP v0）、version 1（GTP v1）、および version 2（GTP v2）をサポートします。GTP のサポートによって、IOS SLB は、「GTP 認識」になり、レイヤ 5 に対する知識を拡張することができます。
- GPRS ロード バランシング マップによって、IOS SLB は Access Point Name（APN）に基づいてユーザ トラフィックを分類し、ルーティングできます。

IOS SLB は 2 種類の GPRS ロード バランシングをサポートします。

- 「GTP Cause Code Inspection なしの GPRS ロード バランシング」（P.32）
- 「GTP Cause Code Inspection ありの GPRS ロード バランシング」（P.33）

GTP Cause Code Inspection なしの GPRS ロード バランシング

Cisco GGSN の場合、GTP Cause Code Inspection をイネーブルにしない GPRS ロード バランシングを推奨します。このロード バランシングには次の特徴があります。

- dispatched モードまたは directed サーバ NAT モードで実行できますが、directed クライアント NAT モードでは実行できません。dispatched モードの場合、GGSN は IOS SLB デバイスに対してレイヤ 2 隣接にする必要があります。
- スティッキ接続がイネーブルの場合にだけ、ステートフル バックアップがサポートされます。詳細については、「ステートフル バックアップ」（P.30）を参照してください。

- 仮想 GGSN の IP アドレス宛てのトンネル作成メッセージを、加重ラウンド ロビン ロード バランシング アルゴリズムを使用して、実際の GGSN の 1 つに配信します。このアルゴリズムの詳細については、「加重ラウンド ロビン アルゴリズム」（P.13）を参照してください。
- GTP v1 および GTP v2 のセカンダリ PDP コンテキストを考慮に入れるには、DFP が必要です。

GTP Cause Code Inspection ありの GPRS ロード バランシング

GTP Cause Code Inspection をイネーブルにした GPRS ロード バランシングを使用すると、IOS SLB は、GGSN サーバ ファームとの間で送受信するすべての PDP コンテキスト シグナリング フローをモニタできます。それによって、GTP 障害の原因コードをモニタし、Cisco GGSN と非 Cisco GGSN の両方について、システム レベルの問題を検出できます。

表 1 は、PDP 作成応答の原因コードと、それに対して IOS SLB で実行されるアクションの一覧です。

表 1　PDP 作成応答原因コードと対応する IOS SLB アクション

原因コード	IOS SLB のアクション
Request Accepted	セッションを確立します
No Resource Available	現在の実サーバを無効と見なし、セッションを再割り当てし、応答をドロップします
All dynamic addresses are occupied	現在の実サーバを無効と見なし、セッションを再割り当てし、応答をドロップします
No memory is available	現在の実サーバを無効と見なし、セッションを再割り当てし、応答をドロップします
System Failure	現在の実サーバを無効と見なし、セッションを再割り当てし、応答をドロップします
Missing or Unknown APN	応答を転送します
Unknown PDP Address or PDP type	応答を転送します
User Authentication Failed	応答を転送します
Semantic error in TFT operation	応答を転送します
Syntactic error in TFT operation	応答を転送します
Semantic error in packet filter	応答を転送します
Syntactic error in packet filter	応答を転送します
Mandatory IE incorrect	応答を転送します
Mandatory IE missing	応答を転送します
Optional IE incorrect	応答を転送します
Invalid message format	応答を転送します
Version not supported	応答を転送します

GTP Cause Code Inspection をイネーブルにした GPRS ロード バランシングには、次の特徴があります。

- 常に directed サーバ NAT モードで動作します。
- ステートフル バックアップをサポートします。詳細については、「ステートフル バックアップ」（P.30）を参照してください。
- 各 GGSN の開いている PDP コンテキスト数を追跡します。それによって GGSN サーバ ファームは、GPRS ロード バランシングに加重最小接続（**leastconns**）アルゴリズムを使用できます。このアルゴリズムの詳細については、「加重最小接続アルゴリズム」（P.13）を参照してください。

- 要求している International Mobile Subscriber ID（IMSI）のキャリア コードが指定した値と一致しない場合、IOS SLB は仮想 GGSN に対するアクセスを拒否できます。
- DFP を使用しなくても、IOS SLB はセカンダリ PDP コンテキストを把握できます。

GTP ロード バランシングに対するデュアルスタック サポート

IPv6 サポートによって、IOS SLB ですべてのバージョンの GTP（v0、v1、v2）に対する GTP ロード バランシング用の IPv6 アドレスを管理することができます。

デュアルスタック サポートを使用すれば、IOS SLB で GTP ロード バランシング用のデュアルスタック実装を管理することができます。デュアルスタック実装とは、IPv4 アドレスと IPv6 アドレスの両方を使用する実装です。

デュアルスタック サポートが GTP ロード バランシング用に設定されている場合は、次の留意点を考慮してください。

- 実サーバは、SLB サーバ ファーム コンフィギュレーション モードで **real** コマンドを使用して、IPv4 アドレスと IPv6 アドレスを持つデュアルスタック実サーバとして設定する必要があります。
- 仮想サーバは、SLB 仮想サーバ ファーム コンフィギュレーション モードで **virtual** コマンドを使用して、IPv4 アドレス、IPv6 アドレス、およびオプションの IPv6 プレフィクスを持つデュアルスタック仮想サーバとして設定する必要があります。
- プライマリ IPv6 サーバ ファームとオプションのバックアップ IPv6 サーバ ファームを指定するには、SLB 仮想サーバ コンフィギュレーション モードで **serverfarm** コマンドを使用します。
- SLB 仮想サーバ コンフィギュレーション モードの **client** コマンドはサポートされていません。
- ゲートウェイは、仮想サーバの IPv4 アドレスと IPv6 アドレスで設定する必要があります。
- IOS SLB とゲートウェイ間のインターフェイスは、デュアルスタック アドレスで設定する必要があります。
- クライアント側インターフェイスのすべての HSRP インスタンス（IPv4 と IPv6 の両方）を同じ HSRP ステートにする必要があります。

Home Agent Director

Home Agent Director は、ホーム エージェント セット（サーバ ファームの実サーバとして設定されます）の中で、Mobile IP Registration Request（RRQ）のロード バランシングを実行します。ホーム エージェントは、モバイル ノードのアンカー ポイントです。ホーム エージェントは、モバイル ノードのフローを現在の外部エージェント（接続ポイント）にルーティングします。

Home Agent Director には次の特徴があります。

- dispatched モードまたは directed サーバ NAT モードで実行できますが、directed クライアント NAT モードでは実行できません。dispatched モードの場合、ホーム エージェントは IOS SLB デバイスに対して レイヤ 2 隣接にする必要があります。
- ステートフル バックアップをサポートしません。詳細については、「ステートフル バックアップ」（P.30）を参照してください。
- 仮想 Home Agent Director の IP アドレス宛ての RRQ を、加重ラウンド ロビン ロード バランシング アルゴリズムを使用して、実際のホーム エージェントの 1 つに配信します。このアルゴリズムの詳細については、「加重ラウンド ロビン アルゴリズム」（P.13）を参照してください。
- 容量に基づいて RRQ を割り当てるには、DFP が必要です。

Mobile IP、ホーム エージェントの詳細と関連するトピックについては、『*Cisco IOS IP Configuration Guide*, Release 12.2』を参照してください。

KeepAlive Application Protocol（KAL-AP）エージェントのサポート

KAL-AP エージェントのサポートを使用すれば、IOS SLB を通して、Global Server Load Balancing（GSLB; グローバル サーバ ロード バランシング）環境でロード バランシングを実行することができます。KAL-AP は、負荷情報とキープアライブ応答メッセージを KAL-AP マネージャまたは GSLB デバイス（Global Site Selector（GSS）など）に提供します。また、GSLB デバイスが、最も負荷が少ない IOS SLB デバイスにクライアント要求の負荷を分散できるように支援します。

KAL-AP エージェントのサポートを IOS SLB に設定する場合、次の注意事項を考慮してください。

- KAL-AP エージェントのサポートによって、受信要求パケットの Virtual Private Network（VPN）Routing and Forwarding（VRF）ID を自動的に検出し、応答のソリューション指示に同じ VRF ID を使用します。
- DNS キャッシングを使用するクライアントは、GSS を介して要求を送信するのではなく、IOS SLB に直接送信できます。そのため、このような状況を回避するために、クライアントで DNS 設定を指定してください。

KAL-AP は、相対的または絶対的のいずれかの方法で、負荷値を算出します（IOS SLB CPU/ メモリ負荷は、最終的な KAL-AP 負荷値に影響を及ぼす可能性があります）。

相対的 KAL-AP 負荷値

サーバ ファーム コンフィギュレーション モードで **farm-weight** コマンドを設定していない場合、または IOS SLB で DFP がイネーブルではない場合、KAL-AP は次の数式を使用して相対的な負荷値を算出します。

KAL-AP 負荷 = 256 -（*アクティブな実サーバの数* *** 256**/ *稼動中の実サーバの数*）

たとえば、サイトに 2 つの実サーバがあり、両方の実サーバがサービスに参加していますが、現在アクティブなサーバは 1 つだけの場合、そのサイトの KAL-AP 負荷値は次のようになります。

KAL-AP 負荷 = 256 - (1 * 256/2) = 256 - 128 = 128

絶対的 KAL-AP 負荷値

サーバ ファーム コンフィギュレーション モードで **farm-weight** コマンドを設定しており、IOS SLB で DFP がイネーブルの場合、KAL-AP は次の数式を使用して絶対的な負荷値を算出します。

KAL-AP 負荷 = 256 -（*実サーバの最大 DFP 加重の合計* *** 256**/ *ファームの加重*）

（注） 実サーバの最大 DFP 加重は、グローバル コンフィギュレーション モードで **gprs dfp max-weight** コマンドを使用して設定します。ただし、KAL-AP にレポートされる実際の DFP 加重は、GGSN の負荷に比例します。たとえば、100 の最大 DFP 加重に GGSN が設定されているが、GGSN の負荷が 50% の場合は、50 の最大 DFP 負荷を KAL-AP に報告します。

実サーバへの DFP 接続がダウンしている場合は、KAL-AP が SLB 実サーバ コンフィギュレーション モードの **weight** コマンドの設定を使用します。実サーバに対して **weight** コマンドが設定されていない場合、KAL-AP では 8 というデフォルトの加重が使用されます。

たとえば、次の設定のサイトがあるとします。

- サーバ ファームには 200 のファーム加重が設定されています。
- GGSN-1 に 100 の最大 DFP 加重が設定され、0% の負荷です（そのため、100 の DFP 加重が報告されます）。

- GGSN-2 に 100 の最大 DFP 加重が設定され、50% の負荷です（そのため、50 の DFP 加重が報告されます）。

このサイトの KAL-AP 負荷値は次のようになります。

KAL-AP 負荷 = 256 - [(100 + 50) * 256/200] = 256 - 192 = 64

最適な結果を得るには、サーバ ファームの実サーバの最大 DFP 加重の合計と等値になるように**ファームの加重**を設定します。たとえば、サーバ ファームに 3 つの実サーバがあり、100、50、および 50 の最大 DFP 加重が設定されている場合、200（つまり、100 + 50 + 50）の**ファームの加重**を設定します。サーバ ファームに実サーバを追加した場合、またはファームから削除した場合、それに従って**ファームの加重**を調整する必要があります。

RADIUS ロード バランシング

IOS SLB には、RADIUS サーバ用の RADIUS ロード バランシング機能があります。さらに IOS SLB は、従来およびモバイルのワイヤレス ネットワークの両方で、RADIUS の認可フローとアカウンティング フローをプロキシするデバイスを必要に応じて負荷を分散できます。そのために IOS SLB では、その加入者フローの RADIUS を処理した同じプロキシに、データ フローが関連付けられます。

IOS SLB は、サービス ゲートウェイ（Cisco Service Selection Gateway（SSG）または Cisco Content Services Gateway（CSG））を使用するモバイル ワイヤレス ネットワークに RADIUS ロード バランシング機能を提供します。次のモバイル ワイヤレス ネットワークがサポートされます。

- GPRS ネットワーク。GPRS モバイル ワイヤレス ネットワークでは、RADIUS クライアントは通常 GGSN です。
- 簡易 IP CDMA2000 ネットワーク。CDMA2000 は Third-Generation（3-G; 第 3 世代）バージョンの Code Division Multiple Access（CDMA; 符号分割多重接続）です。簡易 IP CDMA2000 モバイル ワイヤレス ネットワークの場合、RADIUS クライアントは Packet Data Service Node（PDSN）です。
- Mobile IP CDMA2000 ネットワーク。Mobile IP CDMA2000 モバイル ワイヤレス ネットワークの場合、Home Agent（HA）および PDSN/Foreign Agent（PDSN/FA）の両方が RADIUS クライアントです。

また、次の RADIUS ロード バランシング機能があります。

- 使用可能な RADIUS サーバおよびプロキシ サーバに、RADIUS 要求を分散します。
- RADIUS 要求の再送信（未応答の要求の再送信など）を、元の要求と同じ RADIUS サーバまたはプロキシ サーバにルーティングします。
- すべての加入者の RADIUS フローと、同じ加入者の非 RADIUS データ フローを、同じサービス ゲートウェイにルーティングします。
- 複数のサービス ゲートウェイ サーバ ファームをサポートします（たとえば、SSG ファームと CSG ファーム）。適切なサービス ゲートウェイ サーバ ファームにルーティングするために、パケットの入力インターフェイスが確認されます。
- RADIUS ロード バランシング仮想サーバの背後に、複数の WAP ゲートウェイ サーバ ファームを配置できます。RADIUS 発信ステーション ID およびユーザ名を使用して特定のサーバ ファームを選択できます。この強化によって、コントロール プレーンとデータ プレーンの両方で RADIUS ロード バランシングが可能になります。コントロール プレーンの RADIUS ロード バランシングでは、加入者の認可、認証、およびアカウンティングに関して、RADIUS メッセージの負荷を AAA サーバに分散できます。データ プレーン上の RADIUS ロード バランシングを使用すれば、特定の加入者のデータ フローで、宛先ネットワーク デバイスへの一貫したネットワーク パスを維持できます。さらに、RADIUS 仮想サーバは RADIUS アカウンティング メッセージを承認し、スティッキ オブジェクトを構築または削除できます。メッセージを指定したサーバに転送する必要はありません。

- データ パケットを CSG ファームの実サーバにルーティングしてから、SSG ファームの実サーバにルーティングできます。
- 加入者の RADIUS Access-Request メッセージを処理したサービス ゲートウェイに対して、RADIUS クライアントからの RADIUS Accounting-Request メッセージをルーティングします。その後、サービス ゲートウェイはその加入者に関して作成したホスト エントリを消去できます。
- 加重ラウンド ロビン アルゴリズムを使用します。このアルゴリズムの詳細については、「加重ラウンド ロビン アルゴリズム」（P.13）を参照してください。
- RADIUS プロトコル経由の SSG シングル サインオンを容易にします。
- セッションベースの自動障害検出機能があります。
- ステートレス バックアップとステートフル バックアップの両方をサポートします。

RADIUS ロード バランシングを実行するには、IOS SLB に次の RADIUS スティッキ データベースを使用します。

- IOS SLB RADIUS framed-IP スティッキ データベースは、各加入者の IP アドレスを特定のサービス ゲートウェイに関連付けます。GPRS モバイル ワイヤレス ネットワークの場合、IOS SLB は RADIUS framed-IP スティッキ データベースを使用して、パケットを適切にルーティングします。

（注） 加入者の IP アドレスは、サービス ゲートウェイまたは RADIUS クライアントによって割り当てられます。サービスごとに分離されたゲートウェイ プールから加入者の IP アドレスが割り当てられている場合（そのため、ネクストホップのサービス ゲートウェイを発信元 IP アドレスに基づいて選択できる場合）、加入者フローのルーティングにポリシー ルーティングを使用できます。

- IOS SLB RADIUS calling-station-ID スティッキ データベースは、各加入者の発信ステーション ID を特定のサービス ゲートウェイに関連付けます。
- IOS SLB RADIUS username スティッキ データベースは、各加入者のユーザ名を特定のサービス ゲートウェイに関連付けます。
- RADIUS ロード バランシング マップによって、IOS SLB は RADIUS 発信側ステーション ID とユーザ名に基づいてユーザ トラフィックを分類し、ルーティングすることができます。RADIUS ロード バランシング マップは、Turbo RADIUS ロード バランシングおよび RADIUS ロード バランシング アカウンティングのローカル ACK と同時に使用できません。
- RADIUS ロード バランシング アカウンティング ローカル確認応答：
  - IOS SLB は RADIUS アカウンティング パケットに ACK で応答しながら、そのセッションのスティッキ オブジェクトを維持できるようになります。
  - RADIUS ロード バランシング マップおよび Turbo RADIUS ロード バランシングと相互排他的です。
- CDMA2000 モバイル ワイヤレス ネットワークの場合、パケットを適切にルーティングするには、RADIUS framed-IP スティッキ データベースに加え、RADIUS username スティッキ データベースまたは RADIUS calling-station-ID スティッキ データベースが必要です。
- IOS SLB RADIUS International Mobile Subscriber ID（IMSI）は、各ユーザの IMSI アドレスを対応するゲートウェイにルーティングします。その結果、同じユーザに対する以降のすべてのフローを同じゲートウェイに転送できるようになります。

RADIUS ロード バランシング加速データ プレーン フォワーディング

RADIUS ロード バランシング加速データ プレーン フォワーディング（Turbo RADIUS ロード バランシングとも呼ばれる）は、CSG 環境で基本的な PBR ルート マップを使用して加入者のデータプレーン トラフィックを管理する高性能ソリューションです。

Turbo RADIUS ロード バランシングが RADIUS ペイロードを受信すると、次のアクションを実行します。

1. ペイロードを検査する。
2. framed-IP アトリビュートを抽出する。
3. ルート マップを IP アドレスに適用する。
4. 加入者を管理する CSG を決定する。

Vendor-Specific Attribute（VSA; ベンダー固有アトリビュート）関連付けを設定し、Cisco VSA がバッファリングされている場合、Cisco VSA は RADIUS Accounting-Start パケットに注入されます。

Turbo RADIUS ロード バランシングに VSA 関連付けは必要ありませんが、アカウンティング仮想サーバに **predictor route-map** で設定したサーバ ファームは必要です。

（注） SLB サーバ ファーム コンフィギュレーション モードで **predictor route-map** コマンドを指定する場合、SLB サーバ ファーム コンフィギュレーション モードまたは実サーバ コンフィギュレーション モードで他のコマンドは使用できません。

ポリシーベース ルーティングの詳細については、『*Cisco IOS IP Routing Configuration Guide*』の「Policy-Based Routing」と「Configuring Policy-Based Routing」を参照してください。

mobile Service Exchange Framework（mSEF）環境の場合、CSG クラスタのネットワーク側では、Turbo RADIUS ロード バランシングにファイアウォール ロード バランシングは必要ありません（クラスタのネットワーク側では、標準の RADIUS ロード バランシングにファイアウォール ロード バランシングは必要ありません）。

Turbo RADIUS ロード バランシング

- 単純な IP アクセス コントロール リスト（ACL）をサポートし、ネクストホップ ペアのマッチングと設定を行います。
- RADIUS ロード バランシング マップおよび Turbo RADIUS ロード バランシング アカウンティング ローカル確認応答と相互排他的です。
- オプションの ACL ロキング ファシリティと相互排他的です。Turbo RADIUS ロード バランシングを使用するには、まずロギング ファシリティをディセーブルにする必要があります。詳細については、『*Cisco IOS Security Command Reference*（Cisco IOS 12.4）』の **access-list（IP 標準）**コマンドの説明を参照してください。

WAP ロード バランシング

IOS SLB を使用して、IP ベアラ ネットワーク上の WAP ゲートウェイまたはサーバのグループ内で、WSP セッションを負荷分散させることができます。WAP は、既知のポート セットで、UDP 上で実行されます。各ポートは異なる WAP モードを示します。

- Connectionless WSP モード（IP/UDP [9200]/WSP）。Connectionless WSP モードでは、WSP が、1 つのサーババインド パケットが 1 つまたは複数のパケットのサーバ応答になる単純な 1 要求/1 応答プロトコルになります。
- Connection-oriented WSP モード（IP/UDP [9201]/WTP/WSP）。Connection-oriented WSP モードでは、WTP が WDP イベントの再送信を管理し、WSP が、定義されたセッション起動/切断シーケンスを使用して動作します。セッションの再割り当てには、WSP セッションのイベントによって動作する WAP 対応の Finite State Machine（FSM; 有限状態マシン）が使用されます。この FSM はポート 9201 上でのみ動作します。ここでは、WSP セッションが暗号化されず、WTP が再送信を管理します。
- Connectionless Secure WSP モード（IP/UDP [9202]/WTLS/WSP）。このモードの機能は Connectionless WSP モードと同じですが、WTLS によってセキュリティが提供されます。
- Connection-oriented Secure WSP モード（IP/UDP [9203]/WTLS/WTP/WSP）。このモードの機能は Connection-oriented WSP モードと同じですが、WTLS によってセキュリティが提供されます。

ポート 9201 の WAP スタックの障害を検出するには、WSP プローブを使用します。

冗長ルート プロセッサのステートフル バックアップ

RPR+ を併用した場合、IOS SLB は Cisco Catalyst 6500 スイッチと Cisco 7600 ルータの mSEF に対して、冗長ルート プロセッサのステートフル バックアップをサポートします。これによって、IOS SLB と同じシャーシに Cisco Multiprocessor WAN Application Module（MWAN）を配置しながら、ロード バランシング割り当てのハイ アベイラビリティを維持できます。

フローの永続性

フローの永続性には、負荷分散された IP フローを適切なノードに返す、高度なリターン ルーティング機能があります。負荷分散されたデータ パスの両側でハッシュ メカニズムを調整する必要はありません。また、ネットワーク アドレス変換（NAT）やプロキシを使用して、クライアントまたはサーバの IP アドレスを変更する必要もありません。

IOS SLB 機能の設定方法

IOS SLB の設定には、サーバ ファームの特定、サーバ ファームの実サーバ グループの設定、およびクライアントに対して実サーバを表現する仮想サーバの設定という処理があります。

これらの作業に関連する設定例については、「IOS SLB の設定例」（P.120）を参照してください。

この項の IOS SLB コマンドの詳細な説明については、『*Cisco IOS IP Application Services Command Reference*』の「Server Load Balancing Commands」の章を参照してください。この項に記載されている他のコマンドのマニュアルについては、Cisco.com でオンライン検索してください。

IOS SLB を設定するには、次の項の作業を実行します。

必須と任意の IOS SLB 機能の設定方法

IOS SLB 機能を設定するには、次の項の作業を実行します。必須および任意の作業を示します。

- 「サーバ ファームと実サーバの設定方法」（P.41）（必須）
- 「仮想サーバの設定方法」（P.45）（必須）
- 「仮想サーバの確認方法」（P.51）（任意）
- 「サーバ ファームの確認方法」（P.51）（任意）
- 「クライアントの確認方法」（P.52）（任意）
- 「IOS SLB 接続の確認方法」（P.52）（任意）

サーバ ファームと実サーバの設定方法

サーバ ファームと実サーバを設定するには、この必須作業を実行します。

（注） 複数のユーザ セッションから同時に IOS SLB を設定することはできません。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip slb serverfarm** *server-farm*
4. **access** *interface*
5. **bindid** [*bind-id*]
6. **nat** {**client** *pool* | **server**}
7. **predictor** [**roundrobin** | **leastconns** | **route-map** *mapname*]
8. **probe** *probe*
9. **real** *ipv4-address* [**ipv6** *ipv6-address*] [*port*]
10. **faildetect numconns** *number-of-conns* [**numclients** *number-of-clients*]
11. **maxclients** *number-of-conns*
12. **maxconns** *number-of-conns* [**sticky-override**]
13. **reassign** *threshold*
14. **retry** *retry-value*
15. **weight** *setting*
16. **inservice**

手順の詳細

	コマンド	説明
ステップ 1	**enable** 例： Router> **enable**	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： Router# **configure terminal**	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 3	**ip slb serverfarm** *server-farm* 例： Router(config)# **ip slb serverfarm PUBLIC**	サーバ ファームの定義を IOS SLB 設定に追加し、サーバ ファーム 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	**access** *interface* 例： Router(config-slb-sfarm)# **access GigabitEthernet 0/1.1**	(任意）サーバ ファームのアクセス インターフェイスまたはサブインターフェイスを設定します。
ステップ 5	**bindid** [*bind-id*] 例： Router(config-slb-sfarm)# **bindid 309**	(任意）Dynamic Feedback Protocol（DFP）に使用されるサーバ ファームのバインド ID を指定します。 **（注）** GPRS ロード バランシングおよび Home Agent Director は、このコマンドをサポートしません。
ステップ 6	**nat** {**client** *pool* | **server**} 例： Router(config-slb-sfarm)# **nat server**	(任意）サーバ ファームで、ネットワーク アドレス変換（NAT）クライアントの変換モードまたは NAT サーバ アドレス変換モードを設定します。 同じ仮想サーバに関連付けられたすべての IPv4 または IPv6 サーバ ファームは、同じ NAT 設定にする必要があります。

	コマンド	説明
ステップ 7	**predictor** [**roundrobin** | **leastconns** | **route-map** *mapname*] **例：** Router(config-slb-sfarm)# **predictor leastconns**	（任意）実サーバを選択する方法を決定するために使用するアルゴリズムを指定します。 **（注）** RADIUS ロード バランシングには、デフォルト設定（加重ラウンド ロビン アルゴリズム）が必要です。 GTP Cause Code Inspection がイネーブルになっていない GPRS ロード バランシングでは、デフォルト設定（加重ラウンド ロビン アルゴリズム）を受け入れる必要があります。 Home Agent Director には、デフォルト設定（加重ラウンド ロビン アルゴリズム）が必要です。 SLB サーバ ファーム コンフィギュレーション モードで **predictor route-map** コマンドを指定する場合、SLB サーバ ファーム コンフィギュレーション モードまたは実サーバ コンフィギュレーション モードで他のコマンドは使用できません。 詳細については、次のセクションを参照してください。 • 「加重ラウンド ロビン アルゴリズム」（P.13） • 「加重最小接続アルゴリズム」（P.13） • 「ルート マップ アルゴリズム」（P.14）
ステップ 8	**probe** *probe* **例：** Router(config-slb-sfarm)# **probe PROBE1**	（任意）プローブを実サーバに関連付けます。
ステップ 9	**real** *ipv4-address* [**ipv6** *ipv6-address*] [*port*] **例：** Router(config-slb-sfarm)# **real 10.1.1.1**	サーバ ファームのメンバとして、実サーバを IPv4 アドレスと、オプションの IPv6 アドレスとポート番号で識別し、実サーバ コンフィギュレーション モードを開始します。 **（注）** GPRS ロード バランシングでは、GGSN 機能を実行している実サーバの IP アドレス（Cisco GGSN の場合は仮想テンプレート アドレス）を指定します。 VPN サーバ ロード バランシングでは、VPN ターミネータとして機能している実サーバの IP アドレスを指定します。 Home Agent Director の場合は、ホーム エージェントとして機能している実サーバの IP アドレスを指定します。 GTP ロード バランシングに対するデュアルスタック サポートの場合は、実サーバの IPv4 アドレスと IPv6 アドレスを指定します。

	コマンド	説明
ステップ 10	**faildetect numconns** *number-of-conns* [**numclients** *number-of-clients*] 例： Router(config-slb-real)# **faildetect numconns 10 numclients 3**	（任意）連続する接続エラーの回数、およびオプションで特定クライアントの接続エラーの回数を指定します。この回数を超えると、実サーバの障害と見なされます。 • GPRS ロード バランシングでは、環境内に 1 つの SGSN しか設定されていなければ、値が 1 の **numclients** キーワードを指定します。 • RADIUS ロード バランシングの場合、自動的なセッションベースの障害検出のために、値 1 の **numclients** キーワードを指定します。
ステップ 11	**maxclients** *number-of-conns* 例： Router(config-slb-real)# **maxclients 10**	（任意）個々の仮想サーバに割り当てることができる IOS SLB RADIUS および GTP スティッキ加入者の最大数を指定します。
ステップ 12	**maxconns** *number-of-conns* [**sticky-override**] 例： Router(config-slb-real)# **maxconns 1000**	（任意）実サーバで同時に使用できるアクティブな接続の最大数を指定します。
ステップ 13	**reassign** *threshold* 例： Router(config-slb-real)# **reassign 2**	（任意）連続して ACK が受信されない SYNchronize Sequence Number（SYN）要求または Create Packet Data Protocol（PDP）要求のしきい値を指定します。しきい値を超えると、別の実サーバに接続が試行されます。 **（注）** GPRS ロード バランシングの場合、SGSN の N3-REQUESTS カウンタ値未満の再割り当てしきい値を指定する必要があります。
ステップ 14	**retry** *retry-value* 例： Router(config-slb-real)# **retry 120**	（任意）サーバ障害が検出されてから、そのサーバへの接続を再試行するまでの時間間隔を秒単位で指定します。
ステップ 15	**weight** *setting* 例： Router(config-slb-real)# **weight 24**	（任意）実サーバの作業負荷容量をサーバ ファーム内の他のサーバと比較して指定します。 **（注）** Dynamic Feedback Protocol（DFP）を使用する場合、サーバ ファーム コンフィギュレーション モードで **weight** コマンドを使用して定義したスタティック加重よりも、DFP によって算出された加重の方が優先されます。ネットワークから DFP を外すと、IOS SLB はスタティックな加重に戻されます。
ステップ 16	**inservice** 例： Router(config-slb-real)# **inservice**	実サーバを IOS SLB で使用できるようにします。

（注） サーバ ロード バランシングとファイアウォール ロード バランシングの両方を Cisco Catalyst 6500 ファミリ スイッチ上で実行している場合は、**mls ip slb wildcard search rp** コマンドを使用して、Policy Feature Card（PFC; ポリシー フィーチャ カード）上の Telecommunications Access Method（TCAM）の容量を超える可能性を低減します。詳細については、「ワイルドカード検索の設定方法」（P.112）を参照してください。

仮想サーバの設定方法

仮想サーバを設定するには、この必須作業を実行します。IOS SLB は最大 500 仮想サーバをサポートします。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip slb vserver** *virtual-server*
4. **virtual** *ipv4-address* [*ipv4-netmask* [**group**]] {**esp** | **gre** | *protocol*}

   または

   virtual *ipv4-address* [*ipv4-netmask* [**group**]] [**ipv6** *ipv6-address* [**prefix** *ipv6-prefix*]] {**tcp** | **udp**} [*port* | **any**] [**service** *service*]
5. **serverfarm** *primary-farm* [**backup** *backup-farm* [**sticky**]] [**ipv6-primary** *ipv6-primary-farm* [**ipv6-backup** *ipv6-backup-farm*]] [**map** *map-id* **priority** *priority*]
6. **access** *interface* [**route framed-ip**]
7. **advertise** [**active**]
8. **client** {*ipv4-address netmask* [**exclude**] | **gtp carrier-code** [*code*]}
9. **delay** {*duration* | **radius framed-ip** *duration*}
10. **gtp notification cac** [*reassign-count*]
11. **gtp session**
12. **gw port** *port*
13. **hand-off radius** *duration*
14. **idle** [**asn request** *duration* | **asn msid** *msid* | **gtp imsi** *duration* [**query** [*max-queries*]] | **gtp request** *duration* | **ipmobile request** *duration*| **radius** {**request** | **framed-ip**} *duration*]
15. **purge radius framed-ip acct on-off**
16. **purge radius framed-ip acct stop** {*attribute-number* | {**26** | *vsa*} {*vendor-ID* | **3gpp** | **3gpp2**} *sub-attribute-number*}
17. **radius acct local-ack key** [*encrypt*] *secret-string*
18. **radius inject auth** *group-number* {**calling-station-id** | **username**}
19. **radius inject auth timer** *seconds*
20. **radius inject auth vsa** *vendor-id*
21. **replicate casa** *listen-ip remote-ip port* [*interval*] [**password** [*encrypt*] *secret-string timeout*]
22. **replicate interval** *interval*
23. **replicate slave**
24. **sticky** {*duration* [**group** *group-id*] [**netmask** *netmask*] | **asn msid** [**group** *group-id*] | **gtp imsi** [**group** *group-id*] | **radius calling-station-id** | **radius framed-ip** [**group** *group-id*] | **radius username** [**msid-cisco**] [**group** *group-id*]}
25. **synguard** *syn-count interval*
26. **inservice** [**standby** *group-name*] [**active**]

手順の詳細

	コマンド	説明
ステップ 1	**enable** 例： Router> **enable**	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： Router# **configure terminal**	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 3	**ip slb vserver** *virtual-server* 例： Router(config)# **ip slb vserver PUBLIC_HTTP**	仮想サーバを指定し、仮想サーバ 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	**virtual** *ipv4-address* [*ipv4-netmask* [**group**]] {**esp** | **gre** | *protocol*} または **virtual** *ipv4-address* [*ipv4-netmask* [**group**]] [**ipv6** *ipv6-address* [**prefix** *ipv6-prefix*]] {**tcp** | **udp**} [*port* | **any**] [**service** *service*] 例： Router(config-slb-vserver) # **virtual 10.0.0.1 tcp www**	仮想サーバの IP アドレス、接続の種類、およびオプションの TCP またはユーザ データグラム プロトコル（UDP）のポート番号を指定し、Internet Key Exchange（IKE; インターネット キー エクスチェンジ）または Wireless Session Protocol（WSP）の設定、およびサービスのカップリングを指定します。 **（注）** RADIUS ロード バランシングの場合、**service radius** キーワード オプションを指定します。 **（注）** ASN ロード バランシングの場合、**service asn** キーワード オプションを指定します。 **（注）** GPRS ロード バランシングの場合： – 仮想 GGSN IP アドレスを仮想サーバとして指定し、**udp** キーワード オプションを指定します。 – GTP v1 および GTP v2 セッションの負荷を分散するには、GGSN および SGSN が ETSI 標準に準拠している場合、ポート番号 2123 を指定します。また、全ポート仮想サーバ（つまり、すべてのポート宛てのフローを受け入れる仮想サーバ）を設定するには、ポート番号 0 または **any** を指定します。 – GTP v0 セッションの負荷を分散するには、GGSN および SGSN が ETSI 標準に準拠している場合、ポート番号 3386 を指定します。また、全ポート仮想サーバを設定するには、ポート番号 0 または **any** を指定します。 – GTP Cause Code Inspection *なし*の GPRS ロード バランシングをイネーブルにするには、**service gtp** キーワード オプションを指定します。 – GTP Cause Code Inspection *あり*の GPRS ロード バランシングをイネーブルにするには、**service gtp-inspect** キーワード オプションを指定します。 – GTP ロード バランシングに対するデュアルスタック サポートの場合は、仮想サーバの IPv4 アドレス、IPv6 アドレス、およびオプションの IPv6 プレフィクスを指定します。

	コマンド	説明
ステップ 5	**serverfarm** *primary-farm* [**backup** *backup-farm* [**sticky**]] [**ipv6-primary** *ipv6-primary-farm* [**ipv6-backup** *ipv6-backup-farm*]] [**map** *map-id* **priority** *priority*] 例： Router(config-slb-vserver) # **serverfarm SF1 backup SF2 map 1 priority 1**	実サーバ ファームを仮想サーバに関連付け、オプションで、バックアップ サーバ ファームを設定し、バックアップ サーバ ファームでスティッキ接続を使用することを指定します。 **（注）** RADIUS ロード バランシングと Home Agent Director は、**sticky** キーワードをサポートしません。 複数のサーバ ファームを特定の RADIUS サーバに関連付けるには、複数の **serverfarm** コマンドのそれぞれを一意のマップ ID とプライオリティで設定します（つまり、各マップ ID および各マップ プライオリティは、仮想サーバに関連付けられているすべてのサーバ ファームで固有にする必要があります）。 GPRS ロード バランシングで、複数のサーバ ファームに 1 つの実サーバが定義されている場合、各サーバ ファームは異なる仮想サーバに関連付ける必要があります。 GTP ロード バランシングに対するデュアルスタック サポートの場合は、プライマリ IPv6 サーバ ファームとオプションのバックアップ IPv6 サーバ ファームを指定します。 同じ仮想サーバに関連付けられたすべての IPv4 または IPv6 サーバ ファームは、同じ NAT 設定にする必要があります。
ステップ 6	**access** *interface* [**route framed-ip**] 例： Router(config-slb-vserver) # **access Vlan20 route framed-ip**	（任意）入力インターフェイスを検査するには、framed-IP ルーティングをイネーブルにします。
ステップ 7	**advertise** [**active**] 例： Router(config-slb-vserver) # **advertise**	（任意）仮想サーバ アドレスの Null0 インターフェイスに対するスタティック ルートのインストールを制御します。
ステップ 8	**client** {*ipv4-address netmask* [**exclude**] | **gtp carrier-code** [*code*]} 例： Router(config-slb-vserver) # **client 10.4.4.0 255.255.255.0**	（任意）仮想サーバの使用を許可するクライアントを指定します。 **（注）** GTP Cause Code Inspection がイネーブルの場合に限り、GPRS ロード バランシングは **gtp carrier-code** オプションだけをサポートします。 GTP ロード バランシングに対するデュアルスタック サポートは、このコマンドをサポートしません。
ステップ 9	**delay** {*duration* | **radius framed-ip** *duration*} 例： Router(config-slb-vserver) # **delay 30**	（任意）接続の終了後に IOS SLB が TCP 接続コンテキストを維持する時間を指定します。

	コマンド	説明
ステップ 10	**gtp notification cac** [*reassign-count*] 例： Router(config-slb-vserver) # **gtp notification cac 5**	（任意）IOS SLB が GGSN-IOS SLB メッセージングのために新しい実サーバにセッションを割り当てることができる回数を制限します。
ステップ 11	**gtp session** 例： Router(config-slb-vserver) # **no gtp session**	（任意）IOS SLB で GTP ロード バランシング セッションを作成できるようにします。これがデフォルトの設定です。 GTP 用の sticky-only ロード バランシングをイネーブルにするには、このコマンドの **no** 形式を使用します。 **no gtp session** sticky-only ロード バランシングをイネーブルにした場合は、**sticky（仮想サーバ）**コマンドを使用して、仮想サーバのスティッキ接続もイネーブルにする必要があります。
ステップ 12	**gw port** *port* 例： Router(config-slb-vserver) # **gw port 63082**	（任意）Cisco BWG が IOS SLB との通信に使用するポートを指定します。
ステップ 13	**hand-off radius** *duration* 例： Router(config-slb-vserver) # **hand-off radius 30**	（任意）外部エージェントのハンドオフ時に、IOS SLB が新しい Mobile IP 外部エージェントからの ACCT-START メッセージを待機する時間を変更します。
ステップ 14	**idle** [**asn request** *duration* | **asn msid** *msid* | **gtp imsi** *duration* [**query** [*max-queries*]] | **gtp request** *duration* | **ipmobile request** *duration* | **radius** {**request** | **framed-ip**} *duration*] 例： Router(config-slb-vserver) # **idle 120**	（任意）パケット アクティビティが存在しない場合に、IOS SLB が接続コンテキストを維持する最短時間を指定します。 **（注）** GTP Cause Code Inspection をイネーブルに*しない*GPRS ロード バランシングの場合、SGSN 上の PDP コンテキスト要求間で可能な最も長い間隔よりも、長いアイドル タイマーを指定します。
ステップ 15	**purge radius framed-ip acct on-off** 例： Router(config-slb-vserver) # **purge radius framed-ip acct on-off**	（任意）Accounting ON または OFF メッセージの受信時に、IOS SLB で IOS SLB RADIUS framed-ip スティッキ データベース内のエントリを消去できるようにします。

	コマンド	説明
ステップ 16	**purge radius framed-ip acct stop** {*attribute-number* | {**26** | *vsa*} {*vendor-ID* | **3gpp** | **3gpp2**} *sub-attribute-number*} 例： Router(config-slb-vserver) # **purge radius framed-ip acct stop 44**	（任意）Accounting-Stop メッセージの受信時に、IOS SLB で IOS SLB RADIUS framed-ip スティッキ データベース内のエントリを消去できるようにします。
ステップ 17	**radius acct local-ack key** [*encrypt*] *secret-string* 例： Router(config-slb-vserver) # **radius acct local-ack key SECRET_PASSWORD**	（任意）RADIUS 仮想サーバが RADIUS アカウンティング メッセージを承認できるようにします。
ステップ 18	**radius inject auth** *group-number* {**calling-station-id** | **username**} 例： Router(config-slb-vserver) # **radius inject auth 1 calling-station-id**	（任意）RADIUS ロード バランシング加速データ プレーン フォワーディングの認証仮想サーバについて、ベンダー固有アトリビュート（VSA）関連付けグループを設定します。また、RADIUS 発信ステーション ID または RADIUS ユーザ名に基づいて、IOS SLB で VSA 関連付けエントリを作成するかどうかを指定します。
ステップ 19	**radius inject auth timer** *seconds* 例： Router(config-slb-vserver) # **radius inject auth timer 45**	（任意）IOS SLB RADIUS ロード バランシング加速データ プレーン フォワーディング認証仮想サーバの VSA 関連付け用のタイマーを設定します。
ステップ 20	**radius inject auth vsa** *vendor-id* 例： Router(config-slb-vserver) # **radius inject auth vsa vendor1**	（任意）IOS SLB RADIUS ロード バランシング加速データ プレーン フォワーディング認証仮想サーバの VSA 関連付け用の VSA をバッファします。
ステップ 21	**replicate casa** *listen-ip remote-ip port* [*interval*] [**password** [*encrypt*] *secret-string timeout*] 例： Router(config-slb-vserver) # **replicate casa 10.10.10.11 10.10.11.12 4231**	（任意）IOS SLB ディシジョン テーブルのバックアップ スイッチへのステートフル バックアップを設定します。 **（注）** Home Agent Director はこのコマンドをサポートしません。 **virtual** コマンドに **service gtp** キーワードを指定して、**sticky** コマンドに **gtp imsi** キーワードを指定しなかった場合は、**replicate casa** コマンドがサポートされません（これは、セッションが持続されず、何も複製されないためです）。

	コマンド	説明
ステップ 22	**replicate interval** *interval* 例： Router(config-slb-vserver) # **replicate interval 20**	（任意）IOS SLB 仮想サーバの複製配信間隔を設定します。 **（注）** Home Agent Director はこのコマンドをサポートしません。 **virtual** コマンドに **service gtp** キーワードを指定して、**sticky** コマンドに **gtp imsi** キーワードを指定しなかった場合は、**replicate casa** コマンドがサポートされません（これは、セッションが持続されず、何も複製されないためです）。
ステップ 23	**replicate slave** 例： Router(config-slb-vserver) # **replicate slave**	（任意）IOS SLB 仮想サーバの冗長ルート プロセッサのステートフル バックアップをイネーブルにします。 **（注）** Home Agent Director はこのコマンドをサポートしません。 **virtual** コマンドに **service gtp** キーワードを指定して、**sticky** コマンドに **gtp imsi** キーワードを指定しなかった場合は、**replicate casa** コマンドがサポートされません（これは、セッションが持続されず、何も複製されないためです）。 **replicate slave** が設定された 1 つのスーパーバイザ エンジンを使用している場合は、そのスーパーバイザで out-of-sync メッセージを受信する可能性があります。
ステップ 24	**sticky** {*duration* [**group** *group-id*] [**netmask** *netmask*] | **asn msid** [**group** *group-id*] | **gtp imsi** [**group** *group-id*] | **radius calling-station-id** | **radius framed-ip** [**group** *group-id*] | **radius username** [**msid-cisco**] [**group** *group-id*]} 例： Router(config-slb-vserver) # **sticky 60 group 10**	（任意）クライアント接続の間隔が指定した期間を超えない限り、同じクライアントからの接続が同じ実サーバを使用するように指定します。 **（注）** VPN サーバ ロード バランシングの場合、15 秒以上の *duration* を指定します。 GPRS ロード バランシングおよび Home Agent Director は、このコマンドをサポートしません。
ステップ 25	**synguard** *syn-count interval* 例： Router(config-slb-vserver) # **synguard 50**	（任意）SYN フラッド サービス拒否攻撃を阻止するために、仮想サーバによって管理される TCP SYNchronize Sequence Number（SYN）のレートを指定します。 **（注）** GPRS ロード バランシングおよび Home Agent Director は、このコマンドをサポートしません。
ステップ 26	**inservice** [**standby** *group-name*] [**active**] 例： Router(config-slb-vserver) # **inservice**	仮想サーバを IOS SLB で使用できるようにします。

仮想サーバの確認方法

仮想サーバを確認するには、次の任意作業を実行します。

手順の概要

1. **show ip slb vservers**

手順の詳細

次の **show ip slb vservers** コマンドで、仮想サーバの PUBLIC_HTTP および RESTRICTED_HTTP の設定を確認します。

```
Router# show ip slb vservers

slb vserver      prot  virtual               state         conns
-------------------------------------------------------------------
PUBLIC_HTTP      TCP   10.0.0.1:80           OPERATIONAL     0
RESTRICTED_HTTP  TCP   10.0.0.2:80           OPERATIONAL     0
Router#
```

サーバ ファームの確認方法

サーバ ファームを確認するには、次の任意作業を実行します。

手順の概要

1. **show ip slb reals**
2. **show ip slb serverfarm**

手順の詳細

次の **show ip slb reals** コマンドは、サーバ ファームの PUBLIC と RESTRICTED のステータス、関連する実サーバ、およびそれらのステータスを表示します。

```
Router# show ip slb real

real                    farm name        weight   state          conns
-------------------------------------------------------------------------
10.1.1.1                 PUBLIC           8       OPERATIONAL      0
10.1.1.2                 PUBLIC           8       OPERATIONAL      0
10.1.1.3                 PUBLIC           8       OPERATIONAL      0
10.1.1.20                RESTRICTED       8       OPERATIONAL      0
10.1.1.21                RESTRICTED       8       OPERATIONAL      0
Router#
```

次の **show ip slb serverfarm** コマンドで、サーバ ファーム PUBLIC および RESTRICTED の設定およびステータスを表示します。

```
Router# show ip slb serverfarm

server farm      predictor    nat   reals   bind id
-------------------------------------------------
PUBLIC           ROUNDROBIN   none  3       0
RESTRICTED       ROUNDROBIN   none  2       0
Router#
```

クライアントの確認方法

クライアントを確認するには、次の任意作業を実行します。

手順の概要

1. **show ip slb conns**

手順の詳細

次の **show ip slb conns** コマンドで、制限されたクライアント アクセスおよびステータスを確認します。

```
Router# show ip slb conns

vserver         prot client               real                 state     nat
-------------------------------------------------------------------------------
RESTRICTED_HTTP TCP  10.4.4.0:80          10.1.1.20            CLOSING   none
Router#
```

次の **show ip slb conns** コマンドは、制限されたクライアント アクセス ステータスに関する詳細情報を表示します。

```
Router# show ip slb conns client 10.4.4.0 detail
VSTEST_UDP, client = 10.4.4.0:80
  state = CLOSING, real = 10.1.1.20, nat = none
  v_ip = 10.0.0.2:80, TCP, service = NONE
  client_syns = 0, sticky = FALSE, flows attached = 0
Router#
```

IOS SLB 接続の確認方法

IOS SLB 接続を確認するには、次の任意作業を実行します。

手順の概要

1. **show ip slb stats**

手順の詳細

IOS SLB 機能がインストールされ、正しく動作していることを確認するには、IOS SLB スイッチから実サーバを ping してから、クライアントから仮想サーバを ping します。

次の **show ip slb stats** コマンドは、IOS SLB ネットワーク ステータスに関する詳細情報を表示します。

```
Router# show ip slb stats

 Pkts via normal switching:  0
 Pkts via special switching: 6
 Pkts dropped:               0
 Connections Created:        1
 Connections Established:    1
 Connections Destroyed:      0
 Connections Reassigned:     0
 Zombie Count:               0
 Connections Reused:         0
```

- 通常のスイッチングは、IOS SLB パケットが通常の IOS スイッチング パス（CEF、ファースト スイッチング、およびプロセス レベル スイッチング）上で管理されているときに発生します。
- 特殊なスイッチングは、IOS SLB パケットがハードウェア支援スイッチング パス上で管理されているときに発生します。

IOS SLB ネットワークおよび接続の確認に使用されるその他のコマンドについては、「Cisco IOS SLB 機能のモニタ方法と保守方法」（P.116）を参照してください。

ファイアウォール ロード バランシングの設定方法

基本的な IOS SLB ファイアウォール ロード バランシング ネットワークを設定するには、次の作業を実行します。

IOS SLB ファイアウォール ロード バランシングでは、障害の検出と回復にプローブを使用します。ファイアウォール ファームの各実サーバにプローブを設定する必要があります。ping プローブが推奨されます。詳細については、「ping プローブの設定方法」（P.65）を参照してください。ファイアウォールで、ping プローブの転送を許可していない場合、代わりに HTTP プローブを使用します。詳細については、「HTTP プローブの設定方法」（P.63）を参照してください。ファイアウォール ファームの各ファイアウォールに、複数のプローブを設定できます。また、サポートされる種類（DNS、HTTP、TCP、または ping）のプローブを任意に組み合わせることができます。

サーバ ロード バランシングとファイアウォール ロード バランシングの両方を Cisco Catalyst 6500 スイッチ上で実行している場合は、グローバル コンフィギュレーション モードで **mls ip slb wildcard search rp** コマンドを使用して、PFC 上の TCAM の容量を超える可能性を低減します。詳細については、「ワイルドカード検索の設定方法」（P.112）を参照してください。

IOS SLB の消去率が高くなると、CPU に影響が及ぶ可能性があります。この問題が発生する場合、グローバル コンフィギュレーション モードで **no** 形式の **mls ip slb purge global** コマンドを使用し、TCP および UDP フロー パケットで消去スロットリングをディセーブルにします。詳細については、「MLS エントリのプロトコルレベル消去の設定方法」（P.113）を参照してください。

ここでは、次の IOS SLB ファイアウォール ロード バランシング設定作業について説明します。必須および任意の作業を示します。

- 「ファイアウォール ファームの設定方法」（P.54）（必須）
- 「ファイアウォール ファームの確認方法」（P.58）（任意）
- 「ファイアウォール接続の確認方法」（P.58）（任意）

ファイアウォール ファームの設定方法

ファイアウォール ファームを設定するには、次の必須作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip slb firewallfarm** *firewall-farm*
4. **real** *ip-address*
5. **probe** *probe*
6. **weight** *service*
7. **inservice**
8. **access** [**source** *source-ip netmask*] [**destination** *destination-ip netmask*]
9. **access** [**source** *source-ip netmask* | **destination** *destination-ip netmask* | **inbound** {*inbound-interface* | **datagram connection**} | **outbound** *outbound-interface*]
10. **predictor hash address** [**port**]
11. **purge connection**
12. **purge sticky**
13. **replicate casa** *listen-ip remote-ip port* [*interval*] [**password** [[*encrypt*] *secret-string* [*timeout*]]
14. **replicate interval** *interval*
15. **replicate slave**
16. **protocol tcp**
17. **delay** *duration*
18. **idle** *duration*
19. **maxconns** *maximum-number*
20. **sticky** *duration* [**netmask** *netmask*] [**source** | **destination**]
21. **protocol datagram**
22. **idle** *duration*
23. **maxconns** *maximum-number*
24. **sticky** *duration* [**netmask** *netmask*] [**source** | **destination**]
25. **inservice**

手順の詳細

	コマンド	目的
ステップ 1	**enable** 例： Router> **enable**	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： Router# **configure terminal**	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 3	**ip slb firewallfarm** *firewall-farm* 例： Router(config)# **ip slb firewallfarm FIRE1**	ファイアウォール ファームの定義を IOS SLB 設定に追加し、ファイアウォール ファーム 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	**real** *ip-address* 例： Router(config-slb-fw)# **real 10.1.1.1**	ファイアウォール ファームのメンバとして、ファイアウォールを IP アドレスで指定し、実サーバ コンフィギュレーション モードを開始します。
ステップ 5	**probe** *probe* 例： Router(config-slb-fw-real)# **probe FireProbe**	プローブをファイアウォールに関連付けます。
ステップ 6	**weight** *setting* 例： Router(config-slb-fw-real)# **weight 24**	（任意）ファイアウォールの作業負荷容量を指定します。ファイアウォール ファーム内の他のファイアウォールと相対的な値です。
ステップ 7	**inservice** 例： Router(config-slb-fw-real)# **inservice**	ファイアウォールをファイアウォール ファームと IOS SLB で使用できるようにします。
ステップ 8	**access** [**source** *source-ip netmask* | **destination** *destination-ip netmask* | **inbound** {*inbound-interface* | **datagram connection**} | **outbound** *outbound-interface*] 例： Router(config-slb-fw)# **access destination 10.1.6.0 255.255.255.0**	（任意）特定のフローをファイアウォール ファームにルーティングします。

	コマンド	目的
ステップ 9	**predictor hash address** [**port**] 例： Router(config-slb-fw)# **predictor hash address**	(任意) ファイアウォールを選択するときに、発信元および宛先の IP アドレスに加え、発信元および宛先の TCP またはユーザ データグラム プロトコル (UDP) のポート番号を使用するかどうかを指定します。
ステップ 10	**purge connection** 例： Router(config-slb-fw)# **purge connection**	(任意) IOS SLB ファイアウォール ロード バランシングで接続の消去要求を送信できるようにします。
ステップ 11	**purge sticky** 例： Router(config-slb-fw)# **purge sticky**	(任意) スティッキ タイマーが切れたときに、IOS SLB ファイアウォール ロード バランシングでスティッキ接続の消去要求を送信できるようにします。
ステップ 12	**replicate casa** *listen-ip remote-ip port* [*interval*] [**password** [*encrypt*] *secret-string* [*timeout*]] 例： Router(config-slb-fw)# **replicate casa 10.10.10.11 10.10.11.12 4231**	(任意) IOS SLB ファイアウォール ロード バランシング ディシジョン テーブルのバックアップ スイッチへのステートフル バックアップを設定します。 **(注)** Home Agent Director はこのコマンドをサポートしません。 **virtual** コマンドに **service gtp** キーワードを指定して、**sticky** コマンドに **gtp imsi** キーワードを指定しなかった場合は、**replicate casa** コマンドがサポートされません（これは、セッションが持続されず、何も複製されないためです)。
ステップ 13	**replicate interval** *interval* 例： Router(config-slb-fw)# **replicate interval 20**	(任意) IOS SLB ファイアウォール ファームの複製配信間隔を設定します。 **(注)** Home Agent Director はこのコマンドをサポートしません。 **virtual** コマンドに **service gtp** キーワードを指定して、**sticky** コマンドに **gtp imsi** キーワードを指定しなかった場合は、**replicate interval** コマンドがサポートされません（これは、セッションが持続されず、何も複製されないためです)。
ステップ 14	**replicate slave** 例： Router(config-slb-fw)# **replicate slave**	(任意) IOS SLB ファイアウォール ファームの冗長ルート プロセッサのステートフル バックアップをイネーブルにします。 **(注)** Home Agent Director はこのコマンドをサポートしません。 **virtual** コマンドに **service gtp** キーワードを指定して、**sticky** コマンドに **gtp imsi** キーワードを指定しなかった場合は、**replicate slave** コマンドがサポートされません（これは、セッションが持続されず、何も複製されないためです)。 **replicate slave** が設定された 1 つのスーパーバイザ エンジンを使用している場合は、そのスーパーバイザで out-of-sync メッセージを受信する可能性があります。
ステップ 15	**protocol tcp** 例： Router(config-slb-fw)# **protocol tcp**	(任意) ファイアウォール ファーム TCP プロトコル コンフィギュレーション モードを開始します。

	コマンド	目的
ステップ 16	**delay** *duration* 例： Router(config-slb-fw-tcp)# **delay 30**	(任意) ファイアウォール ファーム TCP プロトコル コンフィギュレーション モードで、接続の終了後に IOS SLB ファイアウォール ロード バランシングが TCP 接続コンテキストを維持する時間を指定します。
ステップ 17	**idle** *duration* 例： Router(config-slb-fw-tcp)# **idle 120**	(任意) ファイアウォール ファーム TCP プロトコル コンフィギュレーション モードで、パケット アクティビティが存在しない場合に、IOS SLB ファイアウォール ロード バランシングが接続コンテキストを維持する最短時間を指定します。
ステップ 18	**maxconns** *maximum-number* 例： Router(config-slb-fw-tcp)# **maxconns 1000**	(任意) ファイアウォール ファーム TCP プロトコル コンフィギュレーション モードで、ファイアウォール ファーム上で同時に使用可能なアクティブ TCP 接続の最大数を指定します。
ステップ 19	**sticky** *duration* [**netmask** *netmask*] [**source** | **destination**] 例： Router(config-slb-fw-tcp)# **sticky 60**	(任意) ファイアウォール ファーム TCP プロトコル コンフィギュレーション モードで、次のいずれかの条件が満たされた場合に、同じ IP アドレスからの接続に同じファイアウォールが使用されるように指定します。 • 同じ IP アドレスのペア間に接続が存在する間（送信元/宛先スティッキ）。 • 最後の接続が破棄された後の *duration* で定義される期間。
ステップ 20	**protocol datagram** 例： Router(config-slb-fw)# **protocol datagram**	(任意) ファイアウォール ファーム データグラム プロトコル コンフィギュレーション モードを開始します。
ステップ 21	**idle** *duration* 例： Router(config-slb-fw-udp)# **idle 120**	(任意) ファイアウォール ファーム データグラム プロトコル コンフィギュレーション モードで、パケット アクティビティが存在しない場合に、IOS SLB ファイアウォール ロード バランシングが接続コンテキストを維持する最短時間を指定します。
ステップ 22	**maxconns** *maximum-number* 例： Router(config-slb-fw-udp)# **maxconns 1000**	(任意) ファイアウォール ファーム データグラム プロトコル コンフィギュレーション モードで、ファイアウォール ファーム上で同時に使用可能なアクティブ データグラム接続の最大数を指定します。
ステップ 23	**sticky** *duration* [**netmask** *netmask*] [**source** | **destination**] 例： Router(config-slb-fw-udp)# **sticky 60**	(任意) ファイアウォール ファーム データグラム プロトコル コンフィギュレーション モードで、次のいずれかの条件が満たされた場合に、同じ IP アドレスからの接続に同じファイアウォールが使用されるように指定します。 • 同じ IP アドレスのペア間に接続が存在する間（送信元/宛先スティッキ）。 • 最後の接続が破棄された後の *duration* で定義される期間。
ステップ 24	**inservice** 例： Router(config-slb-fw)# **inservice**	ファイアウォール ファームを IOS SLB で使用できるようにします。

ファイアウォール ファームの確認方法

ファイウォール ファームを確認するには、次の任意作業を実行します。

手順の概要

1. **show ip slb real**
2. **show ip slb firewallfarm**

手順の詳細

次の **show ip slb reals** コマンドは、ファイアウォール ファーム FIRE1 のステータス、関連する実サーバ、およびそれらのステータスを表示します。

```
Router# show ip slb real

real                  farm name        weight   state          conns
-------------------------------------------------------------------
10.1.1.2              FIRE1            8        OPERATIONAL    0
10.1.2.2              FIRE1            8        OPERATIONAL    0
```

次の **show ip slb firewallfarm** コマンドは、ファイアウォール ファーム FIRE1 の設定とステータスを表示します。

```
Router# show ip slb firewallfarm

firewall farm    hash        state         reals
-------------------------------------------------
FIRE1            IPADDR      INSERVICE     2
```

ファイアウォール接続の確認方法

ファイアウォール接続を確認するには、次の任意作業を実行します。

手順の概要

1. 外部実サーバに ping を送信します。
2. 内部実サーバに ping を送信します。
3. **show ip slb stats**
4. **show ip slb real detail**
5. **show ip slb conns**

手順の詳細

IOS SLB ファイアウォール ロード バランシングが設定され、正しく動作していることを確認するには、次の手順を実行します。

ステップ 1 IOS SLB ファイアウォール ロード バランシング スイッチから外部実サーバ（ファイアウォールの外側にあるサーバ）に ping を送信します。

ステップ 2 クライアントから内部実サーバ（ファイアウォールの内側にあるサーバ）に ping を送信します。

ステップ 3 **show ip slb stats** コマンドを使用して、IOS SLB ファイアウォール ロード バランシングのネットワーク ステータスに関する情報を表示します。

```
Router# show ip slb stats

 Pkts via normal switching:  0
 Pkts via special switching: 0
 Pkts dropped:               0
 Connections Created:        1911871
 Connections Established:    1967754
 Connections Destroyed:      1313251
 Connections Reassigned:     0
 Zombie Count:               0
 Connections Reused:         59752
 Connection Flowcache Purges:1776582
 Failed Connection Allocs:   17945
 Failed Real Assignments:    0
```

- 通常のスイッチングは、IOS SLB パケットが通常の IOS スイッチング パス（CEF、ファースト スイッチング、およびプロセス レベル スイッチング）上で管理されているときに発生します。
- 特殊なスイッチングは、IOS SLB パケットがハードウェア支援スイッチング パス上で管理されているときに発生します。

ステップ 4 **show ip slb real detail** コマンドを使用して、IOS SLB ファイアウォール ロード バランシングの実サーバ ステータスに関する情報を表示します。

```
Router# show ip slb reals detail

172.16.88.5, SF1, state = OPERATIONAL, type = server
  ipv6 = 2342:2342:2343:FF04:2388:BB03:3223:8912
  conns = 0, dummy_conns = 0, maxconns = 4294967295
  weight = 8, weight(admin) = 8, metric = 0, remainder = 0
  reassign = 3, retry = 60
  failconn threshold = 8, failconn count = 0
  failclient threshold = 2, failclient count = 0
  total conns established = 0, total conn failures = 0
  server failures = 0
```

ステップ 5 **show ip slb conns** コマンドを使用して、アクティブな IOS SLB ファイアウォール ロード バランシング接続に関する情報を表示します。

```
Router# show ip slb conns

vserver         prot client               real                 state     nat
-------------------------------------------------------------------------------
FirewallTCP     TCP  80.80.50.187:40000   10.1.1.4             ESTAB     none
FirewallTCP     TCP  80.80.50.187:40000   10.1.1.4             ESTAB     none
FirewallTCP     TCP  80.80.50.187:40000   10.1.1.4             ESTAB     none
FirewallTCP     TCP  80.80.50.187:40000   10.1.1.4             ESTAB     none
FirewallTCP     TCP  80.80.50.187:40000   10.1.1.4             ESTAB     none
```

IOS SLB ネットワークおよび接続の確認に使用されるその他のコマンドについては、「Cisco IOS SLB 機能のモニタ方法と保守方法」（P.116）を参照してください。

プローブの設定方法

ここでは、プローブを設定および確認する方法について説明します。デフォルトで、IOS SLB に設定されているプローブはありません。

IOS SLB で接続を確認し、障害を検出するには、プローブが使用されます。プローブの各種類の詳細については、「プローブ」（P.27）を参照してください。

プローブを設定するには、次の作業を実行します。必須および任意の作業を示します。

- 「カスタム UDP プローブの設定方法」（P.60）（必須）
- 「DNS プローブの設定方法」（P.62）（必須）
- 「HTTP プローブの設定方法」（P.63）（必須）
- 「ping プローブの設定方法」（P.65）（必須）
- 「TCP プローブの設定方法」（P.66）（必須）
- 「WSP プローブの設定方法」（P.67）（必須）
- 「プローブの関連付け方法」（P.68）（必須）
- 「プローブの確認方法」（P.69）（任意）

カスタム UDP プローブの設定方法

カスタム UDP プローブを設定するには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip slb probe** *probe* **custom udp**
4. **address** [*ip-address*] [**routed**]
5. **faildetect** *number-of-probes*
6. **interval** *seconds*
7. **port** *port*
8. **request data** {*start-byte* | **continue**} *hex-data-string*
9. **response** *clause-number* **data** *start-byte hex-data-string*
10. **timeout** *seconds*

手順の詳細

	コマンド	説明
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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。

	コマンド	説明
ステップ 3	**ip slb probe** *probe* **custom udp** 例： `Router(config)# ip slb probe PROBE6 custom udp`	IOS SLB プローブ名を設定し、カスタム UDP プローブ 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	**address** [*ip-address*] [**routed**] 例： `Router(config-slb-probe)# address 10.1.1.1`	（任意）カスタム UDP プローブの送信先 IP アドレスを設定します。
ステップ 5	**faildetect** *number-of-probes* 例： `Router(config-slb-probe)# faildetect 16`	（任意）実サーバの障害の原因となる連続無応答カスタム UDP プローブの数を指定します。
ステップ 6	**interval** *seconds* 例： `Router(config-slb-probe)# interval 11`	（任意）カスタム UDP プローブ送信タイマーを設定します。
ステップ 7	**port** *port* 例： `Router(config-slb-probe)# port 8`	カスタム UDP プローブを接続するポートを設定します。
ステップ 8	**request data** {*start-byte* | **continue**} *hex-data-string* 例： `Router(config-slb-probe)# request data 0 05 04 00 77 18 2A D6 CD 0A AD 53 4D F1 29 29 CF C1 96 59 CB`	カスタム UDP プローブから送信される UDP 要求パケットのペイロードを定義します。
ステップ 9	**response** *clause-number* **data** *start-byte hex-data-string* 例： `Router(config-slb-probe)# response 2 data 44 DD DD`	カスタム UDP プローブ応答パケットに照らして一致するデータ文字列を定義します。
ステップ 10	**timeout** *seconds* 例： `Router(config-slb-probe)# timeout 20`	（任意）カスタム UDP プローブのタイムアウトを設定します。

DNS プローブの設定方法

DNS プローブを設定するには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip slb probe** *probe* **dns**
4. **address** [*ip-address* [**routed**]]
5. **faildetect** *number-of-probes*
6. **interval** *seconds*
7. **lookup** *ip-address*

手順の詳細

	コマンド	説明
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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 3	**ip slb probe** *probe* **dns** 例： `Router(config)# ip slb probe PROBE4 dns`	IOS SLB プローブ名を設定し、DNS プローブ 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	**address** [*ip-address* [**routed**]] 例： `Router(config-slb-probe)# address 10.1.10.1`	（任意）DNS プローブを送信する IP アドレスを設定します。
ステップ 5	**faildetect** *number-of-probes* 例： `Router(config-slb-probe)# faildetect 16`	（任意）実サーバまたはファイアウォールの障害の原因となる連続無応答 DNS プローブの数を指定します。
ステップ 6	**interval** *seconds* 例： `Router(config-slb-probe)# interval 11`	（任意）DNS プローブ送信タイマーを設定します。
ステップ 7	**lookup** *ip-address* 例： `Router(config-slb-probe)# lookup 10.1.10.1`	（任意）DNS サーバがドメイン ネーム解決要求に対する応答で返す必要がある実サーバの IP アドレスを設定します。

HTTP プローブの設定方法

HTTP プローブを設定するには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip slb probe** *probe* **http**
4. **address** [*ip-address* [**routed**]]
5. **credentials** {*username* [*password*]}
6. **expect** [**status** *status-code*] [**regex** *expression*]
7. **header** *field-name* [*field-value*]
8. **interval** *seconds*
9. **port** *port*
10. **request** [**method** {**get** | **post** | **head** | **name** *name*}] [**url** *path*]
11. 仮想サーバへのルートを設定します。

手順の詳細

	コマンド	説明
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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 3	**ip slb probe** *probe* **http** 例： `Router(config)# ip slb probe PROBE2 http`	IOS SLB プローブ名を設定し、HTTP プローブ 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	**address** [*ip-address* [**routed**]] 例： `Router(config-slb-probe)# address 10.1.10.1`	（任意）HTTP プローブの送信先 IP アドレスを設定します。
ステップ 5	**credentials** {*username* [*password*]} 例： `Router(config-slb-probe)# credentials Username1 password`	（任意）HTTP プローブのヘッダー値を設定します。

	コマンド	説明
ステップ 6	**expect** [**status** *status-code*] [**regex** *expression*] 例： `Router(config-slb-probe)# expect status 401 regex Copyright`	（任意）予想される HTTP ステータス コードまたは正規表現を設定します。
ステップ 7	**header** *field-name* [*field-value*] 例： `Router(config-slb-probe)# header HeaderName HeaderValue`	（任意）HTTP プローブのヘッダー値を設定します。
ステップ 8	**interval** *seconds* 例： `Router(config-slb-probe)# interval 11`	（任意）HTTP プローブの送信タイマーを設定します。
ステップ 9	**port** *port* 例： `Router(config-slb-probe)# port 8`	（任意）HTTP プローブが接続するポートを設定します。
ステップ 10	**request** [**method** {**get** | **post** | **head** | **name** *name*}] [**url** *path*] 例： `Router(config-slb-probe)# request method post url /probe.cgi?all`	（任意）サーバからの要求への URL パス、およびサーバへの要求に使用するメソッドを設定します。
ステップ 11	仮想サーバへのルートを設定します。	HTTP プローブには、仮想サーバへのルートが必要です。このルートは使用されませんが、宛先が到達可能かどうかをソケット コードで確認するために必要です。そのため、HTTP プローブが正しく機能するために不可欠です。ルートは次のいずれかにすることができます。 • ホスト ルート：仮想サーバによってアドバタイズされます。 • デフォルト ルート：**ip route 0.0.0.0 0.0.0.0** コマンドなどを使用して指定します。

ping プローブの設定方法

ping プローブを設定するには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip slb probe** *probe* **ping**
4. **address** [*ip-address* [**routed**]]
5. **faildetect** *number-of-pings*
6. **interval** *seconds*

手順の詳細

	コマンド	説明
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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 3	**ip slb probe** *probe* **ping** 例： `Router(config)# ip slb probe PROBE1 ping`	IOS SLB プローブ名を設定し、ping プローブ 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	**address** [*ip-address* [**routed**]] 例： `Router(config-slb-probe)# address 10.1.10.1`	（任意）ping プローブの送信先 IP アドレスを設定します。
ステップ 5	**faildetect** *number-of-pings* 例： `Router(config-slb-probe)# faildetect 16`	（任意）連続して ACK が受信されない ping プローブの数を指定します。この数を超えると、実サーバまたはファイアウォールの障害と見なされます。
ステップ 6	**interval** *seconds* 例： `Router(config-slb-probe)# interval 11`	（任意）ping プローブの送信タイマーを設定します。

TCP プローブの設定方法

TCP プローブを設定するには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip slb probe** *probe* **tcp**
4. **address** [*ip-address* [**routed**]]
5. **interval** *seconds*
6. **port** *port*

手順の詳細

	コマンド	説明
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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 3	**ip slb probe** *probe* **tcp** 例： `Router(config)# ip slb probe PROBE5 tcp`	IOS SLB プローブ名を設定し、TCP プローブ 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	**address** [*ip-address* [**routed**]] 例： `Router(config-slb-probe)# address 10.1.10.1`	（任意）TCP プローブの送信先 IP アドレスを設定します。
ステップ 5	**interval** *seconds* 例： `Router(config-slb-probe)# interval 5`	（任意）TCP プローブの送信タイマーを設定します。
ステップ 6	**port** *port* 例： `Router(config-slb-probe)# port 8`	TCP プローブが接続するポートを設定します。

WSP プローブの設定方法

Wireless Session Protocol（WSP）プローブを設定するには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip slb probe** *probe* **wsp**
4. **address** [*ip-address* [**routed**]]
5. **interval** *seconds*
6. **url** [*path*]

手順の詳細

	コマンド	説明
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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 3	**ip slb probe** *probe* **wsp** 例： `Router(config)# ip slb probe PROBE3 wsp`	IOS SLB プローブ名を設定し、WSP プローブ 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	**address** [*ip-address* [**routed**]] 例： `Router(config-slb-probe)# address 10.1.10.1`	（任意）WSP プローブの送信先 IP アドレスを設定します。
ステップ 5	**interval** *seconds* 例： `Router(config-slb-probe)# interval 11`	（任意）WSP プローブ送信タイマーを設定します。
ステップ 6	**url** [*path*] 例： `Router(config-slb-probe)# url http://localhost/test.txt`	（任意）WSP プローブ URL パスを設定します。

プローブの関連付け方法

プローブを実サーバまたはファイアウォールに関連付けるには、次の作業を実行します。

プローブの設定後に、**probe** コマンドを使用して、実サーバまたはファイアウォールとプローブを関連付ける必要があります。詳細については、「サーバ ファームと実サーバの設定方法」（P.41）および「ファイアウォール ロード バランシングの設定方法」（P.53）を参照してください。

（注） WSP プローブをファイアウォールに関連付けることはできません。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip slb firewallfarm** *firewall-farm*

   または

   ip slb serverfarm *server-farm*
4. **probe** *probe*

手順の詳細

	コマンド	説明
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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 3	**ip slb firewallfarm** *firewall-farm* または **ip slb serverfarm** *server-farm* 例： `Router(config)# ip slb serverfarm PUBLIC` または `Router(config)# ip slb firewallfarm FIRE1`	ファイアウォール ファームを指定し、ファイアウォール ファーム コンフィギュレーション モードを開始します。 または サーバ ファームを指定し、SLB サーバ ファーム 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	**probe** *probe* 例： `Router(config-slb-sfarm)# probe PROBE1` または `Router(config-slb-fw-real)# probe FireProbe`	プローブをファイアウォール ファームまたはサーバ ファームに関連付けます。

プローブの確認方法

プローブを確認するには、次の任意作業を実行します。

概要手順

1. **show ip slb probe**

詳細手順

プローブが適切に設定されていることを確認するには、**show ip slb probe** コマンドを使用します。

```
Router# show ip slb probe

Server:Port             State        Outages  Current  Cumulative
-------------------------------------------------------------------
10.1.1.1:80             OPERATIONAL        0  never    00:00:00
10.1.1.2:80             OPERATIONAL        0  never    00:00:00
10.1.1.3:80             OPERATIONAL        0  never    00:00:00
```

DFP の設定方法

IOS SLB を Dynamic Feedback Protocol（DFP）マネージャとして設定し、IOS SLB が接続を開始可能な DFP エージェントを特定するには、次の作業を実行します。

IOS SLB には、DFP マネージャ、別の DFP マネージャ用の DFP エージェント、または同時に両方の役割を定義できます。ネットワーク設定によっては、IOS SLB を DFP マネージャとして設定するためにコマンドを入力し、同じデバイスまたは別のデバイス上で IOS SLB を DFP エージェントとして設定するためにコマンドを入力します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip slb dfp** [**password** [[*encrypt*] *secret-string* [*timeout*]]
4. **agent** *ip-address port* [*timeout* [*retry-count* [*retry-interval*]]]
5. IOS SLB を DFP エージェントとして設定します。

手順の詳細

	コマンド	説明
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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 3	**ip slb dfp** [**password** [[*encrypt*] *secret-string* [*timeout*]] 例： `Router(config)# ip slb dfp password Password1 360`	Dynamic Feedback Protocol（DFP）を設定し、オプションのパスワードを指定し、DFP 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	**agent** *ip-address port* [*timeout* [*retry-count* [*retry-interval*]]] 例： `Router(config-slb-dfp)# agent 10.1.1.1 2221 30 0 10`	IOS SLB が接続可能な DFP エージェントを特定します。
ステップ 5	IOS SLB を DFP エージェントとして設定します。	IOS SLB を DFP エージェントとして設定するには、Cisco IOS Release 12.2(18)SXB の *DFP Agent Subsystem* 機能のマニュアルを参照してください。

GPRS ロード バランシングの設定作業リスト

General Packet Radio Service（GPRS）ロード バランシングを設定するには、次の作業を実行します。

手順の概要

1. サーバ ファームおよび実サーバを設定します。
2. 仮想サーバを設定します。
3. サーバ内の各ゲートウェイ GPRS サポート ノード（GGSN）でループバックとして仮想 IP アドレスを設定します。
4. 各 GGSN を、それぞれに関連付けられた SGSN にルーティングします。
5. 各 SGSN を、それぞれに関連付けられた Cisco GGSN 上の仮想テンプレート、および GPRS ロード バランシング仮想サーバにルーティングします。
6. GSN アイドル タイマーを設定します。

手順の詳細

	コマンド	説明
ステップ 1	サーバ ファームおよび実サーバを設定します。	「サーバ ファームと実サーバの設定方法」（P.41）を参照してください。 GPRS ロード バランシングのサーバ ファームおよび実サーバを設定する場合、次の注意事項を考慮してください。 • GTP Cause Code Inspection の状態： – イネーブルになっていない場合：**predictor** コマンドのデフォルト設定（加重ラウンド ロビン アルゴリズム）を受け入れます。 – イネーブルになっている場合：加重ラウンド ロビン（**roundrobin**）アルゴリズムと加重最小接続（**leastconns**）アルゴリズムのどちらかを指定します。 • **real** コマンドを使用して、GGSN 機能を実行している実サーバの IP アドレス（Cisco GGSN の場合は仮想テンプレート アドレス）を指定します。 • **reassign** コマンドを使用して、SGSN の N3-REQUESTS カウンタ値未満の再割り当てしきい値を指定します。 • GTP ロード バランシングに対するデュアルスタック サポートをイネーブルにするには： – **real** コマンドを使用して、実サーバの IPv6 アドレスを指定します。
ステップ 2	仮想サーバを設定します。	「仮想サーバの設定方法」（P.45）を参照してください。 **virtual** コマンドを設定する場合、次の注意事項を考慮してください。 • 仮想 GGSN IP アドレスを仮想サーバとして指定し、**udp** キーワード オプションを指定します。 • GTP v1 および GTP v2 セッションの負荷を分散するには、GGSN および SGSN が ETSI 標準に準拠している場合、ポート番号 2123 を指定します。また、全ポート仮想サーバ（つまり、すべてのポート宛てのフローを受け入れる仮想サーバ）を設定するには、ポート番号 0 または **any** を指定します。 • GTP v0 セッションの負荷を分散するには、GGSN および SGSN が ETSI 標準に準拠している場合、ポート番号 3386 を指定します。また、全ポート仮想サーバを設定するには、ポート番号 0 または **any** を指定します。 • GPRS ロード バランシングをイネーブルにするには： – GTP Cause Code Inspection を*使用しない*場合：**service gtp** キーワード オプションを指定します。 GTP Cause Code Inspection をイネーブルに*しない* GPRS ロード バランシングの場合、**idle** コマンドを使用して idle タイマーを設定するときは、SGSN 上の PDP コンテキスト要求間で可能な最も長い間隔よりも、長いアイドル タイマーを指定します。 – GTP Cause Code Inspection を*使用する*場合：**service gtp-inspect** キーワード オプションを指定します。 • GTP ロード バランシングに対するデュアルスタック サポートをイネーブルにするには： – **virtual** コマンドを使用して、仮想サーバの IPv6 アドレスとオプションの IPv6 プレフィクスを指定します。 – **serverfarm** コマンドを使用して、プライマリ IPv6 サーバ ファームとオプションのバックアップ IPv6 サーバ ファームを仮想サーバに関連付けます。 – 設定から **client** コマンドを削除します。

	コマンド	説明
ステップ 3	サーバの各 GGSN でループバックとして仮想 IP アドレスを設定します。	（dispatched モードの場合に必須）この手順が必須なのは、GTP Cause Code Inspection をイネーブルにしないで dispatched モードを使用する場合だけです。詳細については、『*Cisco IOS Interface Configuration Guide*』の「Configuring Virtual Interfaces」を参照してください。
ステップ 4	各 GGSN を、それぞれに関連付けられた SGSN にルーティングします。	スタティック ルートまたはダイナミック ルートを使用できますが、GGSN は SGSN に到達可能な必要があります。詳細については、『*Cisco IOS Mobile Wireless Configuration Guide*』の「Configuring Network Access to the GGSN」を参照してください。
ステップ 5	各 SGSN を、それぞれに関連付けられた Cisco GGSN 上の仮想テンプレート、および GPRS ロード バランシング仮想サーバにルーティングします。	（必須）詳細については、SGSN の設定ガイドを参照してください。
ステップ 6	GSN アイドル タイマーを設定します。	（任意）この手順を適用できるのは、GTP Cause Code Inspection がイネーブルの場合だけです。 詳細については、「GSN アイドル タイマーの設定方法」（P.73）を参照してください。

GSN アイドル タイマーの設定方法

GPRS Support Node（GSN）アイドル タイマーを設定するには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip slb timers gtp gsn** *duration*

手順の詳細

	コマンド	説明
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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 3	**ip slb timers gtp gsn** *duration* 例： `Router(config)# ip slb timers gtp gsn 45`	IOS SLB が、アイドルのゲートウェイ GPRS サポート ノード（GGSN）、または動作中の GPRS サポート ノード（SGSN）との間でやりとりするセッションを維持する時間を変更します。

GGSN-IOS SLB メッセージング作業リスト

GGSN-IOS SLB メッセージングを設定するには、次の作業を実行します。

手順の概要

1. GGSN-IOS SLB メッセージングをサポートするように GGSN を設定します。
2. サーバ ファームおよび実サーバを設定します。
3. 仮想サーバを設定します。

手順の詳細

	タスク	説明
ステップ 1	GGSN-IOS SLB メッセージングをサポートするように GGSN を設定します。	GGSN-IOS SLB メッセージング サポートを設定する場合、同じ GGSN を共有するすべての IOS SLB 仮想サーバを、同じ NAT モード（dispatched モードまたは directed モード）を使用するように設定します。このとき、**gprs slb mode** コマンドを使用します。1 つの GGSN につき 1 つの NAT モードしか設定できないため、仮想サーバは dispatched モードと directed モードを混在して使用できません。 詳細については、Cisco IOS Release 12.3(2)XU 以降の GGSN Release 5.0 に関する『*Cisco IOS Mobile Wireless Configuration Guide*』を参照してください。
ステップ 2	サーバ ファームおよび実サーバを設定します。	「サーバ ファームと実サーバの設定方法」（P.41）を参照してください。 サーバ ファームと実サーバを GGSN-IOS SLB メッセージング用に設定する場合は、セッションを新しい実サーバに再割り当てするときに、IOS SLB が現在の実サーバを停止させないように、**no faildetect inband** コマンドを指定して、自動サーバ障害検出をディセーブルにします。
ステップ 3	仮想サーバを設定します。	「仮想サーバの設定方法」（P.45）を参照してください。 仮想サーバを GGSN-IOS SLB メッセージング用に設定する場合は、**gtp notification cac** コマンドを指定して、IOS SLB が新しい実サーバにセッションを再割り当て可能な回数を制限します。

GPRS ロード バランシング マップの設定方法

GPRS ロード バランシング マップを設定するには、次の作業を実行します。

GPRS ロード バランシング マップによって、IOS SLB は Access Point Name（APN）に基づいてユーザ トラフィックを分類し、ルーティングできます。GPRS ロード バランシング マップをイネーブルにするには、GPRS トンネリング プロトコル（GTP）マップを定義してから、そのマップをサーバ ファームに関連付ける必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip slb map** *map-id* **gtp** | **radius**}
4. **apn** *string*
5. **exit**
6. **ip slb vserver** *virtual-server*
7. **virtual** *ipv4-address* [*ipv4-netmask* [**group**]] [**ipv6** *ipv6-address* [**prefix** *ipv6-prefix*]] {**tcp** | **udp**} [*port* | **any**] [**service** *service*]
8. **serverfarm** *primary-farm* [**backup** *backup-farm* [**sticky**]] [**ipv6-primary** *ipv6-primary-farm* [**ipv6-backup** *ipv6-backup-farm*]] [**map** *map-id* **priority** *priority*]

手順の詳細

	コマンド	説明
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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 3	**ip slb map** *map-id* **gtp** | **radius**} 例： `Router(config)# ip slb map 1 radius`	IOS SLB GTP マップを設定し、SLB GTP マップ 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	**apn** *string* 例： `Router(config-slb-map-gtp) # apn abc`	グローバル パケット ラジオ サービス（GPRS）ロード バランシングのアクセス ポイント ネーム（APN）とマッチングする ASCII 正規表現ストリングを設定します。

ステップ 5	**exit** 例： `Router(config-slb-map-gtp) # exit`	SLB GTP マップ コンフィギュレーション モードを終了します。
ステップ 6	**ip slb vserver** *virtual-server* 例： `Router(config)# ip slb vserver GGSN_SERVER`	仮想サーバを指定し、仮想サーバ コンフィギュレーション モードを開始します。
ステップ 7	**virtual** *ipv4-address* [*ipv4-netmask* [**group**]] [**ipv6** *ipv6-address* [**prefix** *ipv6-prefix*]] {**tcp** | **udp**} [*port* | **any**] [**service** *service*] 例： `Router(config-slb-vserver) # virtual 10.10.10.10 udp 0 service gtp`	仮想サーバの IP アドレス、接続の種類、およびオプションの TCP またはユーザ データグラム プロトコル（UDP）のポート番号を指定し、Internet Key Exchange（IKE; インターネット キー エクスチェンジ）または Wireless Session Protocol（WSP）の設定、およびサービスのカップリングを指定します。 **（注）** GPRS ロード バランシングの場合： – 仮想 GGSN IP アドレスを仮想サーバとして指定し、**udp** キーワード オプションを指定します。 – GTP v1 および GTP v2 セッションの負荷を分散するには、GGSN および SGSN が ETSI 標準に準拠している場合、ポート番号 2123 を指定します。また、全ポート仮想サーバ（つまり、すべてのポート宛てのフローを受け入れる仮想サーバ）を設定するには、ポート番号 0 または **any** を指定します。 – GTP v0 セッションの負荷を分散するには、GGSN および SGSN が ETSI 標準に準拠している場合、ポート番号 3386 を指定します。また、全ポート仮想サーバを設定するには、ポート番号 0 または **any** を指定します。 – GTP Cause Code Inspection *なし*の GPRS ロード バランシングをイネーブルにするには、**service gtp** キーワード オプションを指定します。 – GTP Cause Code Inspection *あり*の GPRS ロード バランシングをイネーブルにするには、**service gtp-inspect** キーワード オプションを指定します。 – GTP ロード バランシングに対するデュアルスタック サポートの場合は、仮想サーバの IPv4 アドレス、IPv6 アドレス、およびオプションの IPv6 プレフィクスを指定します。
ステップ 8	**serverfarm** *primary-farm* [**backup** *backup-farm* [**sticky**]] [**ipv6-primary** *ipv6-primary-farm* [**ipv6-backup** *ipv6-backup-farm*]] [**map** *map-id* **priority** *priority*] 例： `Router(config-slb-vserver) # serverfarm farm1 backup farm2 map 1 priority 3`	GTP マップをサーバ ファームに関連付けます。実サーバ ファームを仮想サーバに関連付け、オプションで、バックアップ サーバ ファームを設定し、バックアップ サーバ ファームでスティッキ接続を使用することを指定します。 **（注）** GPRS ロード バランシングで、複数のサーバ ファームに 1 つの実サーバが定義されている場合、各サーバ ファームは異なる仮想サーバに関連付ける必要があります。 複数のサーバ ファームを特定の仮想サーバに関連付けるには、複数の **serverfarm** コマンドのそれぞれを一意のマップ ID とプライオリティで設定します（つまり、各マップ ID および各マップ プライオリティは、仮想サーバに関連付けられているすべてのサーバ ファームで固有にする必要があります）。 GTP マップを使用しており、複数のサーバ ファームで 1 つの実サーバを設定している場合は、別の仮想サーバを各サーバ ファームに関連付ける必要があります。

KAL-AP エージェント サポートの設定方法

KAL-AP エージェント サポートを設定するには、次の作業を実行します。

KAL-AP エージェントのサポートによって、IOS SLB は Global Server Load Balancing（GSLB; グローバル サーバ ロード バランシング）環境でロード バランシングを実行できます。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip slb capp udp**
4. **peer** [*ip-address*] **port** *port*
5. **peer** [*ip-address*] **secret** [*encrypt*] *secret-string*
6. **exit**
7. **ip slb serverfarm** *server-farm*
8. **kal-ap domain** *tag*
9. **farm-weight** *setting*

手順の詳細

	コマンド	説明
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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 3	**ip slb capp udp** 例： `Router(config)# ip slb capp udp`	KAL-AP エージェントをイネーブルにし、SLB Content Application Peering Protocol（CAPP）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	**peer** [*ip-address*] **port** *port* 例： `Router(config-slb-capp)# peer port 6000`	（任意）KAL-AP エージェントが接続するポートを指定します。
ステップ 5	**peer** [*ip-address*] **secret** [*encrypt*] *secret-string* 例： `Router(config-slb-capp)# peer secret SECRET_STRING`	（任意）KAL-AP エージェントのために Message Digest Algorithm Version 5（MD5）認証をイネーブルにします。
ステップ 6	**exit** 例： `Router(config-slb-map-gtp)# exit`	SLB CAPP コンフィギュレーション モードを終了します。
ステップ 7	**ip slb serverfarm** *server-farm* 例： `Router(config)# ip slb serverfarm PUBLIC`	サーバ ファームを指定し、SLB サーバ ファーム コンフィギュレーション モードを開始します。
ステップ 8	**kal-ap domain** *tag* 例： `Router(config-slb-sfarm)# kal-ap domain chicago-com`	（任意）KAL-AP エージェントが仮想サーバの負荷をレポートするとき、ドメイン タグを確認できるようにします。
ステップ 9	**farm-weight** *setting* 例： `Router(config-slb-sfarm)# farm-weight 16`	（任意）サーバ ファームの負荷値を算出するときに、KAL-AP エージェントが使用する加重を指定します。

RADIUS ロード バランシングの設定作業リスト

RADIUS ロード バランシングを設定するには、次の作業を実行します。

手順の概要

1. サーバ ファームおよび実サーバを設定します。
2. 仮想サーバを設定します。
3. IOS SLB で RADIUS framed-IP スティッキ ルーティング用のパケットを検査できるようにします。
4. RADIUS ロード バランシング マップを設定します。
5. RADIUS ロード バランシング加速データ プレーン フォワーディングを設定します。
6. 使用できるマルチレイヤ スイッチング（MLS）エントリの数を増やします。
7. プローブを設定します。

手順の詳細

	タスク	説明
ステップ 1	サーバ ファームおよび実サーバを設定します。	「サーバ ファームと実サーバの設定方法」（P.41）を参照してください。 RADIUS ロード バランシングのサーバ ファームおよび実サーバを設定する場合、次の注意事項を考慮してください。 • **predictor** コマンドのデフォルト設定（加重ラウンド ロビン アルゴリズム）を受け入れます。 • （任意）セッションベースの障害検出をイネーブルにするには、**faildetect numconns** コマンドの **numclients** キーワードに値 1 を指定します。 • （任意）個々の仮想サーバに割り当てることができる、IOS SLB RADIUS および GTP スティッキ加入者の最大数を指定するには、**maxclients** コマンドを使用します。
ステップ 2	仮想サーバを設定します。	「仮想サーバの設定方法」（P.45）を参照してください。 RADIUS ロード バランシングの仮想サーバを設定する場合、次の注意事項を考慮してください。 • **virtual** コマンドを使用して、**service radius** キーワード オプションを指定します。 • （任意）入力インターフェイスを検査するために framed-IP ルーティングをイネーブルにするには、**access** *interface* **route framed-ip** コマンドを指定します。 **access** *interface* **route framed-ip** コマンドを設定する場合、さらに **service radius** キーワードを指定した **virtual** コマンドを設定する必要があります。 • （任意）外部エージェントのハンドオフ時に、IOS SLB が新しい Mobile IP 外部エージェントからの ACCT-START メッセージを待機する時間を変更するには、**hand-off radius** コマンドを設定します。 • （任意）IOS SLB セッション データベースで RADIUS エントリの時間を設定するには、**radius request** キーワードを指定した **idle** コマンドを設定します。 • （任意）IOS SLB RADIUS framed-IP スティッキ データベースでエントリの時間を設定するには、**radius framed-ip** キーワードを指定した **idle** コマンドを設定します。

タスク	説明
仮想サーバを設定します。（続き）	• （任意）IOS SLB で IOS SLB RADIUS framed-IP スティッキ データベースを作成し、特定の加入者からの RADIUS 要求と非 RADIUS フローを同じサービス ゲートウェイに転送できるようにするには、**sticky** コマンドで **radius framed-ip** キーワードを指定します。 **sticky radius** framed-ip コマンドを設定する場合、さらに **service radius** キーワードを指定した **virtual** コマンドを設定する必要があります。 • （任意）Accounting ON または OFF メッセージの受信時に、IOS SLB で IOS SLB RADIUS framed-IP スティッキ データベース内のエントリを消去できるようにするには、**purge radius framed-ip acct on-off** 仮想サーバ コンフィギュレーション コマンドを指定します。 Accounting ON または OFF メッセージの受信時に、IOS SLB で IOS SLB RADIUS framed-IP スティッキ データベース内のエントリを消去できないようにするには、**no purge radius framed-ip acct on-off** 仮想サーバ コンフィギュレーション コマンドを指定します。 • （任意）Accounting-Stop メッセージの受信時に、IOS SLB で IOS SLB RADIUS framed-IP スティッキ データベース内のエントリを消去できるようにするには、**purge radius framed-ip acct stop** 仮想サーバ コンフィギュレーション コマンドを指定します。 Accounting-Stop メッセージの受信時に、IOS SLB で IOS SLB RADIUS framed-IP スティッキ データベース内のエントリを消去できないようにするには、**no purge radius framed-ip acct stop** 仮想サーバ コンフィギュレーション コマンドを指定します。 • （任意：CDMA2000 ネットワーク専用）IOS SLB で IOS SLB RADIUS calling-station-ID スティッキ データベースを作成し、発信ステーション ID に基づいて、特定の加入者からの RADIUS 要求を同じサービス ゲートウェイに転送できるようにするには、**sticky** コマンドで **radius calling-station-id** キーワードを指定します。 IOS SLB で IOS SLB RADIUS username スティッキ データベースを作成し、ユーザ名に基づいて、特定の加入者からの RADIUS 要求を同じサービス ゲートウェイに転送できるようにするには、**sticky** コマンドで **radius username** キーワードを指定します。 **sticky radius calling-station-id** コマンドまたは **sticky radius username** コマンドを設定する場合、さらに **service radius** キーワードを指定した **virtual** コマンドを設定し、**sticky radius framed-ip** コマンドを設定する必要があります。 同じ仮想サーバに **sticky radius calling-station-id** コマンドと **sticky radius username** コマンドの両方を設定することはできません。 • （任意：RADIUS ロード バランシング加速データ プレーン フォワーディング専用）認証仮想サーバの VSA 関連付けグループを設定し、RADIUS 発信ステーション ID または RADIUS ユーザ名に基づいて IOS SLB で VSA 関連付けエントリを作成するかどうかを指定するには、**radius inject auth** コマンドを設定します。 認証仮想サーバの VSA 関連付けのタイマーを設定するには、**radius inject auth timer** コマンドを設定します。 認証仮想サーバの VSA 関連付けの VSA をバッファリングするには、**radius inject auth vsa** コマンドを設定します。 アカウンティング仮想サーバの VSA 関連付けグループを設定し、VSA 関連付けの Message Digest Algorithm Version 5（MD5）認証をイネーブルにするには、**radius inject acct** コマンドを設定します。

	タスク	説明
ステップ 3	IOS SLB で RADIUS framed-IP スティッキ ルーティング用のパケットを検査できるようにします。	（任意）「IOS SLB で RADIUS Framed-IP スティッキ ルーティング用のパケットを検査できるようにする方法」（P.83）を参照してください。
ステップ 4	RADIUS ロード バランシング マップを設定します。	（任意）「RADIUS ロード バランシング マップの設定方法」（P.84）を参照してください。
ステップ 5	RADIUS ロード バランシング加速データ プレーン フォワーディングを設定します。	（任意）「RADIUS ロード バランシング加速データ プレーン フォワーディングの設定方法」（P.86）を参照してください。
ステップ 6	使用できる MLS エントリの数を増やします。	（任意）Cisco Supervisor Engine 2 が搭載された Cisco Catalyst 6500 シリーズ スイッチ上で IOS SLB を dispatched モードで実行している場合は、**no mls netflow** コマンドを設定することによって性能を向上させることができます。このコマンドで、エンドユーザ フローのハードウェア スイッチングに使用できる MLS エントリの数が増えます。 **（注）** micro-flow QoS、reflexive ACL、TCP intercept、Web Cache Redirect など、ハードウェア NetFlow テーブルを使用する IOS 機能を使用している場合は、**no mls netflow** コマンドは設定しないでください。 MLS NetFlow の設定方法の詳細については、『*Catalyst 6000 Family IOS Software Configuration Guide*』を参照してください。
ステップ 7	プローブを設定します。	「プローブの設定方法」（P.60）を参照してください。 サーバの動作状況を確認するには、ping プローブを設定します。

IOS SLB で RADIUS Framed-IP スティッキ ルーティング用のパケットを検査できるようにする方法

IOS SLB で、RADIUS framed-IP スティッキ ルーティングのパケットを検査できるようにするには、次の作業を実行します。

IP アドレスとサブネット マスクと一致する発信元 IP アドレスのパケットを検査するように設定できます。検査対象のパケットの発信元 IP アドレスが、IOS SLB RADIUS framed-IP スティッキ データベースのエントリと一致する場合、パケットのルーティングにそのエントリが使用されます。それ以外の場合、IOS がパケットをルーティングします。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip slb route** {**framed-ip deny** | *ip-address netmask* **framed-ip** | **inter-firewall**}

手順の詳細

	コマンド	説明
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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 3	**ip slb route** {**framed-ip deny**	*ip-address netmask* **framed-ip**	**inter-firewall**} 例： `Router(config)# ip slb route 10.10.10.1 255.255.255.255 framed-ip`	IOS SLB で、RADIUS framed-IP スティッキ データベースによるパケットのルーティングをイネーブルにします。または、あるファイアウォール実サーバからのパケットを別のファイアウォール実サーバ経由でルーティング バックするのをイネーブルにします。

RADIUS ロード バランシング マップの設定方法

RADIUS ロード バランシング マップを設定するには、次の作業を実行します。

RADIUS ロード バランシング マップによって、IOS SLB は RADIUS 発信側ステーション ID とユーザ名に基づいてユーザ トラフィックを分類し、ルーティングすることができます。RADIUS ロード バランシングのマップをイネーブルにするには、RADIUS マップを定義してから、そのマップをサーバファームに関連付ける必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip slb map** *map-id* **radius**
4. **calling-station-id** *string*
5. **username** *string*
6. **exit**
7. **ip slb vserver** *virtual-server*
8. **virtual** *ipv4-address* [*ipv4-netmask* [**group**]] [**ipv6** *ipv6-address* [**prefix** *ipv6-prefix*]] {**tcp** | **udp**} [*port* | **any**] [**service** *service*]
9. **serverfarm** *primary-farm* [**backup** *backup-farm* [**sticky**]] [**ipv6-primary** *ipv6-primary-farm* [**ipv6-backup** *ipv6-backup-farm*]] [**map** *map-id* **priority** *priority*]

手順の詳細

	コマンド	説明
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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 3	**ip slb map** *map-id* **radius** 例： `Router(config)# ip slb map 1 radius`	IOS SLB RADIUS マップを設定し、SLB RADIUS マップ 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	**calling-station-id** *string* 例： `Router(config-slb-radius-map) # calling-station-id .919*`	RADIUS ロード バランシングの発信ステーション ID アトリビュートとマッチングする ASCII 正規表現ストリングを設定します。
ステップ 5	**username** *string* 例： `Router(config-slb-map-radius) # )# username ...?525*`	RADIUS ロード バランシングのユーザ名アトリビュートとマッチングする ASCII 正規表現ストリングを設定します。
ステップ 6	**exit** 例： `Router(config-slb-map-gtp) # exit`	SLB RADIUS マップ コンフィギュレーション モードを終了します。
ステップ 7	**ip slb vserver** *virtual-server* 例： `Router(config)# ip slb vserver GGSN_SERVER`	仮想サーバを指定し、仮想サーバ コンフィギュレーション モードを開始します。
ステップ 8	**virtual** *ipv4-address* [*ipv4-netmask* [**group**]] [**ipv6** *ipv6-address* [**prefix** *ipv6-prefix*]] {**tcp** | **udp**} [*port* | **any**] [**service** *service*] 例： `Router(config-slb-vserver) # virtual 10.0.0.1 udp 0 service radius`	仮想サーバの IP アドレス、接続の種類、およびオプションの TCP またはユーザ データグラム プロトコル（UDP）のポート番号を指定し、Internet Key Exchange（IKE; インターネット キー エクスチェンジ）または Wireless Session Protocol（WSP）の設定、およびサービスのカップリングを指定します。 **（注）** RADIUS ロード バランシングの場合、**service radius** キーワード オプションを指定します。
ステップ 9	**serverfarm** *primary-farm* [**backup** *backup-farm* [**sticky**]] [**ipv6-primary** *ipv6-primary-farm* [**ipv6-backup** *ipv6-backup-farm*]] [**map** *map-id* **priority** *priority*] 例： `Router(config-slb-vserver) # serverfarm SF1 backup SF2 map 1 priority 1`	RADIUS マップをサーバ ファームに関連付けます。実サーバ ファームを仮想サーバに関連付け、オプションで、バックアップ サーバ ファームを設定し、バックアップ サーバ ファームでスティッキ接続を使用することを指定します。 **（注）** RADIUS ロード バランシングは **sticky** キーワードをサポートしません。 複数のサーバ ファームを特定の仮想サーバに関連付けるには、**複数の serverfarm** コマンドのそれぞれを一意のマップ ID とプライオリティで設定します（つまり、各マップ ID および各マップ プライオリティは、仮想サーバに関連付けられているすべてのサーバ ファームで固有にする必要があります）。

RADIUS ロード バランシング加速データ プレーン フォワーディングの設定方法

RADIUS ロード バランシング加速データ プレーン フォワーディングを設定するには、次の作業を実行します。

RADIUS ロード バランシング加速データ プレーン フォワーディング（Turbo RADIUS ロード バランシングとも呼ばれる）は、CSG 環境で基本的な PBR ルート マップを使用して加入者のデータプレーン トラフィックを管理する高性能ソリューションです。

前提条件

Turbo RADIUS ロード バランシングには、アカウンティング仮想サーバに **predictor route-map** で設定したサーバ ファームが必要です。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip slb serverfarm** *server-farm*
4. **predictor** [**roundrobin** | **leastconns** | **route-map** *mapname*]
5. **exit**
6. **ip slb vserver** *virtual-server*
7. **virtual** *ipv4-address* [*ipv4-netmask* [**group**]] [**ipv6** *ipv6-address* [**prefix** *ipv6-prefix*]] {**tcp** | **udp**} [*port* | **any**] [**service** *service*]
8. **serverfarm** *primary-farm* [**backup** *backup-farm* [**sticky**]] [**ipv6-primary** *ipv6-primary-farm* [**ipv6-backup** *ipv6-backup-farm*]] [**map** *map-id* **priority** *priority*]
9. **radius acct local-ack key** [*encrypt*] *secret-string*
10. **radius inject auth** *group-number* {**calling-station-id** | **username**}
11. **radius inject auth timer** *seconds*
12. **radius inject auth vsa** *vendor-id*

手順の詳細

	コマンド	説明
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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 3	**ip slb serverfarm** *server-farm* 例： `Router(config)# ip slb serverfarm PUBLIC`	サーバ ファームを指定し、SLB サーバ ファーム 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	**predictor** [**roundrobin** | **leastconns** | **route-map** *mapname*] 例： `Router(config-slb-sfarm)# predictor route-map map1`	（任意）実サーバを選択する方法を決定するために使用するアルゴリズムを指定します。 Turbo RADIUS ロード バランシングには、**route-map** キーワードおよび *mapname* 引数が必要です。 **predictor route-map** コマンドを指定する場合、SLB サーバ ファーム コンフィギュレーション モードまたは実サーバ コンフィギュレーション モードで他のコマンドは使用できません。
ステップ 5	**exit** 例： `Router(config-slb-sfarm)# exit`	SLB サーバ ファーム コンフィギュレーション モードを終了します。
ステップ 6	**ip slb vserver** *virtual-server* 例： `Router(config)# ip slb vserver RADIUS_AUTH`	仮想サーバを指定し、仮想サーバ コンフィギュレーション モードを開始します。
ステップ 7	**virtual** *ipv4-address* [*ipv4-netmask* [**group**]] [**ipv6** *ipv6-address* [**prefix** *ipv6-prefix*]] {**tcp** | **udp**} [*port* | **any**] [**service** *service*] 例： `Router(config-slb-vserver)# virtual 10.10.10.10 udp 1813 service radius`	仮想サーバの IP アドレス、接続の種類、およびオプションの TCP またはユーザ データグラム プロトコル（UDP）のポート番号を指定し、Internet Key Exchange（IKE; インターネット キー エクスチェンジ）または Wireless Session Protocol（WSP）の設定、およびサービスのカップリングを指定し、SLB 仮想サーバ コンフィギュレーション モードを開始します。 **（注）** RADIUS ロード バランシングの場合、**service radius** キーワード オプションを指定します。
ステップ 8	**serverfarm** *primary-farm* [**backup** *backup-farm* [**sticky**]] [**ipv6-primary** *ipv6-primary-farm* [**ipv6-backup** *ipv6-backup-farm*]] [**map** *map-id* **priority** *priority*] 例： `Router(config-slb-vserver)# serverfarm AAAFARM`	RADIUS マップをサーバ ファームに関連付けます。実サーバ ファームを仮想サーバに関連付け、オプションで、バックアップ サーバ ファームを設定し、バックアップ サーバ ファームでスティッキ接続を使用することを指定します。 **（注）** RADIUS ロード バランシングは **sticky** キーワードをサポートしません。 複数のサーバ ファームを特定の仮想サーバに関連付けるには、**複数の serverfarm** コマンドのそれぞれを一意のマップ ID とプライオリティで設定します（つまり、各マップ ID および各マップ プライオリティは、仮想サーバに関連付けられているすべてのサーバ ファームで固有にする必要があります）。

ステップ 9	**radius acct local-ack key** [*encrypt*] *secret-string* **例：** `Router(config-slb-vserver) # radius acct local-ack key SECRET_PASSWORD`	（任意）VSA 関連付けを設定し、RADIUS 仮想サーバが RADIUS アカウンティング メッセージを承認できるようにします。 **（注）** ベンダー固有アトリビュート（VSA）関連付けを設定し、Cisco VSA がバッファリングされている場合、Cisco VSA は RADIUS Accounting-Start パケットに注入されます。Turbo RADIUS ロード バランシングに VSA 関連付けは必要ありません。 このコマンドが有効なのは、VSA 関連付けアカウンティング仮想サーバの場合だけです。
ステップ 10	**radius inject auth** *group-number* {**calling-station-id** | **username**} **例：** `Router(config-slb-vserver) # radius inject auth 1 calling-station-id`	（任意）IOS SLB RADIUS ロード バランシング加速データ プレーン フォワーディング認証仮想サーバの VSA 関連付けグループを設定し、RADIUS 発信ステーション ID または RADIUS ユーザ名に基づいて、IOS SLB で VSA 関連付けエントリを作成するかどうかを指定します。 特定の認証仮想サーバに関して、1 つの **radius inject auth** *group-number* **calling-station-id** コマンド、または、1 つの **radius inject auth** *group-number* **username** コマンドを設定できますが、両方同時には使用できません。 このコマンドが有効なのは、VSA 関連付け認証仮想サーバの場合だけです。
ステップ 11	**radius inject auth timer** *seconds* **例：** `Router(config-slb-vserver)# radius inject auth timer 45`	（任意）IOS SLB RADIUS ロード バランシング加速データ プレーン フォワーディング認証仮想サーバの VSA 関連付け用のタイマーを設定します。 このコマンドが有効なのは、VSA 関連付け認証仮想サーバの場合だけです。
ステップ 12	**radius inject auth vsa** *vendor-id* **例：** `Router(config-slb-vserver)# radius inject auth vsa vendor1`	（任意）IOS SLB RADIUS ロード バランシング加速データ プレーン フォワーディング認証仮想サーバの VSA 関連付け用の VSA をバッファします。 このコマンドが有効なのは、VSA 関連付け認証仮想サーバの場合だけです。

mSEF 用 Exchange Director の設定作業リスト

Exchange Director を mSEF 用に設定するには、次の作業を実行します。

ここでは、次の内容について説明します。

Exchange Director 用の RADIUS の設定

Exchange Director 用に RADIUS ロード バランシングを設定するには、次の作業を実行します。

手順の概要

1. サーバ ファームおよび実サーバを設定します。
2. 仮想サーバを設定します。
3. IOS SLB で RADIUS framed-IP スティッキ ルーティング用のパケットを検査できるようにします。
4. RADIUS ロード バランシング マップを設定します。
5. 使用できる MLS エントリの数を増やします。
6. プローブを設定します。

手順の詳細

	タスク	説明
ステップ 1	サーバ ファームおよび実サーバを設定します。	「サーバ ファームと実サーバの設定方法」（P.41）を参照してください。 Exchange Director 用に RADIUS のサーバ ファームおよび実サーバを設定する場合、次の注意事項を考慮してください。 • （任意）セッションベースの障害検出をイネーブルにする場合、**faildetect numconns** コマンドで **numclients** キーワードに値 1 を指定します。 • （任意）個々の仮想サーバに割り当てることができる、IOS SLB RADIUS および GTP スティッキ加入者の最大数を指定するには、**maxclients** コマンドを使用します。
ステップ 2	仮想サーバを設定します。	「仮想サーバの設定方法」（P.45）を参照してください。 Exchange Director 用に RADIUS の仮想サーバを設定する場合、次の注意事項を考慮してください。 • **virtual** コマンドを使用して、**service radius** キーワード オプションを指定します。 • （任意）入力インターフェイスを検査するために framed-IP ルーティングをイネーブルにするには、**access** *interface* **route framed-ip** コマンドを指定します。 **access** *interface* **route framed-ip** コマンドを設定する場合、さらに **service radius** キーワードを指定した **virtual** コマンドを設定する必要があります。 • （任意）外部エージェントのハンドオフ時に、IOS SLB が新しい Mobile IP 外部エージェントからの ACCT-START メッセージを待機する時間を変更するには、**hand-off radius** コマンドを設定します。 • （任意）IOS SLB セッション データベースで RADIUS エントリの時間を設定するには、**radius request** キーワードを指定した **idle** コマンドを設定します。 • （任意）IOS SLB RADIUS framed-IP スティッキ データベースでエントリの時間を設定するには、**radius framed-ip** キーワードを指定した **idle** コマンドを設定します。 • （任意）IOS SLB で IOS SLB RADIUS framed-IP スティッキ データベースを作成し、特定の加入者からの RADIUS 要求と非 RADIUS フローを同じサービス ゲートウェイに転送できるようにするには、**sticky** コマンドで **radius framed-ip** キーワードを指定します。 **sticky radius** framed-ip コマンドを設定する場合、さらに **service radius** キーワードを指定した **virtual** コマンドを設定する必要があります。

	タスク	説明
	仮想サーバを設定します。（続き）	• （任意：CDMA2000 ネットワーク専用）IOS SLB で IOS SLB RADIUS calling-station-ID スティッキ データベースを作成し、発信ステーション ID に基づいて、特定の加入者からの RADIUS 要求を同じサービス ゲートウェイに転送できるようにするには、**sticky** コマンドで **radius calling-station-id** キーワードを指定します。 IOS SLB で IOS SLB RADIUS username スティッキ データベースを作成し、ユーザ名に基づいて、特定の加入者からの RADIUS 要求を同じサービス ゲートウェイに転送できるようにするには、**sticky** コマンドで **radius username** キーワードを指定します。 **sticky radius calling-station-id** コマンドまたは **sticky radius username** コマンドを設定する場合、さらに **service radius** キーワードを指定した **virtual** コマンドを設定し、**sticky radius framed-ip** コマンドを設定する必要があります。 同じ仮想サーバに **sticky radius calling-station-id** コマンドと **sticky radius username** コマンドの両方を設定することはできません。
ステップ 3	IOS SLB で RADIUS framed-IP スティッキ ルーティング用のパケットを検査できるようにします。	（任意）「IOS SLB で RADIUS Framed-IP スティッキ ルーティング用のパケットを検査できるようにする方法」（P.83）を参照してください。
ステップ 4	RADIUS ロード バランシング マップを設定します。	（任意）「RADIUS ロード バランシング マップの設定方法」（P.84）を参照してください。
ステップ 5	使用できる MLS エントリの数を増やします。	（任意）Cisco Supervisor Engine 2 が搭載された Cisco Catalyst 6500 シリーズ スイッチ上で IOS SLB を dispatched モードで実行している場合は、**no mls netflow** コマンドを設定することによって性能を向上させることができます。このコマンドで、エンドユーザ フローのハードウェア スイッチングに使用できる MLS エントリの数が増えます。 **（注）** micro-flow QoS、reflexive ACL、TCP intercept、Web Cache Redirect など、ハードウェア NetFlow テーブルを使用する IOS 機能を使用している場合は、**no mls netflow** コマンドは設定しないでください。 MLS NetFlow の設定方法の詳細については、『*Catalyst 6000 Family IOS Software Configuration Guide*』を参照してください。
ステップ 6	プローブを設定します。	「プローブの設定方法」（P.60）を参照してください。 サーバの動作状況を確認するには、ping プローブを設定します。

Exchange Director 用のファイアウォールの設定

Exchange Director 用にファイアウォール ロード バランシングを設定するには、次の作業を実行します。

ここでは、Exchange Director 用にファイアウォールを設定するための作業リストを示します。詳細な設定情報については、このマニュアルまたは別のマニュアルの該当する項を参照してください。必須および任意の作業を示します。

- 「ファイアウォール ファームの設定方法」（P.92）（必須）
- 「ファイアウォール ファームの確認方法」（P.96）（任意）
- 「ファイアウォール接続の確認方法」（P.96）（任意）
- 「プローブの設定方法」（P.97）（必須）

- 「ワイルドカード検索の設定方法」（P.98）（任意）
- 「MLS エントリのプロトコルレベル消去の設定方法」（P.98）（任意）
- 「接続消去要求動作の設定方法」（P.98）（任意）
- 「スティッキ接続消去要求動作の設定方法」（P.99）（任意）

ファイアウォール ファームの設定方法

ファイアウォール ファームを設定するには、次の必須作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip slb firewallfarm** *firewall-farm*
4. **real** *ip-address*
5. **probe** *probe*
6. **weight** *setting*
7. **inservice**
8. **exit**
9. **access** [**source** *source-ip netmask*] [**destination** *destination-ip netmask*]| **inbound** *inbound-interface* | **outbound** *outbound-interface*]
10. **predictor hash address** [**port**]
11. **purge connection**
12. **purge sticky**
13. **replicate casa** *listen-ip remote-ip port* [*interval*] [**password** [[*encrypt*] *secret-string* [*timeout*]]]
14. **protocol tcp**
15. **delay** *duration*
16. **idle** *duration*
17. **maxconns** *maximum-number*
18. **sticky** *seconds* [**netmask** *netmask*] [**source** | **destination**]
19. **exit**
20. **protocol datagram**
21. **idle** *duration*
22. **maxconns** *maximum-number*
23. **sticky** *seconds* [**netmask** *netmask*] [**source** | **destination**]
24. **exit**
25. **inservice**

手順の詳細

	コマンド	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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 3	**ip slb firewallfarm** *firewall-farm* 例： `Router(config)# ip slb firewallfarm FIRE1`	ファイアウォール ファームの定義を IOS SLB 設定に追加し、ファイアウォール ファーム 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	**real** *ip-address* 例： `Router(config-slb-fw)# real 10.1.1.1`	ファイアウォール ファームのメンバとして、ファイアウォールを IP アドレスで指定し、実サーバ コンフィギュレーション モードを開始します。
ステップ 5	**probe** *probe* 例： `Router(config-slb-fw-real) # probe FireProbe`	プローブをファイアウォールに関連付けます。
ステップ 6	**weight** *setting* 例： `Router(config-slb-fw-real) # weight 16`	（任意）ファイアウォールの作業負荷容量を指定します。ファイアウォール ファーム内の他のファイアウォールと相対的な値です。
ステップ 7	**inservice** 例： `Router(config-slb-fw-real) # inservice`	ファイアウォールをファイアウォール ファームと IOS SLB で使用できるようにします。
ステップ 8	**exit** 例： `Router(config-slb-fw-real) # exit`	実サーバ コンフィギュレーション モードを終了します。

	コマンド	目的
ステップ 9	**access** [**source** *source-ip netmask*] [**destination** *destination-ip netmask*]| **inbound** *inbound-interface* | **outbound** *outbound-interface*] 例： `Router(config-slb-fw)# access destination 10.1.6.0 255.255.255.0`	（任意）特定のフローをファイアウォール ファームにルーティングします。
ステップ 10	**predictor hash address** [**port**] 例： `Router(config-slb-fw)# predictor hash address`	（任意）ファイアウォールを選択するときに、発信元および宛先の IP アドレスに加え、発信元および宛先の TCP またはユーザ データグラム プロトコル（UDP）のポート番号を使用するかどうかを指定します。
ステップ 11	**purge connection** 例： `Router(config-slb-fw)# purge connection`	（任意）IOS SLB ファイアウォール ロード バランシングで接続の消去要求を送信できるようにします。
ステップ 12	**purge sticky** 例： `Router(config-slb-fw)# purge sticky`	（任意）スティッキ アイドル タイマーが切れたときに、IOS SLB ファイアウォール ロード バランシングで消去要求を送信できるようにします。
ステップ 13	**replicate casa** *listen-ip remote-ip port* [*interval*] [**password** [[*encrypt*] *secret-string* [*timeout*]]] 例： `Router(config-slb-fw)# replicate casa 10.10.10.11 10.10.11.12 4231`	（任意）IOS SLB ファイアウォール ロード バランシング ディシジョン テーブルのバックアップ スイッチへのステートフル バックアップを設定します。
ステップ 14	**protocol tcp** 例： `Router(config-slb-fw)# protocol tcp`	（任意）ファイアウォール ファーム TCP プロトコル コンフィギュレーション モードを開始します。
ステップ 15	**delay** *duration* 例： `Router(config-slb-fw-tcp)# delay 30`	（任意）ファイアウォール ファーム TCP プロトコル コンフィギュレーション モードで、接続の終了後に IOS SLB ファイアウォール ロード バランシングが TCP 接続コンテキストを維持する時間を指定します。
ステップ 16	**idle** *duration* 例： `Router(config-slb-fw-tcp)# idle 120`	（任意）ファイアウォール ファーム TCP プロトコル コンフィギュレーション モードで、パケット アクティビティが存在しない場合に、IOS SLB ファイアウォール ロード バランシングが接続コンテキストを維持する最短時間を指定します。

	コマンド	目的
ステップ 17	**maxconns** *maximum-number* 例： Router(config-slb-fw-tcp)# maxconns 1000	(任意) ファイアウォール ファーム TCP プロトコル コンフィギュレーション モードの場合、ファイアウォール ファームで同時に使用できるアクティブな TCP 接続の最大数を指定します。
ステップ 18	**sticky** *seconds* [**netmask** *netmask*] [**source** | **destination**] 例： Router(config-slb-fw-tcp)# sticky 60	(任意) ファイアウォール ファーム TCP プロトコル コンフィギュレーション モードで、次のいずれかの条件を満たす場合、同じ IP アドレスからの接続に、同じファイアウォールを使用することを指定します。 • 同じ IP アドレスのペア間に接続が存在する間（送信元/宛先スティッキ）。 • 最後の接続が破棄された後の *duration* で定義される期間。
ステップ 19	**exit** 例： Router(config-slb-fw-tcp)# exit	ファイアウォール ファーム TCP プロトコル コンフィギュレーション モードを終了します。
ステップ 20	**protocol datagram** 例： Router(config-slb-fw)# protocol datagram	(任意) ファイアウォール ファーム データグラム プロトコル コンフィギュレーション モードを開始します。
ステップ 21	**idle** *duration* 例： Router(config-slb-fw-udp)# idle 120	(任意) ファイアウォール ファーム TCP プロトコル コンフィギュレーション モードで、パケット アクティビティが存在しない場合に、IOS SLB ファイアウォール ロード バランシングが接続コンテキストを維持する最短時間を指定します。
ステップ 22	**maxconns** *maximum-number* 例： Router(config-slb-fw-udp)# maxconns 1000	(任意) ファイアウォール ファーム データグラム プロトコル コンフィギュレーション モードの場合、ファイアウォール ファームで同時に使用できるアクティブな データグラム接続の最大数を指定します。
ステップ 23	**sticky** *seconds* [**netmask** *netmask*] [**source** | **destination**] 例： Router(config-slb-fw-udp)# sticky 60	(任意) ファイアウォール ファーム データグラム プロトコル コンフィギュレーション モードで、次のいずれかの条件を満たす場合、同じ IP アドレスからの接続に、同じファイアウォールを使用することを指定します。 • 同じ IP アドレスのペア間に接続が存在する間（送信元/宛先スティッキ）。 • 最後の接続が破棄された後の *duration* で定義される期間。
ステップ 24	**exit** 例： Router(config-slb-fw-udp)# exit	ファイアウォール ファーム データグラム プロトコル コンフィギュレーション モードを終了します。
ステップ 25	**inservice** 例： Router(config-slb-fw)# inservice	ファイアウォール ファームを IOS SLB で使用できるようにします。

ファイアウォール ファームの確認方法

ファイウォール ファームを確認するには、次の任意作業を実行します。

手順の概要

1. **show ip slb real**
2. **show ip slb firewallfarm**

手順の詳細

ステップ 1 次の **show ip slb real** コマンドで、ファイアウォール ファーム FIRE1 のステータス、関連する実サーバ、およびそのステータスを表示します。

```
Router# show ip slb real

real                  farm name        weight   state          conns
-------------------------------------------------------------------
10.1.1.2              FIRE1            8        OPERATIONAL    0
10.1.2.2              FIRE1            8        OPERATIONAL    0
```

ステップ 2 次の **show ip slb firewallfarm** コマンドで、ファイアウォール ファーム FIRE1 の設定およびステータスを表示します。

```
Router# show ip slb firewallfarm

firewall farm    hash        state         reals
-------------------------------------------------
FIRE1            IPADDR      INSERVICE     2
```

ファイアウォール接続の確認方法

ファイアウォール接続を確認するには、次の任意作業を実行します。

手順の概要

1. 外部実サーバに ping を送信します。
2. 内部実サーバに ping を送信します。
3. **show ip slb stats**
4. **show ip slb real detail**
5. **show ip slb conns**

手順の詳細

IOS SLB ファイアウォール ロード バランシングが設定され、正しく動作していることを確認するには、次の手順を実行します。

ステップ 1 IOS SLB ファイアウォール ロード バランシング デバイスから外部実サーバ（ファイアウォールの外側にあるサーバ）に ping を送信します。

ステップ 2 クライアントから内部実サーバ（ファイアウォールの内側にあるサーバ）に ping を送信します。

ステップ 3 **show ip slb stats** コマンドを使用して、IOS SLB ファイアウォール ロード バランシングのネットワーク ステータスに関する情報を表示します。

```
Router# show ip slb stats

 Pkts via normal switching:  0
 Pkts via special switching: 0
 Pkts dropped:               0
 Connections Created:        1911871
 Connections Established:    1967754
 Connections Destroyed:      1313251
 Connections Reassigned:     0
 Zombie Count:               0
 Connections Reused:         59752
 Connection Flowcache Purges:1776582
 Failed Connection Allocs:   17945
 Failed Real Assignments:    0
```

- 通常のスイッチングは、IOS SLB パケットが通常の IOS スイッチング パス（CEF、ファースト スイッチング、およびプロセス レベル スイッチング）上で管理されているときに発生します。
- 特殊なスイッチングは、IOS SLB パケットがハードウェア支援スイッチング パス上で管理されているときに発生します。

ステップ 4 **show ip slb real detail** コマンドを使用して、IOS SLB ファイアウォール ロード バランシングの実サーバのステータスに関する詳細情報を表示します。

```
Router# show ip slb reals detail

172.16.88.5, SF1, state = OPERATIONAL, type = server
  ipv6 = 2342:2342:2343:FF04:2388:BB03:3223:8912
  conns = 0, dummy_conns = 0, maxconns = 4294967295
  weight = 8, weight(admin) = 8, metric = 0, remainder = 0
  reassign = 3, retry = 60
  failconn threshold = 8, failconn count = 0
  failclient threshold = 2, failclient count = 0
  total conns established = 0, total conn failures = 0
  server failures = 0
```

ステップ 5 **show ip slb conns** コマンドを使用して、アクティブな IOS SLB ファイアウォール ロード バランシング接続に関する情報を表示します。

```
Router# show ip slb conns

vserver         prot client               real                 state     nat
-------------------------------------------------------------------------------
FirewallTCP     TCP  80.80.50.187:40000   10.1.1.4             ESTAB     none
FirewallTCP     TCP  80.80.50.187:40000   10.1.1.4             ESTAB     none
FirewallTCP     TCP  80.80.50.187:40000   10.1.1.4             ESTAB     none
FirewallTCP     TCP  80.80.50.187:40000   10.1.1.4             ESTAB     none
FirewallTCP     TCP  80.80.50.187:40000   10.1.1.4             ESTAB     none
```

IOS SLB ネットワークと接続の確認に使用されるその他のコマンドについては、「Cisco IOS SLB 機能のモニタ方法と保守方法」（P.116）を参照してください。

プローブの設定方法

プローブを設定するには、次の必須作業を実行します。

手順の概要

1. ファイアウォール ファームの各実サーバにプローブを設定します。

手順の詳細

Exchange Director では、障害の検出と回復にプローブを使用します。ファイアウォール ファームの各実サーバにプローブを設定する必要があります。

- ファイアウォール ファーム内の実サーバごとにプローブを ping することを推奨します。詳細については、「ping プローブの設定方法」（P.65）を参照してください。
- ファイアウォールで、ping プローブの転送を許可していない場合、代わりに HTTP プローブを使用します。詳細については、「HTTP プローブの設定方法」（P.63）を参照してください。
- ファイアウォール ファームの各ファイアウォールに、複数のプローブを設定できます。また、サポートされる種類（DNS、HTTP、TCP、または ping）のプローブを任意に組み合わせることができます。

ワイルドカード検索の設定方法

ワイルドカード検索を設定するには、次の任意作業を実行します。

手順の概要

1. **mls ip slb wildcard search rp**

手順の詳細

mls ip slb wildcard search rp コマンドを使用して、PFC 上で TCAM の容量を超える可能性を低減します。

MLS エントリのプロトコルレベル消去の設定方法

アクティブな TCP および UDP フロー パケットからの MLS エントリのプロトコルレベル消去を設定するには、次の作業を実行します。

手順の概要

1. **mls ip slb purge global**

手順の詳細

mls ip slb purge global コマンドを使用して、TCP および UDP フロー パケットの消去スロットリングをイネーブルにします（これがデフォルトの設定です）。

TCP および UDP フロー パケットの消去スロットリングをディセーブルにするには、このコマンドの **no** 形式を使用します。

接続消去要求動作の設定方法

IOS SLB ファイアウォール ロード バランシングから、接続の消去要求を送信できるようにするには、次の作業を実行します。

手順の概要

1. **purge connection**

手順の詳細

purge connection コマンドを使用して、IOS SLB ファイアウォール ロード バランシングから、接続の消去要求を送信できるようにします（これがデフォルトの設定です）。

消去要求の送信を完全に停止するには、このコマンドの **no** 形式を使用します。

スティッキ接続消去要求動作の設定方法

スティッキ タイマーが期限切れになるとき、IOS SLB ファイアウォール ロード バランシングから、スティッキ接続の消去要求を送信できるようにするには、次の作業を実行します。

手順の概要

1. **purge sticky**

手順の詳細

スティッキ タイマーが期限切れになるとき、IOS SLB ファイアウォール ロード バランシングから、スティッキ接続の消去要求を送信できるようにするには、**purge sticky** コマンドを使用します（これがデフォルトの設定です）。

スティッキ接続の消去要求の送信を完全に停止するには、このコマンドの **no** 形式を使用します。

VPN サーバ ロード バランシングの設定作業リスト

VPN サーバ ロード バランシングを設定するには、次の作業を実行します。

手順の概要

1. サーバ ファームおよび実サーバを設定します。
2. 仮想サーバを設定します。
3. プローブを設定します。

手順の詳細

	タスク	説明
ステップ 1	サーバ ファームおよび実サーバを設定します。	「サーバ ファームと実サーバの設定方法」（P.41）を参照してください。 サーバ ファームと実サーバを VPN サーバ ロード バランシング用に設定する場合は、**real** コマンドを使用して、VPN ターミネータとして機能する実サーバの IP アドレスを指定します。
ステップ 2	仮想サーバを設定します。	「仮想サーバの設定方法」（P.45）を参照してください。 IPSec フローの VPN サーバ ロード バランシングの仮想サーバを設定する場合、次の注意事項を考慮してください。 • プロトコルを **udp** に、ポートを **isakmp** に設定した **virtual** コマンドを使用して、UDP 仮想サーバを設定します。**isakmp** キーワードを使用すると、IKE（ポート 500）経由で暗号キーを交換できます。 • プロトコルを **esp** に設定した **virtual** コマンドを使用して、ESP 仮想サーバを設定します。 • 15 秒以上の *duration* を指定した **sticky** コマンドを使用して、UDP 仮想サーバから ESP 仮想サーバ方向とその逆方向のスティッキ接続を指定します。 仮想サーバを Point-to-Point Tunneling Protocol（PPTP）フローの VPN サーバ ロード バランシング用に設定する場合は、次の留意点を考慮してください。 • **tcp** キーワードとポート番号 **1723** を指定した **virtual** コマンドを使用して、TCP 仮想サーバを設定します。 • **gre** キーワードを指定した **virtual** コマンドを使用して、GRE 仮想サーバを設定します。 • 15 秒以上の *duration* を指定した **sticky** コマンドを使用して、TCP 仮想サーバから GRE 仮想サーバ方向とその逆方向のスティッキ接続を指定します。
ステップ 3	プローブを設定します。	「プローブの設定方法」（P.60）を参照してください。 サーバの動作状況を確認するには、ping プローブを設定します。

ASN ロード バランシングの設定作業リスト

Access Service Network（ASN）ゲートウェイ セット全体のロード バランシングを設定するには、次の作業を実行します。

手順の概要

1. ベース ステーションを設定します。
2. サーバ ファームおよび実サーバを設定します。
3. 仮想サーバを設定します。
4. プローブを設定します。

手順の詳細

	タスク	説明
ステップ 1	ベース ステーションを設定します。	IOS SLB で MSS からの要求を管理できるようにするには、IOS SLB デバイスの仮想 IP アドレスを使用してベース ステーションを設定します。
ステップ 2	プローブを設定します。	「プローブの設定方法」（P.60）を参照してください。 サーバの動作状況を確認するには、ping プローブを設定します。
ステップ 3	サーバ ファームおよび実サーバをプローブに関連付けます。	「サーバ ファームと実サーバの設定方法」（P.41）を参照してください。 サーバ ファームと実サーバを ASN ロード バランシング用に設定する場合は、次の留意点を考慮してください。 • **real** コマンドを使用して、ASN ゲートウェイの IP アドレスを指定します。 • （任意）**real** コマンドで **asn purge** オプションを使用して、IOS SLB で、障害が発生した実サーバに関連付けられたオブジェクトを ASN スティッキ データベースから自動的に削除できるようにします。
ステップ 4	仮想サーバをサーバ ファームに関連付けます。	「仮想サーバの設定方法」（P.45）を参照してください。 仮想サーバを ASN ロード バランシング用に設定する場合は、次の留意点を考慮してください。 • サービスを **asn** に設定した **virtual** コマンドを使用して、仮想サーバを設定します。 • **asn request** キーワードを指定した **idle** コマンドを使用して、ASN ロード バランシング用のアイドル接続タイマーを設定します。 • （任意）**sticky** コマンドで **asn msid** オプションを指定して、IOS SLB で特定の MSID の ASN セッションを負荷分散できるようにします。 • （任意）**asn msid** キーワードを指定した **idle** コマンドを使用して、ASN MSID スティッキ データベース用のタイマーを設定します。 • （任意）**gw port** コマンドを使用して、Cisco BWG ポートを設定します。

Home Agent Director の設定作業リスト

Home Agent Director を設定するには、次の作業を実行します。

手順の概要

1. サーバ ファームおよび実サーバを設定します。
2. 仮想サーバを設定します。
3. サーバの各ホーム エージェントでループバックとして仮想 IP アドレスを設定します。
4. Dynamic Feedback Protocol（DFP）を設定します。

手順の詳細

	タスク	説明
ステップ 1	サーバ ファームおよび実サーバを設定します。	「サーバ ファームと実サーバの設定方法」（P.41）を参照してください。 Home Agent Director 用にサーバ ファームおよび実サーバを設定する場合、次の注意事項を考慮してください。 • **predictor** コマンドのデフォルト設定（加重ラウンド ロビン アルゴリズム）を受け入れます。 • **real** コマンドを使用して、ホーム エージェントとして動作する実サーバの IP アドレスを指定します。
ステップ 2	仮想サーバを設定します。	「仮想サーバの設定方法」（P.45）を参照してください。 **virtual** コマンドを使用して Home Agent Director 用に仮想サーバを設定する場合、次の注意事項を考慮してください。 • 仮想サーバとして Home Agent Director の IP アドレスを指定します。 • **udp** キーワード オプションを指定します。 • ホーム エージェントが IP Mobility Support（RFC 2002）に準拠している場合、ポート番号 434 を指定します。また、全ポート仮想サーバ（つまり、すべてのポート宛てのフローを受け入れる仮想サーバ）を設定するには、ポート番号 0 または **any** を指定します。 • **service ipmobile** キーワード オプションを指定します。
ステップ 3	サーバの各ホーム エージェントでループバックとして仮想 IP アドレスを設定します。	（dispatched モードの場合に必須）この手順が必須なのは、dispatched モードを使用する場合だけです。詳細については、『*Cisco IOS Interface Configuration Guide*, Release 12.2』の「Configuring a Loopback Interface」の項を参照してください。
ステップ 4	DFP を設定します。	（任意）「DFP の設定方法」（P.70）を参照してください。 Home Agent Director 用に DFP を設定する場合、次の注意事項を考慮してください。 • ホーム エージェントから IOS SLB に送信する DFP の最大加重を制御するには、**ip mobile home-agent dfp-max-weight** コマンドを使用します。 • 実ホーム エージェントのアドレスとして、Registration Reply（RRP）の発信元アドレスおよびホーム エージェント アドレス フィールドを設定するには、**ip mobile home-agent dynamic-address** コマンドを使用します。 • バインディングの最大数を設定するには、**ip mobile home-agent max-binding** コマンドを使用します。 これらの Mobile IP コマンドの詳細については、『*Cisco Mobile Wireless Home Agent Release 2.0*』のフィーチャ モジュールを参照してください。

NAT の設定方法

クライアント NAT 用の IOS SLB NAT クライアント アドレス プールを設定するには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip slb natpool pool** *start-ip end-ip* [**netmask** *netmask* | **prefix-length** *leading-1-bits*] [**entries** *init-address* [*max-address*]]
4. **nat** {**client** *pool* | **server**}

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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 3	**ip slb natpool pool** *start-ip end-ip* [**netmask** *netmask*	**prefix-length** *leading-1-bits*] [**entries** *init-address* [*max-address*]] 例： `Router(config)# ip slb natpool web-clients 10.1.10.1 10.1.10.5 netmask 255.255.0.0`	クライアント アドレス プールを設定します。 GPRS ロード バランシングはこのコマンドをサポートしません。 サーバ NAT 用のクライアント アドレス プールは設定する必要がありません。
ステップ 4	**nat** {**client** *pool*	**server**} 例： `Router(config-slb-sfarm)# nat server`	SLB NAT を設定し、NAT モードを指定します。 同じ仮想サーバに関連付けられたすべての IPv4 または IPv6 サーバ ファームは、同じ NAT 設定にする必要があります。

また、**nat** コマンドを使用して、サーバ ファームで NAT クライアント変換モードまたは NAT サーバ アドレス変換モードを指定する必要があります。詳細については、「サーバ ファームと実サーバの設定方法」（P.41）を参照してください。NAT の仮想サーバを設定する場合、ESP または GRE 仮想サーバにクライアント NAT は設定できません。

スタティック NAT の設定方法

スタティック NAT を設定するには、次の作業を実行します。

スタティック NAT を使用すれば、一部のユーザが NAT を使用し、同じイーサネット インターフェイス上の他のユーザは引き続き独自の IP アドレスを使用することができます。このオプションによって、実サーバからの応答と、実サーバが開始した接続要求とを区別することで、実サーバのデフォルトの NAT 動作を設定できます。

（注） 予期しない結果を回避するために、スタティック NAT 設定が仮想サーバ設定を反映するようにします。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip slb static** {**drop** | **nat** {**virtual** | *virtual-ip* [**per-packet** | **sticky**]}}
4. **real** *ip-address* [*port*]

手順の詳細

	コマンド	説明
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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 3	**ip slb static** {**drop** | **nat** {**virtual** | *virtual-ip* [**per-packet** | **sticky**]}} 例： `Router(config)# ip slb static nat 10.1.10.1 per-packet`	実サーバの NAT 動作を設定し、スタティック NAT コンフィギュレーション モードを開始します。 **（注）** *virtual-ip* 引数を指定して、**per-packet** オプションを指定しなかった場合は、IOS SLB でサーバ ポート変換を使用して、別の実サーバによって開始された接続要求が区別されます。
ステップ 4	**real** *ip-address* [*port*] 例： `Router(config-slb-static)# real 10.1.1.3`	スタティック NAT を使用するように 1 つまたは複数の実サーバを設定します。

ステートレス バックアップの設定作業リスト

IOS SLB デバイス間の VLAN でステートレス バックアップを設定するには、次の作業を実行します。

（注） 複数の IOS SLB デバイスが仮想 IP アドレスを共有しているアクティブ スタンバイの場合、重複しないクライアントの範囲を使用する必要があります。また、ポリシー ルーティングを使用して、適切な IOS SLB デバイスにフローを転送する必要があります。

手順の概要

1. 必須および任意の IOS SLB 機能を設定します。
2. ファイアウォール ロード バランシングを設定します。
3. IP ルーティング プロトコルを設定します。
4. IOS SLB デバイス間の VLAN を設定します。
5. ステートレス バックアップ設定を確認します。

手順の詳細

	タスク	説明
ステップ 1	必須および任意の IOS SLB 機能を設定します。	（サーバ ロード バランシングの場合に必須）「必須と任意の IOS SLB 機能の設定方法」（P.41）を参照してください。
ステップ 2	ファイアウォール ロード バランシングを設定します。	（ファイアウォール ロード バランシングの場合に必須）「ファイアウォール ロード バランシングの設定方法」（P.53）を参照してください。
ステップ 3	IP ルーティング プロトコルを設定します。	詳細については、『*Cisco IOS IP Configuration Guide*, Release 12.2』の「IP Routing Protocols」の章を参照してください。
ステップ 4	IOS SLB デバイス間の VLAN を設定します。	詳細については、『*Cisco IOS Switching Services Configuration Guide*, Release 12.2』の「Virtual LANs」の章を参照してください。
ステップ 5	ステートレス バックアップ設定を確認します。	（任意）「ステートレス バックアップ設定の確認方法」（P.106）を参照してください。

ステートレス バックアップ設定の確認方法

ステートレス バックアップ設定を確認するには、次の作業を実行します。

手順の概要

1. **show ip slb vservers**
2. **show ip slb vservers detail**
3. **show ip slb firewallfarm**
4. **show ip slb firewallfarm details**

手順の詳細

サーバ ロード バランシングの場合、ステートレス バックアップが設定済みで、適切に動作していることを確認するには、次の **show ip slb vservers** コマンドを使用して、IOS SLB 仮想サーバのステータスに関する情報を表示します。

```
Router# show ip slb vservers

slb vserver      prot  virtual               state         conns
-------------------------------------------------------------------
VS1              TCP   10.10.10.12:23        OPERATIONAL     2
VS2              TCP   10.10.10.18:23        OPERATIONAL     2

Router# show ip slb vservers detail

VS1, state = OPERATIONAL, v_index = 10
  virtual = 10.10.10.12:23, TCP, service = NONE, advertise = TRUE
  server farm = SERVERGROUP1, delay = 10, idle = 3600
  sticky timer = 0, sticky subnet = 255.255.255.255
  sticky group id = 0
  synguard counter = 0, synguard period = 0
  conns = 0, total conns = 0, syns = 0, syn drops = 0
  standby group = None
VS2, state = INSERVICE, v_index = 11
  virtual = 10.10.10.18:23, TCP, service = NONE, advertise = TRUE
  server farm = SERVERGROUP2, delay = 10, idle = 3600
  sticky timer = 0, sticky subnet = 255.255.255.255
  sticky group id = 0
  synguard counter = 0, synguard period = 0
  conns = 0, total conns = 0, syns = 0, syn drops = 0
  standby group = None
```

ファイアウォール ロード バランシングの場合、ステートレス バックアップが設定済みで、適切に動作していることを確認するには、次の **show ip slb firewallfarm** コマンドを使用して、IOS SLB ファイアウォール ファームのステータスに関する情報を表示します。

```
Router# show ip slb firewallfarm

firewall farm    hash        state         reals
-----------------------------------------------
FIRE1            IPADDR      INSERVICE     2

Router# show ip slb firewallfarm details

FIRE1, hash = IPADDRPORT, state = INSERVICE, reals = 2
  FirewallTCP:
   sticky timer = 0, sticky subnet = 255.255.255.255
   idle = 3600, delay = 10, syns = 1965732, syn drop = 0
   maxconns = 4294967295, conns = 597445, total conns = 1909512
  FirewallUDP:
   sticky timer = 0, sticky subnet = 255.255.255.255
   idle = 3600
   maxconns = 1, conns = 0, total conns = 1
  Real firewalls:
    10.1.1.3, weight = 10, OPERATIONAL, conns = 298823
    10.1.1.4, weight = 10, OPERATIONAL, conns = 298622
  Total connections = 597445
```

冗長ルート プロセッサのステートフル バックアップの設定作業リスト

冗長ルート プロセッサのステートフル バックアップを設定するには、次の作業を実行します。

手順の概要

1. スレーブ レプリケーションのレプリケーション メッセージ レートを設定します。
2. 必須および任意の IOS SLB 機能を設定します。
3. ファイアウォール ロード バランシングを設定します。

手順の詳細

	タスク	説明
ステップ 1	スレーブ レプリケーションのレプリケーション メッセージ レートを設定します。	グローバル コンフィギュレーション モードで **ip slb replicate slave rate** コマンドを指定します。
ステップ 2	必須および任意の IOS SLB 機能を設定します。	（サーバ ロード バランシングの場合に必須）「必須と任意の IOS SLB 機能の設定方法」（P.41）を参照してください。 冗長ルート プロセッサのステートフル バックアップの仮想サーバを設定する場合、次の注意事項を考慮してください。 • **replicate slave** コマンドを指定します。 • （任意）仮想サーバのレプリケーション配信間隔を設定するには、**replicate interval** コマンドを設定します。
ステップ 3	ファイアウォール ロード バランシングを設定します。	（ファイアウォール ロード バランシングの場合に必須）「ファイアウォール ロード バランシングの設定方法」（P.53）を参照してください。 冗長ルート プロセッサのステートフル バックアップのファイアウォール ファームを設定する場合、次の注意事項を考慮してください。 • **replicate slave** コマンドを指定します。 • （任意）ファイアウォール ファームのレプリケーション配信間隔を設定するには、**replicate interval** コマンドを設定します。

データベース エントリの設定方法

データベース エントリを設定するには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip slb entries** [**conn** [*init-conn* [*max-conn*]] | **frag** [*init-frag* [*max-frag*] | **lifetime** *timeout*] | **gtp** {**gsn** [*init-gsn* [*max-gsn*] | **nsapi** [*init-nsapi* [*max-nsapi*]} | **sticky** [*init-sticky* [*max-sticky*]]]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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 3	**ip slb entries** [**conn** [*init-conn* [*max-conn*]]	**frag** [*init-frag* [*max-frag*]	**lifetime** *timeout*]	**gtp** {**gsn** [*init-gsn* [*max-gsn*]	**nsapi** [*init-nsapi* [*max-nsapi*]}	**sticky** [*init-sticky* [*max-sticky*]]] 例： `Router(config)# ip slb entries conn 128000 512000`	初期割り当てと IOS SLB データベース エントリの最大値を指定します。 **（注）** このコマンドは、残りの IOS SLB 設定を入力する*前*に入力します。IOS SLB 設定がすでに存在する場合、このコマンドを入力してから、IOS SLB をリロードする必要があります。

フラグメント データベース用のバッファの設定方法

フラグメント データベースのバッファを設定するには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip slb maxbuffers frag** *buffers*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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 3	**ip slb maxbuffers frag** *buffers* 例： `Router(config)# ip slb maxbuffers frag 300`	IOS SLB フラグメント データベース用のバッファの最大数を設定します。

データベースとカウンタのクリア方法

データベースおよびカウンタをクリアするには、次の作業を実行します。

手順の概要

1. **clear ip slb connections** [**firewallfarm** *firewall-farm* | **serverfarm** *server-farm* | **vserver** *virtual-server*]
2. **clear ip slb counters** [**kal-ap**]
3. **clear ip slb sessions** [**firewallfarm** *firewall-farm* | **serverfarm** *server-farm* | **vserver** *virtual-server*]
4. **clear ip slb sticky asn msid** *msid*
5. **clear ip slb sticky gtp imsi** [**id** *imsi*]
6. **clear ip slb sticky radius** {**calling-station-id** [**id** *string*] | framed-ip [*framed-ip* [*netmask*]]}

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**clear ip slb connections** [**firewallfarm** *firewall-farm* | **serverfarm** *server-farm* | **vserver** *virtual-server*] 例： `Router# clear ip slb connections vserver VSERVER1`	1 つまたは複数のファイアウォール ファーム、サーバ ファーム、または仮想サーバの IOS SLB 接続データベースをクリアします。
ステップ 2	**clear ip slb counters** [**kal-ap**] 例： `Router# clear ip slb counters`	IOS SLB カウンタをクリアします。 IP IOS SLB KeepAlive Application Protocol（KAL-AP）だけをクリアするには、**kal-ap** キーワードを使用します。
ステップ 3	**clear ip slb sessions** [**firewallfarm** *firewall-farm* | **serverfarm** *server-farm* | **vserver** *virtual-server*] 例： `Router# clear ip slb sessions serverfarm FARM1`	1 つまたは複数のファイアウォール ファーム、サーバ ファーム、または仮想サーバの IOS SLB RADIUS セッション データベースをクリアします。
ステップ 4	**clear ip slb sticky asn msid** *msid* 例： `Router# clear ip slb sticky asn msid 001646013fc0`	IOS SLB ASN MSID スティッキ データベースからエントリをクリアします。
ステップ 5	**clear ip slb sticky gtp imsi** [**id** *imsi*] 例： `Router# clear ip slb sticky gtp imsi`	IOS SLB GTP IMSI スティッキ データベースからエントリをクリアします。
ステップ 6	**clear ip slb sticky radius** {**calling-station-id** [**id** *string*] | framed-ip [*framed-ip* [*netmask*]]} 例： `Router# clear ip slb sticky radius framed-ip`	IOS SLB RADIUS スティッキ データベースからエントリをクリアします。

ワイルドカード検索の設定方法

ワイルドカード検索を設定するには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **mls ip slb search**

手順の詳細

ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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 3	`Router(config)# mls ip slb search {wildcard [pfc | rp] | icmp}` 例： `Router(config)# mls ip slb search wildcard rp`	IOS SLB ワイルドカード検索の動作を指定します。 このコマンドは、Cisco Catalyst 6500 シリーズ スイッチに対してのみサポートされています。

MLS エントリのプロトコルレベル消去の設定方法

アクティブな TCP および UDP フロー パケットからの MLS エントリのプロトコルレベル消去を指定するには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **mls ip slb purge global**

手順の詳細

ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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 3	`Router(config)# mls ip slb purge global` 例： `Router(config)# mls ip slb purge global`	アクティブな TCP および UDP フロー パケットからの MLS エントリのプロトコルレベル消去を指定します。 このコマンドは、Cisco Catalyst 6500 シリーズ スイッチに対してのみサポートされています。

接続の消去方法と再割り当て方法

接続を消去し、再割り当てするには、次の作業を実行します。

アイドル タイマーの期限が切れていない場合でも、障害が発生したサーバおよびファイアウォールへの接続を接続データベースから自動的に削除する機能をイネーブルにできます。この機能は、発信元ポートを循環させないアプリケーション（IKE など）の場合、およびフローを区別するポートがないプロトコル（ESP など）の場合に有効です。

また、障害が発生した実サーバまたはファイアウォール宛ての RADIUS スティッキ オブジェクトを、新しい実サーバまたはファイアウォールに自動的に再割り当てする機能をイネーブルにできます。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip slb serverfarm** *server-farm*
4. **failaction** [**purge** | **asn purge** | **gtp purge** | **radius reassign**]
5. **exit**
6. **ip slb firewallfarm** *firewall-farm*

7. failaction purge

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： Router> **enable**	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： Router# **configure terminal**	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 3	**ip slb serverfarm** *server-farm* 例： Router(config)# ip slb serverfarm PUBLIC	サーバ ファーム 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	**failaction** [**purge** | **asn purge** | **gtp purge** | **radius reassign**] 例： Router(config-slb-sfarm)# **failaction purge**	実サーバで障害が発生した場合の IOS SLB 動作を設定します。
ステップ 5	**exit** 例： Router(config-slb-sfarm)# exit	サーバ ファーム コンフィギュレーション モードを終了します。
ステップ 6	**ip slb firewallfarm** *firewall-farm* 例： Router(config)# ip slb firewallfarm fire1	ファイアウォール ファーム コンフィギュレーション モードを開始します。
ステップ 7	**failaction purge** 例： Router(config-slb-fw)# failaction purge	ファイアウォールで障害が発生した場合の IOS SLB 動作を設定します。

自動サーバ障害検出のディセーブル方法

自動サーバ障害検出をディセーブルにするには、次の作業を実行します。

全ポート仮想サーバ（つまり、GTP ポートを除くすべてのポート宛てのフローを受け入れる仮想サーバ）を設定した場合、アプリケーション ポートが存在しないサーバにフローを渡すことができます。サーバがこのようなフローを拒否すると、IOS SLB はそのサーバを無効と見なし、ロード バランシングから除外することがあります。この状況は、RADIUS ロード バランシング環境の応答が遅い AAA サーバの場合にも発生する可能性があります。この状況を回避するには、自動サーバ障害検出をディセーブルにします。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip slb serverfarm** *server-farm*
4. **real** *ipv4-address* [**ipv6** ***ipv6-address***] [***port***]
5. **no faildetect inband**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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 3	**ip slb serverfarm** *server-farm* 例： `Router(config)# ip slb serverfarm PUBLIC`	サーバ ファーム 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	**real** *ipv4-address* [**ipv6** *ipv6-address*] [*port*] 例： `Router(config-slb-sfarm)# real 10.1.1.1`	サーバ ファームのメンバとして実サーバを指定し、実サーバ コンフィギュレーション モードを開始します。 **（注）** GTP ロード バランシングに対するデュアルスタック サポートの場合は、実サーバの IPv4 アドレスと IPv6 アドレスを指定します。
ステップ 5	**no faildetect inband** 例： `Router(config-slb-real)# no faildetect inband`	自動サーバ障害検出をディセーブルにします。 **（注）** **no faildetect inband** コマンドを使用して自動サーバ障害検出をディセーブルにした場合は、1 つ以上のプローブを設定することを推奨します。 **no faildetect inband** コマンドを指定した場合は、指定された **faildetect numconns** コマンドが無視されます。

Cisco IOS SLB 機能のモニタ方法と保守方法

IOS SLB の実行時情報を取得および表示するには、次の作業を実行します。

手順の概要

1. **show ip slb conns**
2. **show ip slb dfp**
3. **show ip slb firewallfarm**
4. **show ip slb fragments**
5. **show ip slb gtp**
6. **show ip slb map**
7. **show ip slb natpool**
8. **show ip slb probe**
9. **show ip slb reals**
10. **show ip slb replicate**
11. **show ip slb serverfarms**
12. **show ip slb sessions**
13. **show ip slb static**
14. **show ip slb stats**
15. **show ip slb sticky**
16. **show ip slb vservers**
17. **show ip slb wildcard**

手順の詳細

ステップ 1　**show ip slb conns** [**vserver** *virtual-server* | **client** *ip-address* | **firewall** *firewall-farm*] [**detail**]

IOS SLB によって管理されるすべての接続、または、オプションで特定の仮想サーバまたはクライアントに関連付けられた接続のみを表示します。次に、このコマンドのサンプル出力を示します。

```
Router# show ip slb conns

vserver          prot   client               real                 state
---------------------------------------------------------------------------
TEST             TCP    10.150.72.183:328    10.80.90.25:80       INIT
TEST             TCP    10.250.167.226:423   10.80.90.26:80       INIT
TEST             TCP    10.234.60.239:317    10.80.90.26:80       ESTAB
TEST             TCP    10.110.233.96:747     10.80.90.26:80       ESTAB
TEST             TCP    10.162.0.201:770      10.80.90.30:80       CLOSING
TEST             TCP    10.22.225.219:995     10.80.90.26:80       CLOSING
TEST             TCP    10.2.170.148:169      10.80.90.30:80
```

ステップ 2　**show ip slb dfp** [**agent** *agent-ip port* | **manager** *manager-ip* | **detail** | **weights**]

Dynamic Feedback Protocol（DFP）および DFP エージェントに関する情報、および実サーバに割り当てられた加重に関する情報を表示します。次に、このコマンドのサンプル出力を示します。

```
Router# show ip slb dfp

DFP Manager:
Current passwd:NONE Pending passwd:NONE
Passwd timeout:0 sec
```

```
Agent IP          Port    Timeout   Retry Count   Interval
-------------------------------------------------------------
172.16.2.34       61936   0         0             180 (Default)
```

ステップ 3 **show ip slb firewallfarm** [**detail**]

ファイアウォール ファームに関する情報を表示します。次に、このコマンドのサンプル出力を示します。

```
Router# show ip slb firewallfarm

firewall farm    hash        state         reals
-------------------------------------------------
FIRE1            IPADDR      OPERATIONAL     2
```

ステップ 4 **show ip slb fragments**

IOS SLB フラグメント データベースの情報を表示します。次に、このコマンドのサンプル出力を示します。

```
Router# show ip slb fragments

ip src          id    forward         src nat         dst nat
-----------------------------------------------------------------------
10.11.2.128     12    10.11.2.128     10.11.11.11     10.11.2.128
10.11.2.128     13    10.11.2.128     10.11.11.11     10.11.2.128
10.11.2.128     14    10.11.2.128     10.11.11.11     10.11.2.128
10.11.2.128     15    10.11.2.128     10.11.11.11     10.11.2.128
10.11.2.128     16    10.11.2.128     10.11.11.11     10.11.2.128
```

ステップ 5 **show ip slb gtp** {**gsn** [*gsn-ip-address*] | **nsapi** [*nsapi-key*] [**detail**]

IOS SLB GTP 情報を表示します。次に、このコマンドのサンプル出力を示します。

```
Router# show ip slb gtp gsn 10.0.0.0
type ip              recovery-ie  purging
-----------------------------------------
SGSN 10.0.0.0 UNKNOWN      N
```

ステップ 6 **show ip slb map** [*map-id*]

IOS SLB プロトコル マップに関する情報を表示します。次に、このコマンドのサンプル出力を示します。

```
Router# show ip slb map

ID: 1, Service: GTP
 APN: Cisco.com, yahoo.com
 PLMN ID(s): 11122, 444353
 SGSN access list: 100
ID: 2, Service: GTP
 PLMN ID(s): 67523, 345222
 PDP Type: IPv4, PPP
ID: 3, Service: GTP
 PDP Type: IPv6
ID: 4, Service: RADIUS
 Calling-station-id: "?919*"
ID: 5, Service: RADIUS
 Username: ". .778cisco.*"
```

ステップ 7 **show ip slb natpool** [**name** *pool*] [**detail**]

IOS SLB NAT 設定に関する情報を表示します。次に、このコマンドのサンプル出力を示します。

```
Router# show ip slb natpool

nat client B 209.165.200.225 1.1.1.6 1.1.1.8 Netmask 255.255.255.0
nat client A 10.1.1.1 1.1.1.5 Netmask 255.255.255.0
```

ステップ 8 **show ip slb probe** [**name** *probe*] [**detail**]

IOS SLB に対して定義されたプローブに関する情報を表示します。次に、このコマンドのサンプル出力を示します。

```
Router# show ip slb probe

Server:Port            State        Outages  Current  Cumulative
-----------------------------------------------------------------
10.10.4.1:0            OPERATIONAL        0  never    00:00:00
10.10.5.1:0            FAILED             1  00:00:06 00:00:06
```

ステップ 9 **show ip slb reals** [**sfarm** *server-farm*] [**detail**]

IOS SLB に対して定義された実サーバに関する情報を表示します。次に、このコマンドのサンプル出力を示します。

```
Router# show ip slb reals

real             farm name        weight   state           conns
-------------------------------------------------------------------
10.80.2.112      FRAG             8        OUTOFSERVICE    0
10.80.5.232      FRAG             8        OPERATIONAL     0
10.80.15.124     FRAG             8        OUTOFSERVICE    0
10.254.2.2       FRAG             8        OUTOFSERVICE    0
10.80.15.124     LINUX            8        OPERATIONAL     0
10.80.15.125     LINUX            8        OPERATIONAL     0
10.80.15.126     LINUX            8        OPERATIONAL     0
10.80.90.25      SRE              8        OPERATIONAL     220
10.80.90.26      SRE              8        OPERATIONAL     216
10.80.90.27      SRE              8        OPERATIONAL     216
10.80.90.28      SRE              8        TESTING         1
10.80.90.29      SRE              8        OPERATIONAL     221
10.80.90.30      SRE              8        OPERATIONAL     224
10.80.30.3       TEST             100      READY_TO_TEST   0
10.80.30.4       TEST             100      READY_TO_TEST   0
10.80.30.5       TEST             100      READY_TO_TEST   0
10.80.30.6       TEST             100      READY_TO_TEST   0
```

ステップ 10 **show ip slb replicate**

IOS SLB 複製設定に関する情報を表示します。次に、このコマンドのサンプル出力を示します。

```
Router# show ip slb replicate

VS1, state = NORMAL, interval = 10
 Slave Replication: Enabled
 Slave Replication statistics:
  unsent conn updates:         0
  conn updates received:       0
  conn updates transmitted:    0
  update messages received:    0
  update messages transmitted: 0
 Casa Replication:
  local = 10.1.1.1 remote = 10.2.2.2 port = 1024
  current password = <none> pending password = <none>
  password timeout = 180 sec (Default)
 Casa Replication statistics:
  unsent conn updates:        0
  conn updates received:      0
  conn updates transmitted:   0
  update packets received:    0
  update packets transmitted: 0
  failovers:                  0
```

ステップ 11　show ip slb serverfarms [**name** *server-farm*] [**detail**]

IOS SLB に対して定義された実サーバ ファームに関する情報を表示します。次に、このコマンドのサンプル出力を示します。

```
Router# show ip slb serverfarms

server farm      predictor     reals   bind id
-----------------------------------------------
FRAG             ROUNDROBIN    4       0
LINUX            ROUNDROBIN    3       0
SRE              ROUNDROBIN    6       0
TEST             ROUNDROBIN    4       0
```

ステップ 12　show ip slb sessions [**asn** | **gtp** [**ipv6**] | **gtp-inspect** | **ipmobile** | **radius**] [**vserver** *virtual-server*] [**client** *ipv4-address netmask*] [**detail**]

IOS SLB によって管理されるセッションに関する情報を表示します。次に、このコマンドのサンプル出力を示します。

```
Router# show ip slb sessions radius

Source               Dest                   Retry
Addr/Port            Addr/Port           Id Count  Real            Vserver
-------------------------------------------------------------------------------
10.10.11.1/1645      10.10.11.2/1812     15     1  10.10.10.1  RADIUS_ACCT
```

ステップ 13　show ip slb static

IOS SLB サーバの NAT 設定に関する情報を表示します。次に、このコマンドのサンプル出力を示します。

```
Router# show ip slb static

real                     action         address         counter
-----------------------------------------------------------------
10.11.3.4                drop           0.0.0.0         0
10.11.3.1                NAT            10.11.11.11     3
10.11.3.2                NAT sticky     10.11.11.12     0
10.11.3.3                NAT per-packet 10.11.11.13     0
```

ステップ 14　show ip slb stats

IOS SLB 統計情報を表示します。次に、このコマンドのサンプル出力を示します。

```
Router# show ip slb stats

Pkts via normal switching:     779
Pkts via special switching:    0
Pkts via slb routing:          0
Pkts Dropped:                  4
Connections Created:           4
Connections Established:       4
Connections Destroyed:         4
Connections Reassigned:        5
Zombie Count:                  0
Connections Reused:            0
Connection Flowcache Purges:   0
Failed Connection Allocs:      0
Failed Real Assignments:       0
RADIUS Framed-IP Sticky Count: 0
RADIUS username Sticky Count:            0
RADIUS calling-station-id Sticky Count:  0
GTP IMSI Sticky Count:         0
Failed Correlation Injects:    0
Pkt fragments drops in ssv:    0
```

```
ASN MSID sticky count:         1
```

ステップ 15 **show ip slb sticky** [**client** *ip-address netmask* | **radius calling-station-id** [**id** *string*] | **radius framed-ip** [**client** *ip-address netmask*] | **radius username** [**name** *string*]]

IOS SLB に対して定義されたスティッキ接続に関する情報を表示します。次に、このコマンドのサンプル出力を示します。

```
Router# show ip slb sticky
client           netmask          group  real                  conns
-------------------------------------------------------------------------
10.10.2.12       255.255.0.0      4097   10.10.3.2             1
```

ステップ 16 **show ip slb vservers** [**name** *virtual-server*] [**redirect**] [**detail**]

IOS SLB に対して定義された仮想サーバに関する情報を表示します。次に、このコマンドのサンプル出力を示します。

```
Router# show ip slb vservers

slb vserver      prot   virtual               state          conns
-----------------------------------------------------------------------
TEST             TCP     10.80.254.3:80        OPERATIONAL    1013
TEST21           TCP     10.80.254.3:21        OUTOFSERVICE   0
TEST23           TCP     10.80.254.3:23        OUTOFSERVICE   0
```

ステップ 17 **show ip slb wildcard**

IOS SLB に対して定義された仮想サーバのワイルドカード表現に関する情報を表示します。次に、このコマンドのサンプル出力を示します。

```
Router# show ip slb wildcard

Interface Source Address         Port  Destination Address    Port  Prot
ANY       0.0.0.0/0              0     3.3.3.3/32             2123  UDP
ANY       0.0.0.0/0              0     3.3.3.3/32             0     UDP
ANY       0.0.0.0/0              0     0.0.0.0/0              0     ICMP

Interface: ANY
Source Address [Port]: ::/0[0]
Destination Address [Port]: 2342:2342:2343:FF04:2341:AA03:2323:8912/128[0]
Protocol: ICMPV6

Interface: ANY
Source Address [Port]: ::/0[0]
Destination Address [Port]: 2342:2342:2343:FF04:2341:AA03:2323:8912/128[2123]
Protocol: UDP
```

IOS SLB の設定例

ここでは、IOS SLB の使用例を紹介します。この項の IOS SLB コマンドの詳細な説明については、『*Cisco IOS IP Application Services Command Reference*』を参照してください。この項に記載されている他のコマンドのマニュアルについては、Cisco.com でオンライン検索してください。

ここでは、次の設定例について説明します。

- 「例：基本的な IOS SLB ネットワークの設定方法」（P.121）
- 「例：包括的な IOS SLB ネットワークの設定方法」（P.123）
- 「例：ファイアウォール ロード バランシングを使用した IOS SLB の設定方法」（P.124）
- 「例：プローブを使用した IOS SLB の設定方法」（P.132）

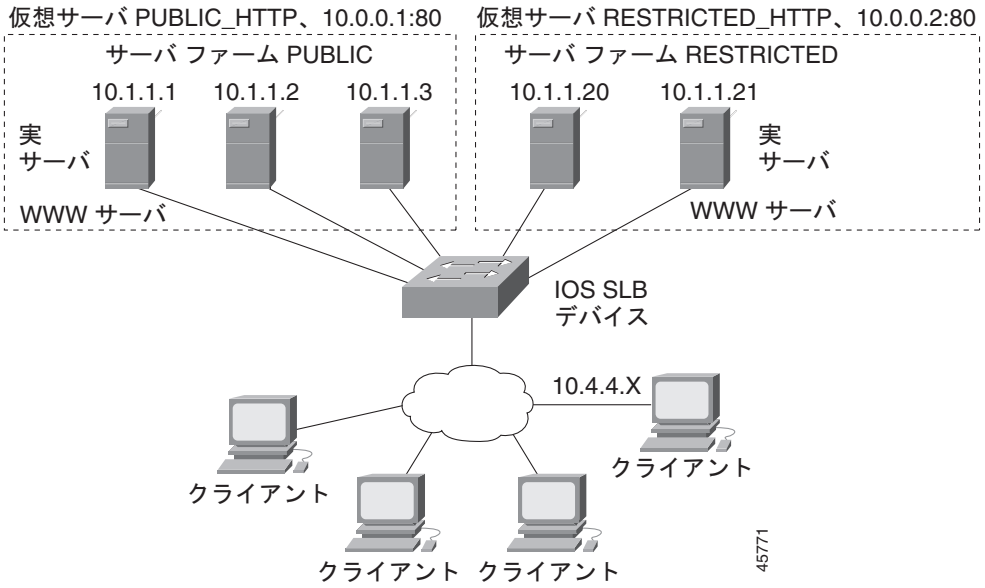
（注） 例に使用される IP アドレスおよびネットワーク アドレスは一般的なものです。実際のネットワークのアドレスで置き換えてください。

例：基本的な IOS SLB ネットワークの設定方法

図 2 に、次のコンポーネントを使用した IOS SLB ネットワークの例を示します。

- 2 つのサーバ ファーム：1 つはパブリック アクセスを許可するように設定し、PUBLIC という名前をつけ、もう 1 つはアクセスを限定的になるように設定し、RESTRICTED という名前をつけます。
- 5 つの実サーバは次のように設定します。
  - PUBLIC サーバ ファームの 3 つの実サーバには、IP アドレス 10.1.1.1、10.1.1.2、および 10.1.1.3 を設定します。
  - RESTRICTED サーバ ファームの 2 つの実サーバには､IP アドレス 10.1.1.20 および 10.1.1.21 を設定します。
- 2 つの仮想サーバ：1 つはパブリック アクセスを許可するように設定し、PUBLIC_HTTP という名前をつけ、もう 1 つはアクセスを限定的になるように設定し、RESTRICTED_HTTP という名前をつけます。
  - 仮想サーバ PUBLIC_HTTP は、IP アドレス 10.0.0.1、ロード バランシング TCP 接続 WWW ポート（80）と設定します。
  - 仮想サーバ RESTRICTED_HTTP は、IP アドレス 10.0.0.2、ロード バランシング TCP 接続 WWW ポート（80）と設定します。また、ネットワーク 10.4.4.0 255.255.255.0 のクライアントからのアクセスだけを許可します。

図 2　　IOS SLB ネットワークの例



次の項では、図 2 に示す IOS SLB ネットワークの設定および確認に使用するコンフィギュレーション コマンドの例を紹介します。

- 「サーバ ファームの設定」（P.122）
- 「仮想サーバの設定」（P.123）
- 「限定されたクライアントの設定」（P.123）

サーバ ファームの設定

次に、3 つの実サーバに関連付けられたサーバ ファーム PUBLIC の設定例を示します。

```
ip slb serverfarm PUBLIC
  real 10.1.1.1
    reassign 2
    faildetect numconns 4 numclients 2
    retry 20
    inservice
    exit
  real 10.1.1.2
    reassign 2
    faildetect numconns 4
    retry 20
    inservice
    exit
  real 10.1.1.3
    reassign 2
    faildetect numconns 4
    retry 20
    inservice
    end
```

次に、2 つの実サーバに関連付けられたサーバ ファーム RESTRICTED の設定例を示します。

```
ip slb serverfarm RESTRICTED
  real 10.1.1.20
    reassign 2
```

```
    faildetect numconns 4
    retry 20
    inservice
    exit
  real 10.1.1.21
    reassign 2
    faildetect numconns 4
    retry 20
    inservice
    end
```

仮想サーバの設定

次に、仮想サーバ PUBLIC_HTTP および RESTRICTED_HTTP の設定例を示します。

```
ip slb vserver PUBLIC_HTTP
  virtual 10.0.0.1 tcp www
  serverfarm PUBLIC
  idle 120
  delay 5
  inservice
  exit
ip slb vserver RESTRICTED_HTTP
  virtual 10.0.0.2 tcp www
  serverfarm RESTRICTED
  idle 120
  delay 5
  inservice
  end
```

限定されたクライアントの設定

次に、仮想サーバ RESTRICTED_HTTP の設定例を示します。

```
ip slb vserver RESTRICTED_HTTP
  no inservice
  client 10.4.4.0 255.255.255.0
  inservice
  end
```

例：包括的な IOS SLB ネットワークの設定方法

次に、この機能マニュアルで説明しているコマンドの多数を使用した設定例の一式を示します。

```
ip slb probe PROBE2 http
 request method POST url /probe.cgi?all
 header HeaderName HeaderValue
!
ip slb serverfarm PUBLIC
 nat server
 real 10.1.1.1
  reassign 4
  faildetect numconns 16
  retry 120
  inservice
 real 10.1.1.2
  reassign 4
  faildetect numconns 16
  retry 120
  inservice
```

```
probe PROBE2
!
ip slb serverfarm RESTRICTED
 predictor leastconns
 bindid 309
 real 10.1.1.1
  weight 32
  maxconns 1000
  reassign 4
  faildetect numconns 16
  retry 120
  inservice
 real 10.1.1.20
  reassign 4
  faildetect numconns 16
  retry 120
  inservice
 real 10.1.1.21
  reassign 4
  faildetect numconns 16
  retry 120
  inservice
!
ip slb vserver PUBLIC_HTTP
 virtual 10.0.0.1 tcp www
 serverfarm PUBLIC
!
ip slb vserver RESTRICTED_HTTP
 virtual 10.0.0.2 tcp www
 serverfarm RESTRICTED
 no advertise
 sticky 60 group 1
 idle 120
 delay 5
 client 10.4.4.0 255.255.255.0
 synguard 3600000
 inservice
```

例：ファイアウォール ロード バランシングを使用した IOS SLB の設定方法

ここでは次の例を紹介し、さまざまな IOS SLB ファイアウォール ロード バランシング設定を示します。

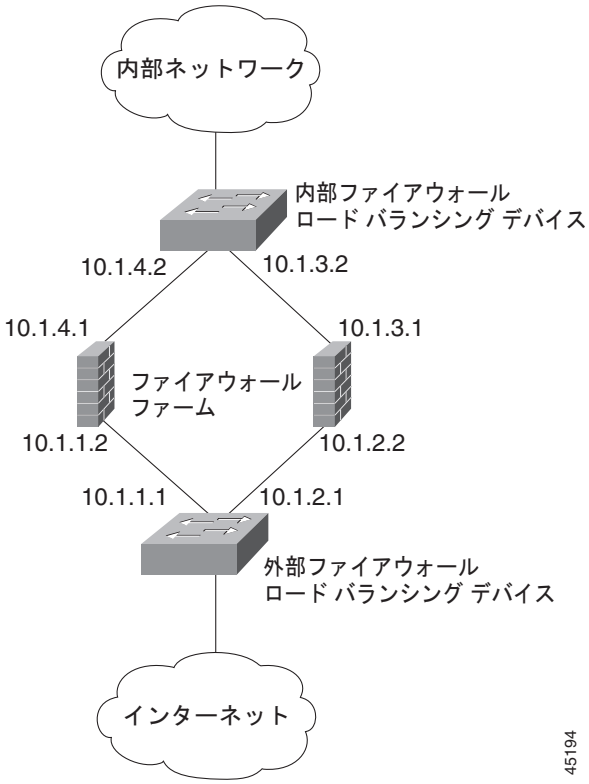
- 「例：基本的なファイアウォール ロード バランシングを使用した IOS SLB の設定方法」（P.125）
- 「例：サーバ ロード バランシングとファイアウォール ロード バランシングを使用した IOS SLB の設定方法」（P.127）
- 「例：複数のファイアウォール ファームを使用した IOS SLB の設定方法」（P.129）
- 「例：二重ファイアウォール ロード バランシング「サンドイッチ」を使用した IOS SLB の設定方法」（P.130）
- 「例：RADIUS ロード バランシング/ファイアウォール ロード バランシング「サンドイッチ」を使用した IOS SLB の設定方法」（P.180）

例：基本的なファイアウォール ロード バランシングを使用した IOS SLB の設定方法

図 3 に、次のコンポーネントを使用した IOS SLB ファイアウォール ロード バランシング ネットワークの例を示します。

- 図のように IP アドレスを指定した 2 つのファイアウォール
- ファイアウォールのセキュア側に内部ファイアウォール ロード バランシング デバイス
- ファイアウォールのインターネット側に外部ファイアウォール ロード バランシング デバイス
- 両方のファイアウォールを含む、FIRE1 という 1 つのファイアウォール ファーム

図 3　別のサブネット内のレイヤ 3 ファイアウォールを使用した IOS SLB



IOS SLB ファイアウォール ロード バランシングを設定する場合、ロード バランシング デバイスでは、そのファイアウォール宛てのフローを認識するためにルート検索が使用されます。ルート検索をイネーブルにするには、そのデバイスにフローをルーティングする各ファイアウォールの IP アドレスを使用して、各デバイスを設定する必要があります。

次のファイアウォール ファーム設定例の場合：

- 内部（セキュア側）のファイアウォール ロード バランシング デバイスは、ファイアウォール IP アドレス 10.1.3.1 および 10.1.4.1 を使用して設定します。
- 外部（インターネット側）のファイアウォール ロード バランシング デバイスは、ファイアウォール IP アドレス 10.1.1.2 および 10.1.2.2 を使用して設定します。

内部ファイアウォール ロード バランシング デバイス

次に、ping プローブ PROBE1、HTTP プローブ PROBE2、およびファイアウォール ファーム FIRE1 の設定例を示します。これらは、ファイアウォールの内部（セキュア側）にあるロード バランシング デバイスの 2 つの実サーバに関連付けられています。

```
!-----Ping probe
ip slb probe PROBE1 ping
!-----IP address of other load-balancing device
  address 10.1.1.1
  faildetect 4
!-----HTTP probe
  ip slb probe PROBE2 http
!-----IP address of other load-balancing device
  address 10.1.2.1
  expect status 401
!-----Firewall farm FIRE1
ip slb firewallfarm FIRE1
!-----First firewall
  real 10.1.4.1
    probe PROBE1
!-----Enable first firewall
    inservice
!-----Second firewall
    real 10.1.3.1
    probe PROBE2
!-----Enable second firewall
    inservice
```

外部ファイアウォール ロード バランシング デバイス

次に、ping プローブ PROBE1、HTTP プローブ PROBE2、およびファイアウォール ファーム FIRE1 の設定例を示します。これらは、ファイアウォールの外部（インターネット側）にあるロード バランシング デバイスの 2 つの実サーバに関連付けられています。

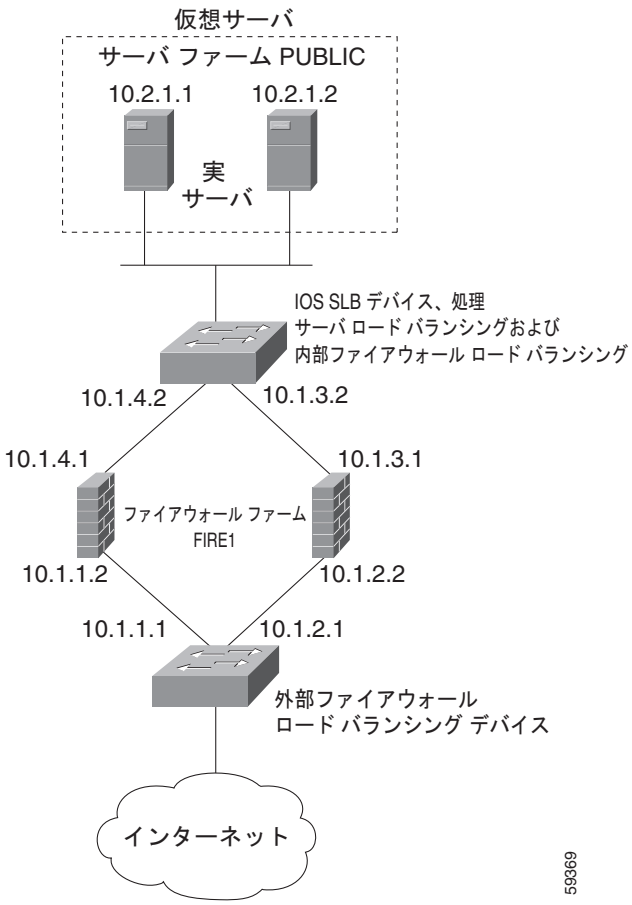
```
!-----Ping probe
ip slb probe PROBE1 ping
!-----IP address of other load-balancing device
  address 10.1.4.2
  faildetect 4
!-----HTTP probe
ip slb probe PROBE2 http
!-----IP address of other load-balancing device
  address 10.1.3.2
  expect status 401
!-----Firewall farm FIRE1
ip slb firewallfarm FIRE1
!-----First firewall
  real 10.1.1.2
    probe PROBE1
!-----Enable first firewall
    inservice

!-----Second firewall
  real 10.1.2.2
    probe PROBE2
!-----Enable second firewall
    inservice
    exit
  inservice
```

例：サーバ ロード バランシングとファイアウォール ロード バランシングを使用した IOS SLB の設定方法

図 4 に、サーバ ロード バランシングおよびファイアウォール ロード バランシングの両方と、次のコンポーネントを使用する IOS SLB ロード バランシング ネットワークの例を示します。

- 図のように IP アドレスを指定した 2 つの実サーバ
- 両方の実サーバを含む、PUBLIC という 1 つのサーバ ファーム
- 図のように IP アドレスを指定した 2 つのファイアウォール
- 両方のファイアウォールを含む、FIRE1 という 1 つのファイアウォール ファーム
- サーバ ロード バランシングおよびファイアウォール ロード バランシングを実行する、ファイアウォールのセキュア側にある内部 IOS SLB デバイス
- ファイアウォールのインターネット側にある、外部ファイアウォール ロード バランシング デバイス

図 4　サーバ ロード バランシングとファイアウォール ロード バランシングを使用した IOS SLB



次のファイアウォール ファーム設定例の場合：

- 内部（セキュア側）のファイアウォール ロード バランシング デバイスは、ファイアウォール IP アドレス 10.1.3.1 および 10.1.4.1 を使用して設定します。

- 外部（インターネット側）のファイアウォール ロード バランシング デバイスは、ファイアウォール IP アドレス 10.1.1.2 および 10.1.2.2 を使用して設定します。

内部サーバおよびファイアウォール ロード バランシング デバイス

次に、ファイアウォールの内部（セキュア側）にあるロード バランシング デバイスの ping プローブ ABCPROBE および XYZPROBE、ファイアウォール ファーム FIRE1、およびサーバ ファーム PUBLIC の設定例を示します。

```
ip slb probe ABCPROBE ping
  address 10.1.1.1
ip slb probe XYZPROBE ping
  address 10.1.2.1
!
ip slb firewallfarm FIRE1
  real 10.1.4.1
    probe ABCPROBE
    inservice
  real 10.1.3.1
    probe XYZPROBE
    inservice
  inservice
!
ip slb serverfarm PUBLIC
  nat server
  real 10.2.1.1
    inservice
    real 10.2.1.2
    inservice
!
ip slb vserver HTTP1
  virtual 128.1.0.1 tcp www
  serverfarm PUBLIC
  idle 120
  delay 5
  inservice
```

（注） Cisco Catalyst 6500 シリーズ スイッチ上では、グローバル コンフィギュレーション モードで **mls ip slb search wildcard rp** コマンドを使用して、IOS SLB ワイルドカード検索がルート プロセッサによって実行されるように指定することもできます。

外部ファイアウォール ロード バランシング デバイス

次に、ファイアウォールの外部（インターネット側）にあるロード バランシング デバイスの ping プローブ ABCPROBE および XYZPROBE、およびファイアウォール ファーム FIRE1 の設定例を示します。

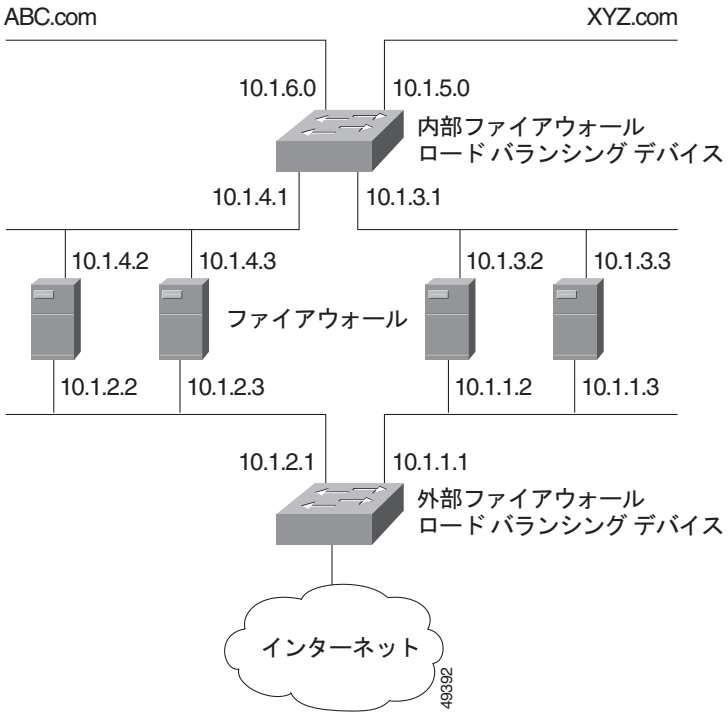
```
ip slb probe ABCPROBE ping
  address 10.1.4.2
  ip slb probe XYZPROBE ping
  address 10.1.3.2
  ip slb firewallfarm FIRE1
  real 10.1.1.2
    probe ABCPROBE
    inservice
    probe XYZPROBE
    inservice
```

例：複数のファイアウォール ファームを使用した IOS SLB の設定方法

図 5 に、複数のファイアウォール ファームと次のコンポーネントを使用した IOS SLB ファイアウォール ロード バランシング ネットワークの例を示します。

- 図のように IP アドレスを指定した 4 つのファイアウォール
- ファイアウォールのセキュア側にある、内部ファイアウォール ロード バランシング デバイス
- ファイアウォールのインターネット側にある、外部ファイアウォール ロード バランシング デバイス
- 左側に 2 つのファイアウォールを含む ABCFARM という 1 つのファイアウォール ファーム
- 右側に 2 つのファイアウォールを含む XYZFARM という 1 つのファイアウォール ファーム

図 5　　複数のファイアウォール ファームを使用した IOS SLB



次のファイアウォール ファーム設定例の場合：

- 内部（セキュア側）のファイアウォール ロード バランシング デバイスは、ファイアウォール IP アドレス 10.1.3.1 および 10.1.4.1 を使用して設定します。
- 外部（インターネット側）のファイアウォール ロード バランシング デバイスは、ファイアウォール IP アドレス 10.1.1.2 および 10.1.2.2 を使用して設定します。

内部ファイアウォール ロード バランシング デバイス

次に、ファイアウォールの内部（セキュア側）にあるロード バランシング デバイスの ping プローブ ABCPROBE および XYZPROBE、およびファイアウォール ファーム ABCFARM および XYZFARM の設定例を示します。

```
ip slb probe ABCPROBE ping
  address 10.1.2.1
ip slb probe XYZPROBE ping
```

```
  address 10.1.1.1
ip slb firewallfarm ABCFARM
  access source 10.1.6.0 255.255.255.0
  inservice
  real 10.1.4.2
    probe ABCPROBE
    inservice
  real 10.1.4.3
    probe ABCPROBE
    inservice
ip slb firewallfarm XYZFARM
  access source 10.1.5.0 255.255.255.0
  inservice
  real 10.1.3.2
    probe XYZPROBE
    inservice
  real 10.1.3.3
    probe XYZPROBE
    inservice
```

外部ファイアウォール ロード バランシング デバイス

次に、ファイアウォールの外部（インターネット側）にあるロード バランシング デバイスの ping プローブ ABCPROBE および XYZPROBE、およびファイアウォール ファーム ABCFARM および XYZFARM の設定例を示します。

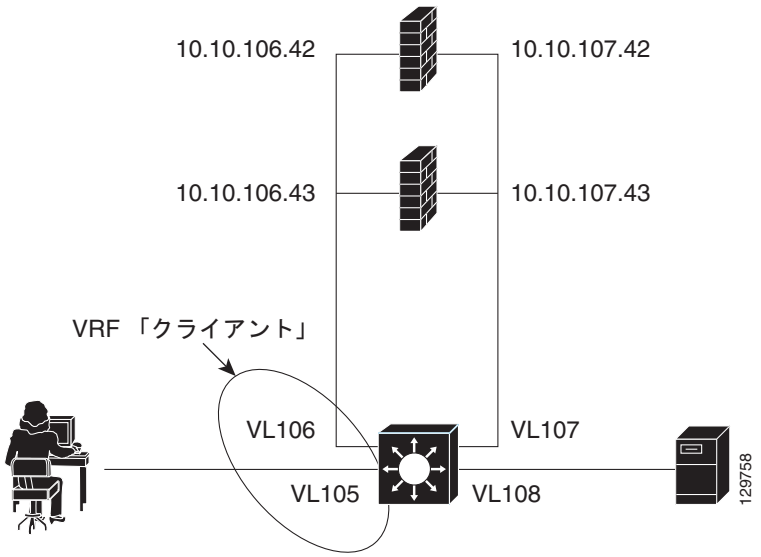
```
ip slb probe ABCPROBE ping
  address 10.1.4.1
ip slb probe XYZPROBE ping
  address 10.1.3.1
ip slb firewallfarm ABCFARM
  access destination 10.1.6.0 255.255.255.0
  inservice
  real 10.1.2.2
    probe ABCPROBE
    inservice
  real 10.1.2.3
    probe ABCPROBE
    inservice
ip slb firewallfarm XYZFARM
  access destination 10.1.5.0 255.255.255.0
  inservice
  real 10.1.1.2
    probe XYZPROBE
    inservice
  real 10.1.1.3
    probe XYZPROBE
    inservice
```

例：二重ファイアウォール ロード バランシング「サンドイッチ」を使用した IOS SLB の設定方法

図 6 に、1 台の IOS SLB デバイス上でホストされる基本的な二重ファイアウォール ロード バランシング「サンドイッチ」を示します。これには、VRF とアクセス インターフェイスの設定が含まれています。VL105、VL106、VL107、および VL108 は VLAN です。

（注） この設定のクライアントとサーバは直接接続されています。より一般的な展開では、VRF の内側と外側に追加のルータが必要です。

図 6　二重ファイアウォール ロード バランシング「サンドイッチ」を使用した IOS SLB



次に、図 6 の設定の IOS SLB 設定文を示します。

```
ip vrf client
 rd 0:1
!
ip slb probe P642 ping
 address 10.10.106.42
 interval 120
ip slb probe P643 ping
 address 10.10.106.43
 interval 120
ip slb probe P742 ping
 address 10.10.107.42
 interval 120
ip slb probe P743 ping
 address 10.10.107.43
 interval 120
!
ip slb firewallfarm CLIENT
 access inbound Vlan105
 access outbound Vlan106
 no inservice
!
 real 10.10.106.42
  probe P642
  inservice
 real 10.10.106.43
  probe P643
  inservice
 protocol tcp
  sticky 180 source
 protocol datagram
  sticky 180 source
 predictor hash address port
!
ip slb firewallfarm SERVER
 access inbound Vlan108
 access outbound Vlan107
 inservice
!
```

```
 real 10.10.107.42
  probe P742
  inservice
 real 10.10.107.43
  probe P743
  inservice
 protocol tcp
  sticky 180 destination
 protocol datagram
  sticky 180 destination
 predictor hash address port
!
mls flow ip interface-full
!
!************************************************
!* Switchports, port channels and trunks         *
!* added to vlans 105-108 (left out for brevity) *
!************************************************
!
interface Vlan105
 ip vrf forwarding client
 ip address 10.10.105.2 255.255.255.0
!
interface Vlan106
 ip vrf forwarding client
 ip address 10.10.106.2 255.255.255.0
!
interface Vlan107
 ip address 10.10.107.2 255.255.255.0
!
interface Vlan108
 ip address 10.10.108.2 255.255.255.0
!
ip route 10.10.105.0 255.255.255.0 10.10.107.42
ip route vrf client 10.10.108.0 255.255.255.0 10.10.106.42
```

例：プローブを使用した IOS SLB の設定方法

ここでは次の例を紹介し、さまざまな IOS SLB プローブ設定を示します。

- 「例：ping と HTTP プローブを使用した IOS SLB の設定方法」（P.132）
- 「例：ルーテッド プローブを使用した IOS SLB の設定方法」（P.134）

例：ping と HTTP プローブを使用した IOS SLB の設定方法

図 7 に、サーバ ファームの一部として設定された IOS SLB 実サーバ接続を含む設定例を示します。サーバ負荷分散されたアプリケーションの ping と HTTP プローブを使用したモニタに焦点が当てられています。

図 7　ping プローブおよび HTTP プローブ トポロジの例

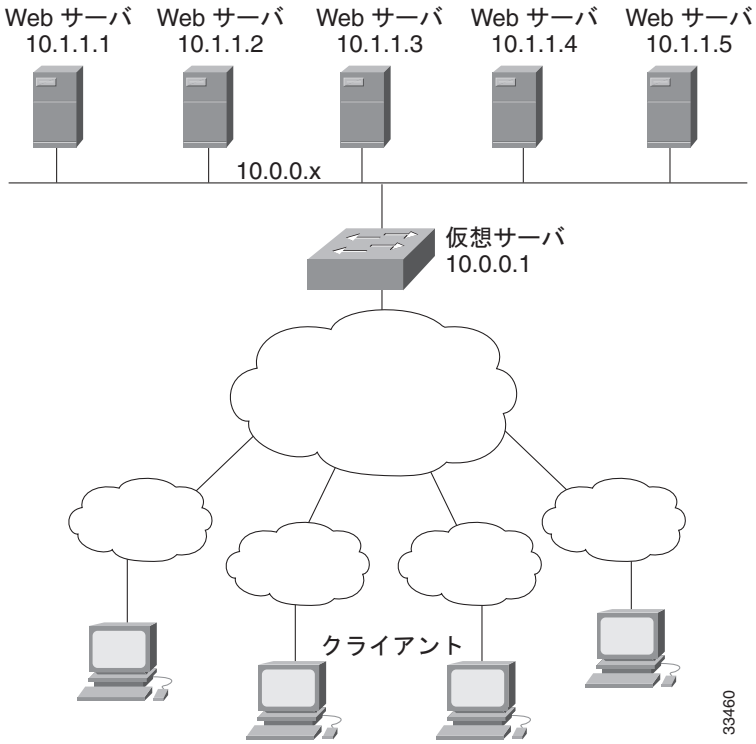


図 7 に示すトポロジは、1 つの仮想サーバにサービスを提供する異機種混合サーバ ファームです。次に、このトポロジの設定文を示します。トポロジには、PROBE1 という ping プローブと PROBE2 という HTTP プローブがあります。

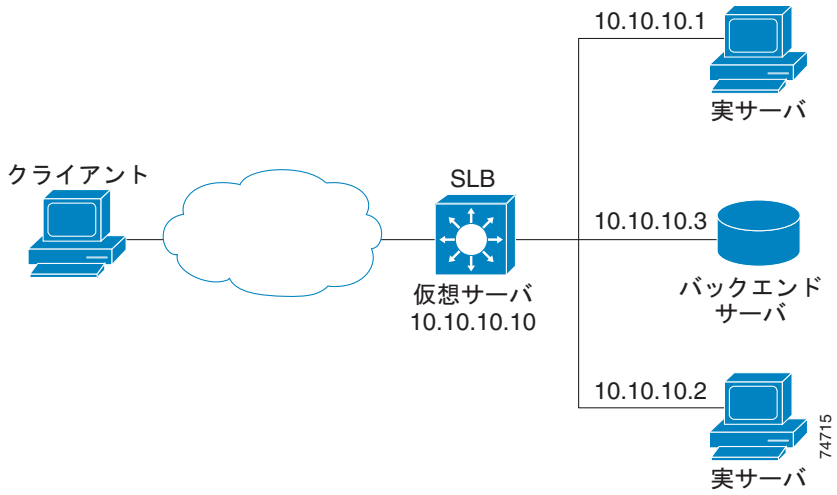
```
! Configure ping probe PROBE1, change CLI to IOS SLB probe configuration mode
ip slb probe PROBE1 ping
! Configure probe to receive responses from IP address 13.13.13.13
  address 13.13.13.13
! Configure unacknowledged ping threshold to 16
  faildetect 16
! Configure ping probe timer interval to send every 11 seconds
  interval 11
! Configure HTTP probe PROBE2
  ip slb probe PROBE2 http
! Configure request method as POST, set URL as /probe.cgi?all
  request method post url /probe.cgi?all
! Configure header HeaderName
  header HeaderName HeaderValue
! Configure basic authentication username and password
  credentials Semisweet chips
! Exit to global configuration mode
  exit
! Enter server farm configuration mode for server farm PUBLIC
ip slb serverfarm PUBLIC
! Configure NAT server and real servers on the server farm
  nat server
  real 10.1.1.1
   inservice
  real 10.1.1.2
   inservice
  real 10.1.1.3
   inservice
  real 10.1.1.4
```

```
   inservice
  real 10.1.1.5
   inservice
! Configure ping probe on the server farm
  probe PROBE1
! Configure HTTP probe on the server farm
  probe PROBE2
  end
```

例：ルーテッド プローブを使用した IOS SLB の設定方法

図 8 に、一般的なデータセンターと IOS SLB の設定を示します。仮想サーバ ACME_VSERVER は、サーバ ファーム ACME_FARM の 2 つの実サーバ（10.10.10.1 と 10.10.10.2）を使用して設定されています。ユーザは、バックエンド サーバ（10.10.10.3）の動作状況に基づいて、実サーバに障害が発生していると見なすことを希望しています。実サーバ経由でヘルス チェックを送信せずにこの設定を実現するには、BACKEND、つまり、バックエンド サーバの IP アドレスへのルーテッド ping プローブを定義します。

図 8　　ルーテッド ping プローブを使用した IOS SLB



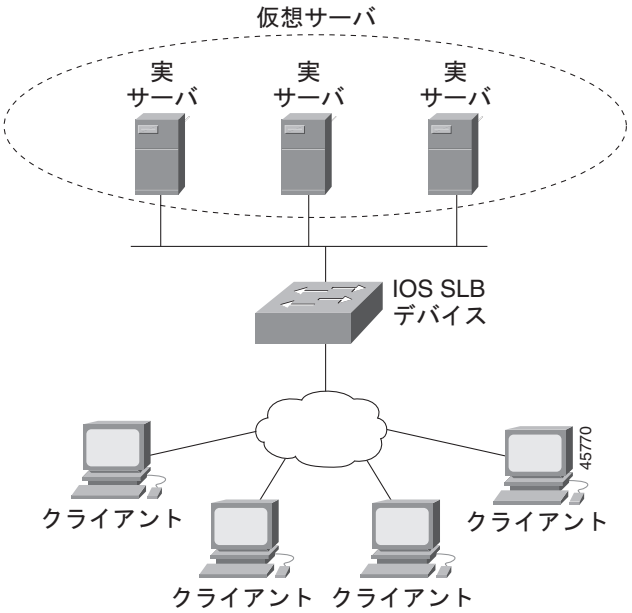
次に、図 8 の設定の IOS SLB 設定文を示します。

```
ip slb probe BACKEND ping
  address 10.10.10.3 routed

ip slb serverfarm ACME_SFARM
  nat server
  probe BACKEND
  real 10.10.10.1
   inservice
  real 10.10.10.2
   inservice
ip slb vserver ACME_VSERVER
  virtual 10.10.10.10 tcp 80
  serverfarm ACME_SFARM
  inservice
```

例：IOS SLB を備えたレイヤ 3 スイッチの設定方法

図 9 に、サーバ ファームの一部として設定した IOS SLB サーバ接続の設定例を示します。

図 9　　IOS SLB のネットワーク設定



次の設定例に示すように、このトポロジ例には 3 つのパブリック Web サーバと、サブネット 10.4.4.0 の権限を持つクライアントに限定された 2 つの Web サーバがあります。パブリック Web サーバは容量に応じて加重が設定され、サーバ 10.1.1.2 は最も容量が低く、接続が制限されています。制限付きの Web サーバは、同じスティッキ グループのメンバとして設定されているため、同じクライアントの HTTP 設定と Secure Socket Layer（SSL）接続は、同じ実サーバを使用します。

前述した IOS SLB 機能を備えるネットワーク設定は、次のとおりです。

```
ip slb probe PROBE2 http
  request method POST url /probe.cgi?all
  header HeaderName HeaderValue
  header Authorization Basic U2VtaXN3ZWV0OmNoaXBz
!
ip slb serverfarm PUBLIC
  nat server
  predictor leastconns
! First real server
  real 10.1.1.1
    reassign 4
    faildetect numconns 16
    retry 120
    inservice
! Second real server
  real 10.1.1.2
    reassign 4
    faildetect numconns 16
    retry 120
    inservice
! Third real server
  real 10.1.1.3
    reassign 4
    faildetect numconns 16
```

```
    retry 120
    inservice
! Probe
  probe PROBE2
! Restricted web server farm
ip slb serverfarm RESTRICTED
  predictor leastconns
! First real server
  real 10.1.1.20
    reassign 2
    faildetect numconns 4
    retry 20
    inservice
! Second real server
  real 10.1.1.21
    reassign 2
    faildetect numconns 4
    retry 20
    inservice
!
! Unrestricted web virtual server
ip slb vserver PUBLIC_HTTP
  virtual 10.0.0.1 tcp www
  serverfarm PUBLIC
  idle 120
  delay 5
  inservice
!
! Restricted HTTP virtual server
ip slb vserver RESTRICTED_HTTP
  virtual 10.0.0.1 tcp www
  serverfarm RESTRICTED
  client 10.4.4.0 255.255.255.0
  sticky 60 group 1
  idle 120
  delay 5
  inservice
!
! Restricted SSL virtual server
ip slb vserver RESTRICTED_SSL
  virtual 10.0.0.1 tcp https
  serverfarm RESTRICTED
  client 10.4.4.0 255.255.255.0
  sticky 60 group 1
  idle 120
  delay 5
  inservice
!
interface GigabitEthernet1/1
  switchport
  switchport access vlan 3
  switchport mode access
  no ip address
!
interface FastEthernet2/1
  switchport
  switchport access vlan 2
  switchport mode access
  no ip address
!
interface FastEthernet2/2
  switchport
  switchport access vlan 2
  switchport mode access
```

```
  no ip address
!
interface FastEthernet2/3
  switchport
  switchport access vlan 2
  switchport mode access
  no ip address
!
interface Vlan2
  ip address 10.1.1.100 255.255.255.0
!
interface Vlan3
  ip address 40.40.40.1 255.255.255.0
```

例：NAT とスタティック NAT を使用した IOS SLB の設定方法

ここでは次の例を紹介し、さまざまな IOS SLB NAT 設定を示します。

- 「例：NAT を使用した IOS SLB の設定方法」（P.137）
- 「例：スタティック NAT を使用した IOS SLB の設定方法」（P.140）
- 「例：GPRS ロード バランシングと NAT を使用した IOS SLB の設定方法」（P.168）
- 「例：GPRS ロード バランシング、NAT、および GTP Cause Code Inspection を使用した IOS SLB の設定方法」（P.171）

例：NAT を使用した IOS SLB の設定方法

図 10 に、サーバ ファームの一部として IOS SLB 実サーバ接続を設定した例を示します。NAT サーバおよびクライアントのアドレス プールの設定を中心に説明します。

図 10　IOS SLB NAT トポロジの例

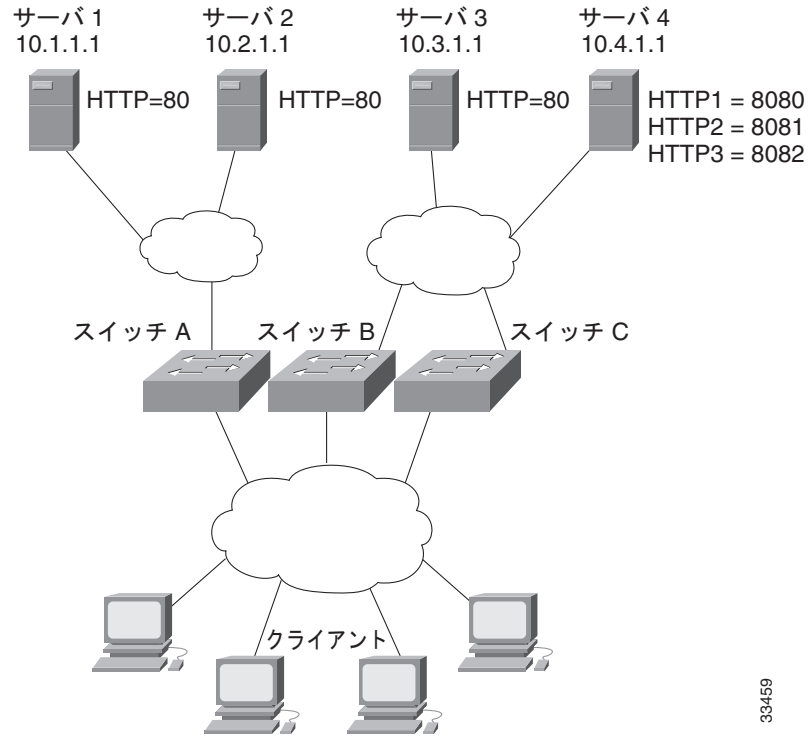


図 10 のトポロジには 4 つの Web サーバがあり、次のように設定されています。

- サーバ 1、2、および 3 は、ポート 80 をリスンする HTTP サーバ アプリケーションを実行しています。
- サーバ 4 には、ポート 8080、8081、および 8082 をリスンする複数の HTTP サーバ アプリケーションがあります。

サーバ 1 とサーバ 2 は、スイッチ A を使用して負荷が分散されます。スイッチ A はサーバ アドレス変換を実行します。

サーバ 3 とサーバ 4 は、スイッチ B とスイッチ C を使用して負荷が分散されます。これら 2 つのスイッチは、クライアントとサーバ間に複数のパスがあるため、サーバ アドレスとクライアント アドレス両方の変換を実行します。また、これらのスイッチでは、HTTP パケットとサーバ 4 の間でサーバ ポートの変換を実行する必要があります。

スイッチ A の設定文

```
ip slb serverfarm FARM1
! Translate server addresses
  nat server
! Server 1 port 80
  real 10.1.1.1
    reassign 2
    faildetect numconns 4 numclients 2
    retry 20
    inservice
! Server 2 port 80
  real 10.2.1.1
    reassign 2
    faildetect numconns 4
    retry 20
```

```
    inservice
!
ip slb vserver HTTP1
! Manage HTTP (port 80) requests
  virtual 128.1.0.1 tcp www
  serverfarm FARM1
  idle 120
  delay 5
  inservice
```

スイッチ B の設定文

```
ip slb natpool web-clients 128.3.0.1 128.3.0.254
! NAT address pool for clients
ip slb serverfarm FARM2
! Translate server addresses
  nat server
! Translate client addresses
  nat client web-clients
! Server 3 port 80
  real 10.3.1.1
    reassign 2
    faildetect numconns 4
    retry 20
    inservice
! Server 4 port 8080
  real 10.4.1.1 port 8080
    reassign 2
    faildetect numconns 4
    retry 20
    inservice
! Server 4 port 8081
  real 10.4.1.1 port 8081
    reassign 2
    faildetect numconns 4
    retry 20
    inservice
! Server 4 port 8082
  real 10.4.1.1 port 8082
    reassign 2
    faildetect numconns 4
    retry 20
    inservice
!
ip slb vserver HTTP2
! Manage HTTP (port 80) requests
  virtual 128.2.0.1 tcp www
  serverfarm FARM2
  idle 120
  delay 5
  inservice
```

スイッチ C の設定文

```
ip slb natpool web-clients 128.5.0.1 128.5.0.254
! NAT address pool for clients
ip slb serverfarm FARM2
! Translate server addresses
  nat server
! Translate client addresses
  nat client web-clients
! Server 3 port 80
  real 10.3.1.1
```

```
    reassign 2
    faildetect numconns 4
    retry 20
    inservice
! Server 4 port 8080
  real 10.4.1.1 port 8080
    reassign 2
    faildetect numconns 4
    retry 20
    inservice
! Server 4 port 8081
  real 10.4.1.1 port 8081
    reassign 2
    faildetect numconns 4
    retry 20
    inservice
! Server 4 port 8082
  real 10.4.1.1 port 8082
    reassign 2
    faildetect numconns 4
    retry 20
    inservice
!
ip slb vserver HTTP2
! Manage HTTP (port 80) requests
  virtual 128.4.0.1 tcp www
  serverfarm FARM2
  idle 120
  delay 5
  inservice
```

例：スタティック NAT を使用した IOS SLB の設定方法

次の例では、次のアイテムの設定文を示します。

- DNS プローブの PROBE4。ドメイン名解決要求に対して、実サーバの IP アドレス 13.13.13.13 を返すように設定します。
- サーバ ファームの DNS。サーバ NAT および PROBE4 を使用するように設定します。
- サーバ ファームの DNS に関連付けられた全ポート仮想サーバの 10.11.11.11。UDP 接続にパケット別サーバ ロード バランシングを実行します。
- サーバ ファームの DNS に関連付けられた実サーバ 10.1.1.3。スタティック NAT およびパケット別サーバ ロード バランシング用に設定します。

```
ip slb probe PROBE4 dns
 lookup 13.13.13.13
!
ip slb serverfarm DNS
 nat server
 probe PROBE4
 real 10.1.1.3
  inservice
!
ip slb vserver DNS
 virtual 10.11.11.11 UDP 0 service per-packet
 serverfarm DNS
!
ip slb static nat 10.11.11.11 per-packet
 real 10.1.1.3
```

例：冗長性を使用した IOS SLB の設定方法

ここでは次の例を紹介し、冗長性を使用するさまざまな IOS SLB 設定を示します。

- 「例：ステートレス バックアップを使用した IOS SLB の設定方法」（P.141）
- 「例：ステートフル バックアップを使用した IOS SLB の設定方法」（P.150）
- 「例：冗長ルート プロセッサのステートフル バックアップを使用した IOS SLB の設定方法」（P.152）
- 「例：アクティブ スタンバイを使用した IOS SLB の設定方法」（P.153）

例：ステートレス バックアップを使用した IOS SLB の設定方法

IOS SLB ステートレス バックアップを設定する方法は複数あります。各設定方法の違いは、ロード バランシング デバイスのネットワーキング機能、およびクライアント トラフィックをロード バランシング デバイスに送信する配信デバイスの機能によって変わります。

- ロード バランシング デバイスがレイヤ 2 スイッチングと VLAN トランキングに対応している場合（Cisco Catalyst 6500 シリーズ スイッチなど）は、デバイスとその実サーバを直接接続して、デバイスが IOS SLB のスタンバイとして機能しながら、実サーバからの発信フローを管理できます。HSRP は、ロード バランシング デバイスのサーバ側 VLAN で使用され、実サーバは HSRP アドレスにルーティングされます。
- ロード バランシング デバイスにレイヤ 2 スイッチングと VLAN トランキングの両方の機能がない場合、そのデバイスと実サーバを レイヤ 2 スイッチに接続する必要があります。この設定は、サーバ側 VLAN で HSRP を使用するために必要です。
- 配信デバイスに レイヤ 3 スイッチングの機能がある場合、アクティブなロード バランシング デバイスにフローを送信するように経路再配布を使用できます。
- 配信デバイスに レイヤ 2 スイッチングの機能がある場合、アクティブなロード バランシング デバイスにフローを送信するように、ロード バランシング デバイスでクライアント側の HSRP を使用できます。
- ほとんどの設定で、HSRP によってフェールオーバー時間が短縮され、さらにルーティングの収束も速くなります。ロード バランシング デバイスでクライアント側およびサーバ側の HSRP の両方を使用する場合、HSRP インターフェイス トラッキングおよびプライオリティを使用して、クライアント側およびサーバ側の HSRP グループを同期する必要があります。

ここでは次の例を紹介し、さまざまな IOS SLB ステートレス バックアップ設定を示します。

- 「例：ダイナミック ルーティングとトランキングの設定方法」（P.142）
- 「例：ダイナミック ルーティングとトランキングなしの設定方法」（P.143）
- 「例：スタティック ルーティングとトランキングの設定方法」（P.145）
- 「例：スタティック ルーティングとトランキングなしの設定方法」（P.147）

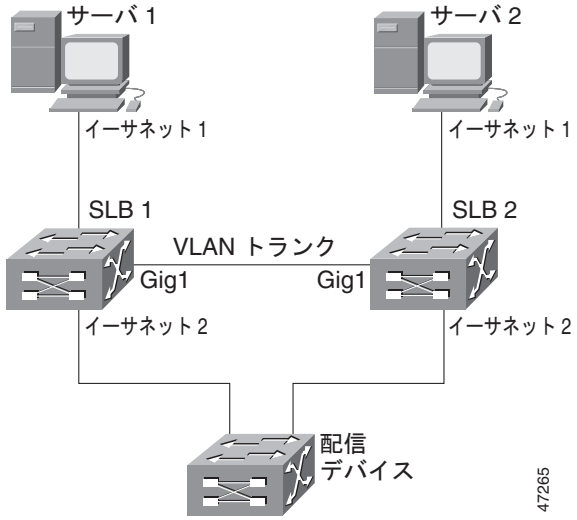
（注） 簡略化するために、この例ではステートフル バックアップを省略しています。ステートフル バックアップを使用する例については、「例：ステートフル バックアップを使用した IOS SLB の設定方法」（P.150）を参照してください。

例：ダイナミック ルーティングとトランキングの設定方法

図 11 に、次の特徴を持つ IOS SLB ステートレス バックアップ設定の例を示します。

- 実サーバ 1 の IP アドレスは 10.10.1.3、実サーバ 2 は 10.10.1.4 で、10.10.1.100 を介してクライアントにルーティングされます。
- 仮想サーバの IP アドレスは 10.10.14.1 です。
- VLAN 1 の IP アドレスは 10.10.1.0 で、サブネット マスクは 255.255.255.0 です。
- サブネット 2 の IP アドレスは 10.10.2.0 で、サブネット マスクは 255.255.255.0 です。
- サブネット 3 の IP アドレスは 10.10.3.0 で、サブネット マスクは 255.255.255.0 です。
- 配信デバイスは、EIGRP を使用して、IOS SLB がアクティブかどうかによって 10.10.2.1 と 10.10.3.1 のどちらかを通して 10.10.14.1 へのルートを学習します。

図 11　　レイヤ 3 およびトランキングを使用するステートレス バックアップ



SLB 1 の設定文

```
ip slb serverfarm SF1
  real 10.10.1.3
    reassign 2
    faildetect numconns 4 numclients 2
    retry 20
    inservice
  real 10.10.1.4
    reassign 2
    faildetect numconns 4
    retry 20
    inservice
ip slb vserver VS1
  virtual 10.10.14.1 tcp www
  serverfarm SF1
  idle 120
  delay 5
  inservice standby SERVER
!
interface Ethernet1
  switchport
  switchport vlan 1
```

```
interface Ethernet2
  ip address 10.10.2.1 255.255.255.0
interface vlan 1
  ip address 10.10.1.1 255.255.255.0
  standby ip 10.10.1.100
  standby priority 10 preempt delay sync 20
  standby name SERVER
  standby track Ethernet2
  standby timers 1 3
router eigrp 666
  redistribute static
  network 10.0.0.0
```

SLB 2 の設定文

```
ip slb serverfarm SF1
  real 10.10.1.3
    reassign 2
    faildetect numconns 4
    retry 20
    inservice
  real 10.10.1.4
    reassign 2
    faildetect numconns 4
    retry 20
    inservice
ip slb vserver VS1
  virtual 10.10.14.1 tcp www
  serverfarm SF1
  idle 120
  delay 5
  inservice standby SERVER
!
interface GigabitEthernet1
  no ip address
  switchport
  switchport trunk encapsulation isl
interface Ethernet1
  switchport
  switchport vlan 1
interface Ethernet2
  ip address 10.10.3.1 255.255.255.0
interface vlan 1
  ip address 10.10.1.2 255.255.255.0
  standby ip 10.10.1.100
  standby priority 5 preempt delay sync 20
  standby name SERVER
  standby track Ethernet2
  standby timers 1 3
router eigrp 666
  redistribute static
  network 10.0.0.0
```

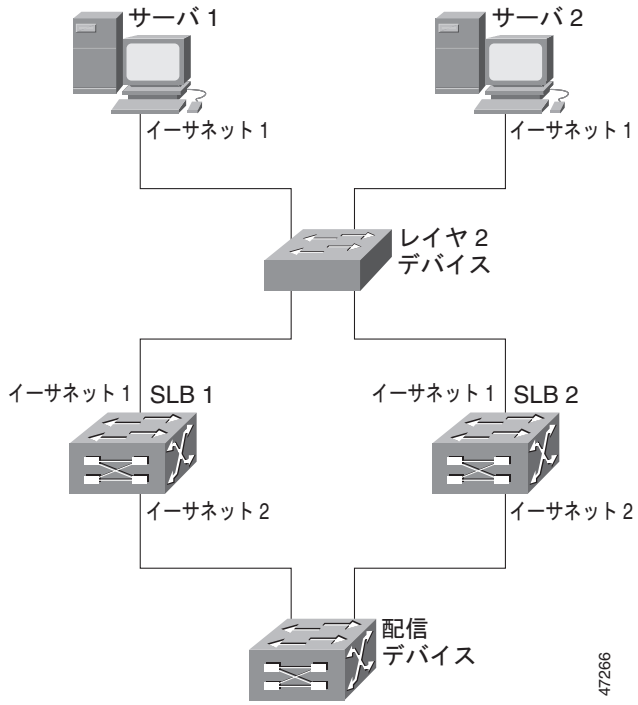
例：ダイナミック ルーティングとトランキングなしの設定方法

図 12 に、次の特徴を持つ IOS SLB ステートレス バックアップ設定の例を示します。

- 実サーバ 1 の IP アドレスは 10.10.1.3、実サーバ 2 は 10.10.1.4 で、10.10.1.100 を介してクライアントにルーティングされます。
- 仮想サーバの IP アドレスは 10.10.14.1 です。
- サブネット 2 の IP アドレスは 10.10.2.0 で、サブネット マスクは 255.255.255.0 です。

- サブネット 3 の IP アドレスは 10.10.3.0 で、サブネット マスクは 255.255.255.0 です。
- 配信デバイスは、EIGRP を使用して、IOS SLB がアクティブかどうかによって 10.10.2.2 と 10.10.3.2 のどちらかを通して 10.10.14.1 へのルートを学習します。

図 12　　レイヤ 3 あり、トランキングなしのステートレス バックアップ



SLB 1 の設定文

```
ip slb serverfarm SF1
  real 10.10.1.3
    reassign 2
    faildetect numconns 4
    retry 20
    inservice
  real 10.10.1.4
    reassign 2
    faildetect numconns 4
    retry 20
    inservice
ip slb vserver VS1
  virtual 10.10.14.1 tcp www
  serverfarm SF1
  idle 120
  delay 5
  inservice standby SERVER
!
interface Ethernet1
  ip address 10.10.1.1 255.255.255.0
  standby ip 10.10.1.100
  standby priority 10 preempt delay sync 20
  standby name SERVER
  standby track Ethernet2
  standby timers 1 3
interface Ethernet2
```

```
  ip address 10.10.2.1 255.255.255.0
router eigrp 666
  redistribute static
  network 10.0.0.0
```

SLB 2 の設定文

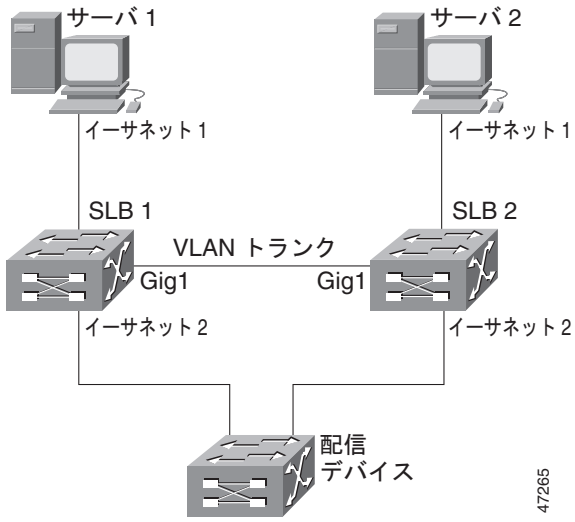
```
ip slb serverfarm SF1
  real 10.10.1.3
    reassign 2
    faildetect numconns 4
    retry 20
    inservice
  real 10.10.1.4
    reassign 2
    faildetect numconns 4
    retry 20
    inservice
ip slb vserver VS1
  virtual 10.10.14.1 tcp www
  serverfarm SF1
  idle 120
  delay 5
  inservice standby SERVER
!
interface Ethernet1
  ip address 10.10.1.2 255.255.255.0
  standby ip 10.10.1.100
  standby priority 5 preempt delay sync 20
  standby name SERVER
  standby track Ethernet2
  standby timers 1 3
interface Ethernet2
  ip address 10.10.3.1 255.255.255.0
router eigrp 666
  redistribute static
  network 10.0.0.0
```

例：スタティック ルーティングとトランキングの設定方法

図 13 に、次の特徴を持つ IOS SLB ステートレス バックアップ設定の例を示します。

- 実サーバ 1 の IP アドレスは 10.10.1.3、実サーバ 2 は 10.10.1.4 で、10.10.1.100 を介してクライアントにルーティングされます。
- 仮想サーバの IP アドレスは 10.10.14.1 です。
- VLAN 1 の IP アドレスは 10.10.1.0 で、サブネット マスクは 255.255.255.0 です。
- サブネット 2 の IP アドレスは 10.10.2.0 で、サブネット マスクは 255.255.255.0 です。
- サブネット 3 の IP アドレスは 10.10.3.0 で、サブネット マスクは 255.255.255.0 です。
- この設定では、配信デバイスで HSRP ルートにスタティック ルーティングを使用します。

図 13　　レイヤ 2 およびトランキングを使用するステートレス バックアップ



SLB 1 の設定文

```
ip slb serverfarm SF1
  real 10.10.1.3
    reassign 2
    faildetect numconns 4
    retry 20
    inservice
  real 10.10.1.4
    reassign 2
    faildetect numconns 4
    retry 20
    inservice
ip slb vserver VS1
  virtual 10.10.14.1 tcp www
  serverfarm SF1
  idle 120
  delay 5
  inservice standby SERVER
!
interface Ethernet1
  switchport
  switchport vlan 1
interface Ethernet2
  ip address 10.10.2.1 255.255.255.0
  standby ip 10.10.2.100
  standby priority 10 preempt delay sync 20
  standby track vlan1
  standby timers 1 3
interface vlan 1
  ip address 10.10.1.1 255.255.255.0
  standby ip 10.10.1.100
  standby priority 10 preempt delay sync 20
  standby name SERVER
  standby track Ethernet2
  standby timers 1 3
```

SLB 2 の設定文

```
ip slb serverfarm SF1
  real 10.10.1.3
    reassign 2
    faildetect numconns 4
    retry 20
    inservice
  real 10.10.1.4
    reassign 2
    faildetect numconns 4
    retry 20
    inservice
ip slb vserver VS1
  virtual 10.10.14.1 tcp www
  serverfarm SF1
  idle 120
  delay 5
  inservice standby SERVER
!
interface GigabitEthernet1
  no ip address
  switchport
  switchport trunk encapsulation isl
interface Ethernet1
  switchport
  switchport vlan 1
interface Ethernet2
  ip address 10.10.2.2 255.255.255.0
  standby ip 10.10.2.100
  standby priority 5 preempt delay sync 20
  standby track vlan 1
  standby timers 1 3
interface vlan 1
  ip address 10.10.1.2 255.255.255.0
  standby ip 10.10.1.100
  standby priority 5 preempt delay sync 20
  standby name SERVER
  standby track Ethernet2
  standby timers 1 3
```

配信デバイスの設定文

```
interface Ethernet1
  switchport
  switchport distribution vlan 2
interface Ethernet2
  switchport
  switchport distribution vlan 2
interface vlan2
  ip address 10.10.2.3 255.255.255.0
  no shut
ip route 10.10.14.1 255.255.255.255 10.10.2.100
```

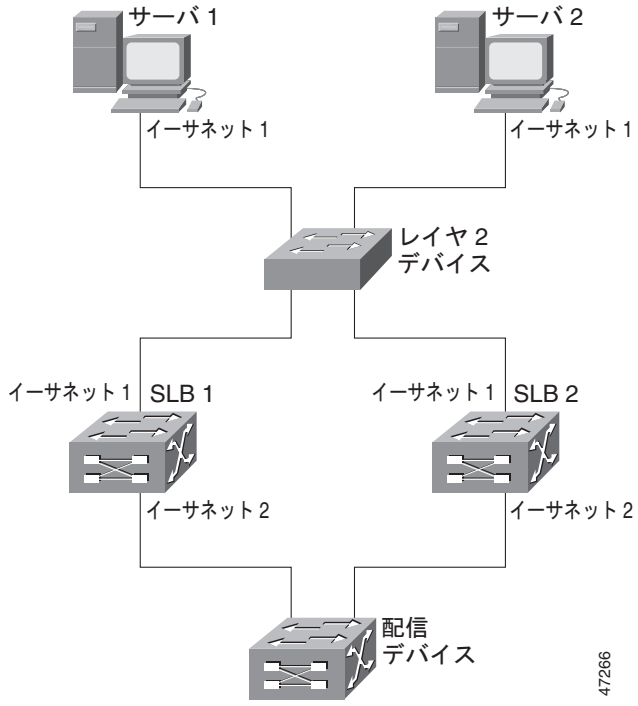
例：スタティック ルーティングとトランキングなしの設定方法

図 14 に、次の特徴を持つ IOS SLB ステートレス バックアップ設定の例を示します。

- 実サーバ 1 の IP アドレスは 10.10.1.3、実サーバ 2 は 10.10.1.4 で、10.10.1.100 を介してクライアントにルーティングされます。
- 仮想サーバの IP アドレスは 10.10.14.1 です。
- サブネット 2 の IP アドレスは 10.10.2.0 で、サブネット マスクは 255.255.255.0 です。

- サブネット 3 の IP アドレスは 10.10.3.0 で、サブネット マスクは 255.255.255.0 です。
- この設定では、配信デバイスで HSRP ルートにスタティック ルーティングを使用します。

図 14　　レイヤ 2 あり、トランキングなしのステートレス バックアップ



SLB 1 の設定文

```
ip slb serverfarm SF1
  real 10.10.1.3
    reassign 2
    faildetect numconns 4
    retry 20
    inservice
  real 10.10.1.4
    reassign 2
    faildetect numconns 4
    retry 20
    inservice
ip slb vserver VS1
  virtual 10.10.14.1 tcp www
  serverfarm SF1
  idle 120
  delay 5
  inservice standby SERVER
!
interface Ethernet1
  ip address 10.10.1.1 255.255.255.0
  standby ip 10.10.1.100
  standby priority 10 preempt delay sync 20
  standby name SERVER
  standby track Ethernet2
  standby timers 1 3
interface Ethernet2
  ip address 10.10.2.1 255.255.255.0
```

```
  standby ip 10.10.2.100
  standby priority 10 preempt delay sync 20
  standby track Ethernet1
  standby timers 1 3
```

SLB 2 の設定文

```
ip slb serverfarm SF1
  real 10.10.1.3
    reassign 2
    faildetect numconns 4
    retry 20
    inservice
  real 10.10.1.4
    reassign 2
    faildetect numconns 4
    retry 20
    inservice
ip slb vserver VS1
  virtual 10.10.14.1 tcp www
  serverfarm SF1
  idle 120
  delay 5
  inservice standby SERVER
!
interface Ethernet1
  ip address 10.10.1.2 255.255.255.0
  standby ip 10.10.1.100
  standby priority 5 preempt delay sync 20
  standby name SERVER
  standby track Ethernet2
  standby timers 1 3
!
interface Ethernet2
  ip address 10.10.2.2 255.255.255.0
  standby ip 10.10.2.100
  standby priority 5 preempt delay sync 20
  standby track Ethernet1
  standby timers 1 3
```

配信デバイスの設定文

```
interface Ethernet1
  switchport
  switchport distribution vlan 2
interface Ethernet2
  switchport
  switchport distribution vlan 2
interface vlan2
  ip address 10.10.2.3 255.255.255.0
  no shut
ip route 10.10.14.1 255.255.255.255 10.10.2.100
```

例：ステートフル バックアップを使用した IOS SLB の設定方法

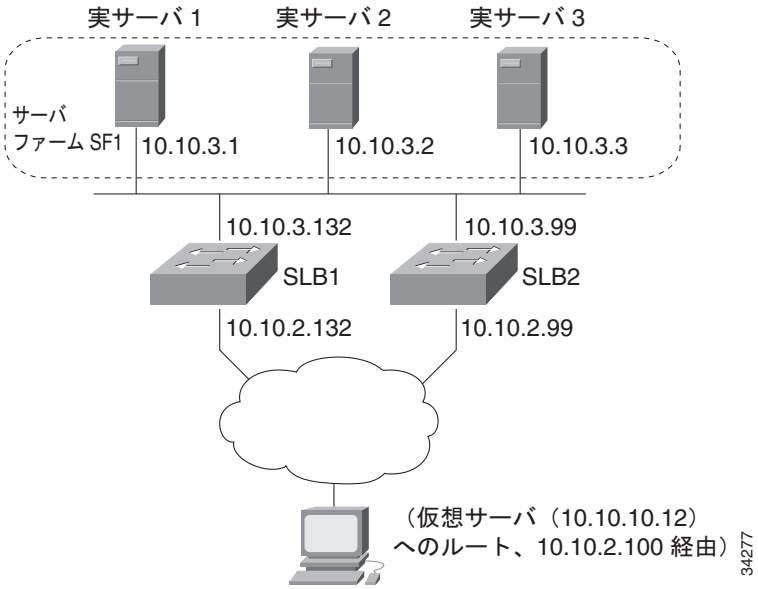
この設定例では、サーバ ファームの一部として設定されている IOS SLB 実サーバ接続と、ステートフル バックアップ スタンバイ接続を使用するファスト イーサネット インターフェイス上の実サーバおよび仮想サーバを中心に説明します。

図 15 は、クライアント側とサーバ側の両方で HSRP を使用してフェールオーバーを管理するステートフル バックアップ設定の例です。実サーバは発信フローを 10.10.3.100 にルーティングします。これはサーバ側インターフェイスの HSRP アドレスです。クライアント（アクセス ルータ）は、クライアント側の HSRP アドレスである 10.10.2.100 を介して、仮想 IP アドレス（10.10.10.12）にルーティングされます。

ループバック インターフェイスは、これらのメッセージ交換のために、両方のデバイスで設定されています。また、各 IOS SLB には、他のスイッチ ループバック アドレス宛ての二重ルートを割り当てる必要があります。この設定では、インターフェイスで障害が発生しても、レプリケーション メッセージを送信できます。

（注） HSRP が適切に機能するには、IOS SLB スイッチ間のすべての レイヤ 2 デバイスに **set spantree portfast** コマンドを設定する必要があります。

図 15　　IOS SLB ステートフル環境



スイッチ SLB1 の設定文

```
ip slb serverfarm SF1
  nat server
  real 10.10.3.1
   inservice
  real 10.10.3.2
   inservice
  real 10.10.3.3
   inservice
!
ip slb vserver VS1
  virtual 10.10.10.12 tcp telnet
  serverfarm SF1
```

```
  replicate casa 10.10.99.132 10.10.99.99 1024 password PASS
  inservice standby virt
!
interface loopback 1
  ip address 10.10.99.132 255.255.255.255
!
interface FastEthernet1
  ip address 10.10.3.132 255.255.255.0
  no ip redirects
  no ip mroute-cache
  standby priority 5 preempt
  standby name out
  standby ip 10.10.3.100
  standby track FastEthernet2
  standby timers 1 3
interface FastEthernet2
  ip address 10.10.2.132 255.255.255.0
  no ip redirects
  standby priority 5
  standby name virt
  standby ip 10.10.2.100
  standby timers 1 3
```

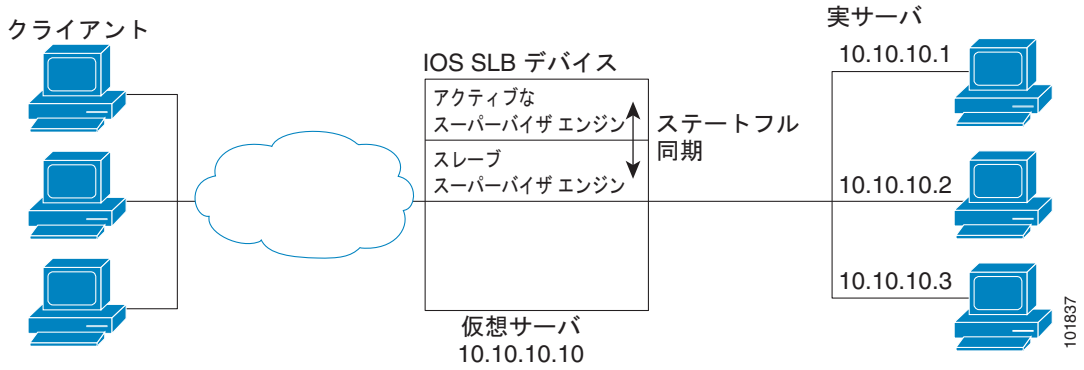
スイッチ SLB2 の設定文

```
ip slb serverfarm SF1
  nat server
  real 10.10.3.1
   inservice
  real 10.10.3.2
   inservice
  real 10.10.3.3
   inservice
!
ip slb vserver VS1
  virtual 10.10.10.12 tcp telnet
  serverfarm SF1
  replicate casa 10.10.99.99 10.10.99.132 1024 password PASS
  inservice standby virt
!
interface loopback 1
  ip address 10.10.99.99 255.255.255.255
!
interface FastEthernet2
  ip address 10.10.2.99 255.255.255.0
  no ip redirects
  no ip route-cache
  no ip mroute-cache
  standby priority 10 preempt delay sync 20
  standby name virt
  standby ip 10.10.2.100
  standby track FastEthernet3
  standby timers 1 3
!
interface FastEthernet3
  ip address 10.10.3.99 255.255.255.0
  no ip redirects
  no ip route-cache
  no ip mroute-cache
  standby priority 10 preempt delay 20
  standby name out
  standby ip 10.10.3.100
  standby track FastEthernet2
  standby timers 1 3
```

例：冗長ルート プロセッサのステートフル バックアップを使用した IOS SLB の設定方法

図 16 の IOS SLB デバイスには、ステートフル バックアップ用に設定されている 2 つのスーパーバイザ エンジンが含まれます。アクティブなスーパーバイザ エンジンに障害が発生すると、IOS SLB 同期情報が生成されている RPR+ を通して、バックアップ スーパーバイザ エンジンが引き継ぎます。IOS SLB は、アクティブなスーパーバイザ エンジンの仮想サーバ ACME_VSERVER（10.10.10.10）の状態情報を、20 秒ごとにバックアップにレプリケートします。実サーバ（10.10.10.1、10.10.10.2、および 10.10.10.3）は、サーバ ファーム ACME_SFARM に設定されます。

図 16　　冗長ルート プロセッサを使用した IOS SLB



次に、図 16 の設定の IOS SLB 設定文を示します。

```
ip slb replicate slave rate 300

ip slb serverfarm ACME_SFARM
  nat server
  real 10.10.10.1
   inservice
  real 10.10.10.2
   inservice
  real 10.10.10.3
   inservice

ip slb vserver ACME_VSERVER
 virtual 10.10.10.10 tcp 80
 replicate interval 20
 replicate slave
 serverfarm ACME_SFARM
 inservice
```

例：アクティブ スタンバイを使用した IOS SLB の設定方法

図 17 に、アクティブ スタンバイに設定されている IOS SLB ネットワークを示します。このネットワークには、同じ仮想 IP アドレスの負荷を分散し、さらに相互にバックアップしあう 2 つの IOS SLB デバイスがあります。どちらかのデバイスで障害が発生した場合は、残りのデバイスが通常の HSRP フェールオーバーと IOS SLB ステートレス冗長性を通して負荷を引き継ぎます。

図 17　　IOS SLB アクティブ スタンバイ

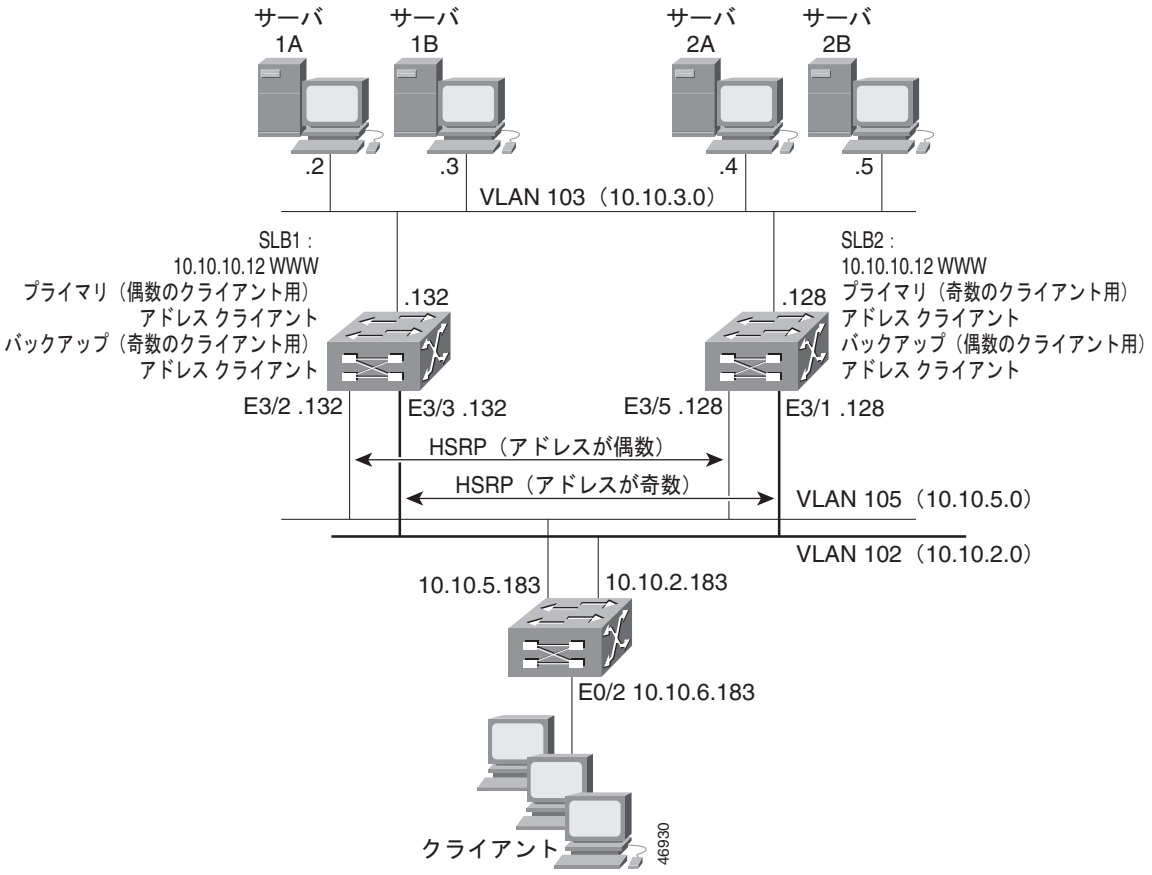


図 17 のネットワーク設定例には、次の特徴があります。

- SLB 1 はサーバ 1A および 1B の負荷を分散し、SLB 2 は 2A および 2B の負荷を分散します。
- 1 つの仮想 IP アドレス（Web の場合は 10.10.10.12）が、2 つの IOS SLB デバイスでサポートされます。
- クライアント トラフィックはアクセス ルータで分割され、IP アドレスが偶数のクライアントは HSRP1（10.10.5.100）に送信され、IP アドレスが奇数のクライアントは HSRP2（10.10.2.100）に送信されます。IP アドレスが奇数のクライアントの場合、SLB 1 がプライマリとして設定され、IP アドレスが奇数のクライアントの場合、SLB 2 がプライマリになります。
- IOS SLB デバイスは、分離された各実サーバ セットにトラフィックを分散します（この例でクライアント NAT を使用する場合、この特徴は必須ではなくなります）。
- 各実サーバ セットには、IOS SLB デバイスに設定されているデフォルト ゲートウェイがあります。
- VLAN 105 の HSRP アドレスは 10.10.5.100 です。VLAN 102 の HSRP アドレスは 10.10.2.100 です。

SLB 1 の設定文

```
ip slb serverfarm EVEN
 nat server
 real 10.10.3.2
  reassign 2
  faildetect numconns 4 numclients 2
  retry 20
  inservice
 real 10.10.3.3
  reassign 2
  faildetect numconns 4
  retry 20
  inservice
!
ip slb serverfarm ODD
 nat server
 real 10.10.3.2
  reassign 2
  faildetect numconns 4
  retry 20
  inservice
 real 10.10.3.3
  reassign 2
  faildetect numconns 4
  retry 20
  inservice
!-----Same EVEN virtual server as in SLB 2
ip slb vserver EVEN
 virtual 10.10.10.12 tcp www
 serverfarm EVEN
 client 0.0.0.0 0.0.0.1
 idle 120
 delay 5
!-----See standby name in Ethernet 3/3 below
 inservice standby STANDBY_EVEN
!-----Same ODD virtual server as in SLB 2
ip slb vserver ODD
 virtual 10.10.10.12 tcp www
 serverfarm ODD
 client 0.0.0.1 0.0.0.1
 idle 120
 delay 5
!-----See standby name in Ethernet 3/2 below
 inservice standby STANDBY_ODD
!
interface Ethernet3/2
 ip address 10.10.5.132 255.255.255.0
 standby priority 20 preempt delay sync 20
!-----See standby name in SLB 2, Ethernet 3/5
 standby name STANDBY_ODD
 standby ip 10.10.5.100
 standby track Ethernet3/3
 standby timers 1 3
!
interface Ethernet3/3
 ip address 10.10.2.132 255.255.255.0
 standby priority 10
!-----See standby name in SLB 2, Ethernet 3/1
 standby name STANDBY_EVEN
 standby ip 10.10.2.100
 standby track Ethernet3/2
 standby timers 1 3
```

SLB 2 の設定文

```
ip slb serverfarm EVEN
 nat server
 real 10.10.3.4
  reassign 2
  faildetect numconns 4
  retry 20
  inservice
 real 10.10.3.5
  reassign 2
  faildetect numconns 4
  retry 20
  inservice
!
ip slb serverfarm ODD
 nat server
 real 10.10.3.4
  reassign 2
  faildetect numconns 4
  retry 20
  inservice
 real 10.10.3.5
  reassign 2
  faildetect numconns 4
  retry 20
  inservice
!-----Same EVEN virtual server as in SLB 1
ip slb vserver EVEN
 virtual 10.10.10.12 tcp www
 serverfarm EVEN
 client 0.0.0.0 0.0.0.1
 idle 120
 delay 5
!-----See standby name in Ethernet 3/1 below
 inservice standby STANDBY_EVEN
!-----Same ODD virtual server as in SLB 1
ip slb vserver ODD
 virtual 10.10.10.12 tcp www
 serverfarm ODD
 client 0.0.0.1 0.0.0.1
 idle 120
 delay 5
!-----See standby name in Ethernet 3/5 below
 inservice standby STANDBY_ODD
!
interface Ethernet3/1
 ip address 10.10.2.128 255.255.255.0
 standby priority 20 preempt delay sync 20
!-----See standby name in SLB 1, Ethernet 3/3
 standby name STANDBY_EVEN
 standby ip 10.10.2.100
 standby track Ethernet3/5
 standby timers 1 3
!
interface Ethernet3/5
 ip address 10.10.5.128 255.255.255.0
 standby priority 10 preempt delay sync 20
!-----See standby name in SLB 1, Ethernet 3/2
 standby name STANDBY_ODD
 standby ip 10.10.5.100
 standby track Ethernet3/1
 standby timers 1 3
```

アクセス ルータの設定文

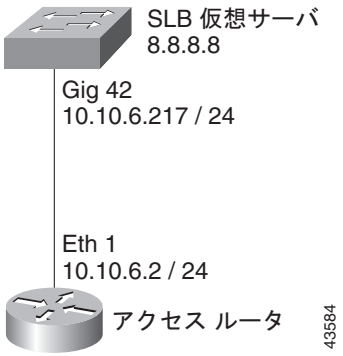
```
interface Ethernet0/0
 ip address 10.10.5.183 255.255.255.0
 no ip directed-broadcast
 no ip route-cache
 no ip mroute-cache
!
interface Ethernet0/1
 ip address 10.10.2.183 255.255.255.0
 no ip directed-broadcast
 no ip route-cache
 no ip mroute-cache
!
interface Ethernet0/2
 ip address 10.10.6.183 255.255.255.0
 no ip directed-broadcast
 no ip route-cache
 no ip mroute-cache
 ip policy route-map virts
!
access-list 100 permit ip 0.0.0.1 255.255.255.254 host 10.10.10.12
access-list 101 permit ip 0.0.0.0 255.255.255.254 host 10.10.10.12
route-map virts permit 10
match ip address 100
set ip next-hop 10.10.5.100
!
route-map virts permit 15
match ip address 101
set ip next-hop 10.10.2.100
```

例：スタティック ルートの再配布を使用した IOS SLB の設定方法

図 18 に、スタティック ルートを仮想サーバの IP アドレスに配布するように設定されている IOS SLB ネットワークを示します。仮想サーバをサービスに参加させるとき（**inservice** コマンドを使用します）、アドレスをアドバタイズする場合、そのアドレスへのルートは、**static** としてルーティング テーブルに追加されます。仮想サーバの IP アドレスをアドバタイズする方法の詳細については、『*Cisco IOS IP Application Services Command Reference*』の **advertise** コマンドの説明を参照してください。

ルーティング設定はプロトコルによって異なるため、いくつかのルーティング プロトコルの設定例を示します。

図 18　　スタティック ルートの IOS SLB 再配布



Routing Information Protocol（RIP）

図 18 の IOS SLB スイッチの RIP スタティック ルートの再配布設定を次に示します。

```
router rip
 redistribute static
 network 10.0.0.0
 network 8.0.0.0
```

図 18 のルーティングの更新をリスンするアクセス ルータに関する RIP スタティック ルートの再配布設定を次に示します。

```
router rip
 network 10.0.0.0
 network 8.0.0.0
```

Open Shortest Path First（OSPF）

図 18 の IOS SLB スイッチの OSPF スタティック ルートの再配布設定を次に示します。

```
router ospf 1
 redistribute static subnets
 network 10.10.6.217 0.0.0.0 area 0
 network 8.8.8.0 0.0.0.255 area 0
```

図 18 のルーティングの更新をリスンするアクセス ルータに関する OSPF スタティック ルートの再配布設定を次に示します。

```
router ospf 1
 network 10.10.6.2 0.0.0.0 area 0
 network 8.8.8.0 0.0.0.255 area 0
```

Interior Gateway Routing Protocol（IGRP）

図 18 の IOS SLB スイッチの IGRP スタティック ルートの再配布設定を次に示します。

```
router igrp 1
 redistribute connected
 redistribute static
 network 8.0.0.0
 network 10.0.0.0
```

図 18 のルーティングの更新をリスンするアクセス ルータに関する IGRP スタティック ルートの再配布設定を次に示します。

```
router igrp 1
 network 8.0.0.0
 network 10.0.0.0
```

Enhanced Interior Gateway Routing Protocol（Enhanced IGRP）

図 18 の IOS SLB スイッチの Enhanced IGRP スタティック ルートの再配布設定を次に示します。

```
router eigrp 666
 redistribute static
 network 10.0.0.0
 network 8.0.0.0
```

図 18 のルーティングの更新をリスンするアクセス ルータに関する Enhanced IGRP スタティック ルートの再配布設定を次に示します。

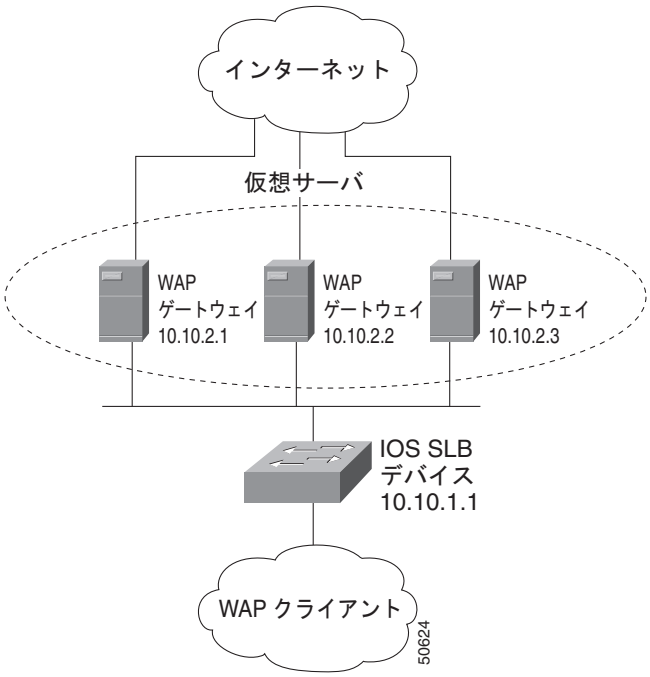
```
router eigrp 666
 network 10.0.0.0
 network 8.0.0.0
```

例：WAP および UDP ロード バランシングを使用した IOS SLB の設定方法

図 19 に、WAP フローの負荷を分散するように設定されている IOS SLB ネットワークを示します。この例の場合：

- WAP フローの負荷は、WAP ゲートウェイ 10.10.2.1、10.10.2.2、および 10.10.2.3 で分散されます。
- クライアントは、IOS SLB 仮想サーバ アドレス 10.10.1.1 に接続します。
- 接続のアイドル時間が仮想サーバのアイドル接続タイマーよりも長い場合（この例では 3000 秒）、そのセッションに関するロード バランシングの判断は変わります。

図 19　　WAP ロード バランシングを使用した IOS SLB



WAP の場合に IOS SLB のロード バランシングを設定するには、2 つの方法があります。

- コネクション型 WSP モードで実行されているセッションの負荷を分散するには、WSP プローブを定義し、WAP ロード バランシングを使用します。WAP ロード バランシングには、WAP ポートの 1 つで、WAP 仮想サーバを設定する必要があります。
- コネクションレス型 WSP モード、コネクションレス型セキュア WSP モード、およびコネクション型セキュア WSP モードで実行されているセッションの負荷を分散するには、ping プローブまたは WSP プローブを定義し、低いアイドル タイマーを指定した標準の UDP ロード バランシングを使用します。

例：UDP ポート 9201 上での WAP フローのバランス方法

次に、図 19 に示す IOS SLB デバイスの設定例を示します。UDP ポート 9201 の WAP フローの負荷を分散します（WSP/WTP/UDP）。

```
ip slb probe PROBE3 wsp
  url http://localhost/test.txt
!
ip slb serverfarm WAPFARM
  nat server
  real 10.10.2.1
  inservice
  real 10.10.2.2
  inservice
  real 10.10.2.3
  inservice
  probe PROBE3
!
ip slb vserver VSERVER
  virtual 10.10.1.1 udp 9201
  serverfarm WAPFARM
  idle 3000
  inservice
```

例：UDP ポート 9203 上での WAP フローのバランス方法

次に、図 19 に示す IOS SLB デバイスの設定例を示します。UDP ポート 9203 の WAP フローの負荷を分散します（WSP/WTP/WTLS/UDP）。

```
ip slb probe PROBE1 ping
!
ip slb serverfarm WAPFARM
  nat server
  real 10.10.2.1
  inservice
  real 10.10.2.2
  inservice
  real 10.10.2.3
  inservice
  probe PROBE1
!
ip slb vserver VSERVER
  virtual 10.10.1.1 udp 9203
  serverfarm WAPFARM
  idle 3000
  inservice
```

例：ルート ヘルス インジェクションを使用した IOS SLB の設定方法

ここでは次の例を紹介し、さまざまな IOS SLB ルート ヘルス インジェクションの設定を示します。

- 「例：1 台ずつの Web サーバを使用した 2 つの分散サイトの設定方法」（P.160）
- 「例：2 台ずつの Web サーバを使用した 2 つの分散サイトの設定方法」（P.161）
- 「例：1 台ずつの Web サーバとバックアップ IOS SLB スイッチを使用した 2 つの分散サイトの設定方法」（P.162）

例：1 台ずつの Web サーバを使用した 2 つの分散サイトの設定方法

図 20 に、次の特徴を持つルート ヘルス インジェクションを使用して設定した IOS SLB ネットワークを示します。

- 両方の IOS SLB デバイスは、同じ仮想 IP アドレスで設定されます。
- 各 IOS SLB デバイスには、実サーバとしてローカルで接続された Web サーバだけを含むサーバファームがあります。
- SLB A へのパスは低い加重です。

図 20　　1 つずつ Web サーバがある 2 つの分散サイト

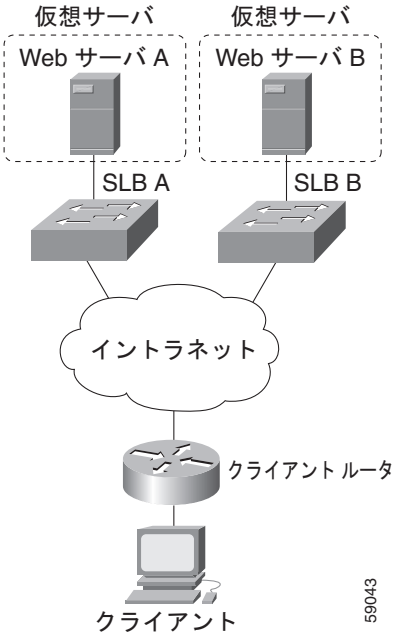


図 20 の両方の Web サーバが動作している場合、クライアント ルータは、両方の IOS SLB デバイスからホスト ルートを受信します。

Web サーバ A に障害が発生すると、SLB A 上にある仮想 IP アドレスの仮想サーバは FAILED 状態になり、仮想 IP アドレスのホスト ルートのアドバタイジングを停止します。すると、クライアント ルータは、SLB B へのルートを使用し始めます。

Web サーバ A がまた使用可能になると、仮想サーバは仮想 IP アドレスのホスト ルートを改めてアドバタイズし、クライアント ルータは SLB A の使用を開始します。

例：2 台ずつの Web サーバを使用した 2 つの分散サイトの設定方法

図 21 に、次の特徴を持つルート ヘルス インジェクションを使用して設定した IOS SLB ネットワークを示します。

- 両方の IOS SLB デバイスは、同じ仮想 IP アドレスで設定されます。
- 各 IOS SLB デバイスには、実サーバとしてローカルで接続された 2 つの Web サーバを含むサーバ ファームがあります。
- SLB A へのパスは低い加重です。

図 21　　2 つずつ Web サーバがある 2 つの分散サイト

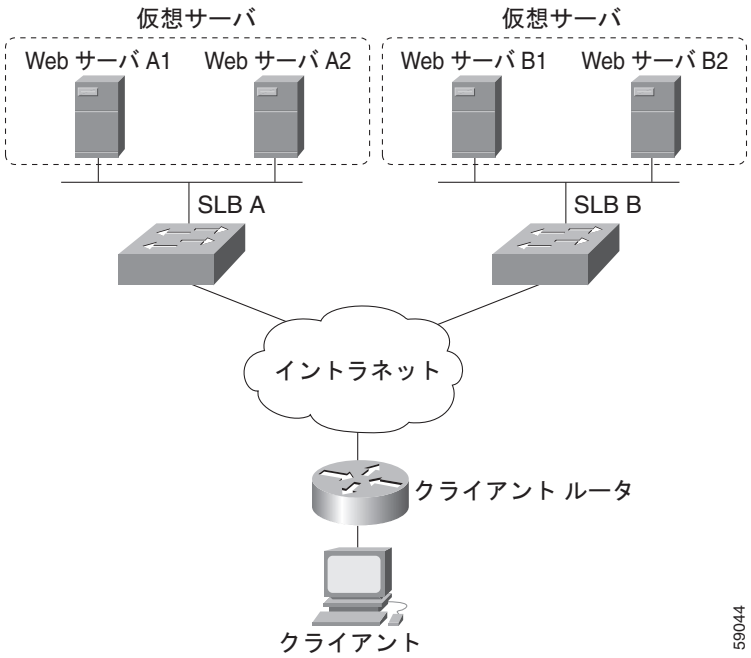


図 21 のすべての Web サーバが動作している場合、クライアント ルータは、両方の IOS SLB デバイスからホスト ルートを受信します。

いずれかのサーバ ファームの一方の Web サーバに障害が発生すると、その IOS SLB デバイスによるルートのアドバタイジングは継続されます。

Web サーバ A1 と Web サーバ A2 の両方に障害が発生すると、SLB A 上にある仮想 IP アドレスの仮想サーバは FAILED 状態になり、仮想 IP アドレスのホスト ルートのアドバタイジングを停止します。すると、クライアント ルータは、SLB B へのルートを使用し始めます。

Web サーバ A1 または Web サーバ A2 がまた使用可能になると、仮想サーバは仮想 IP アドレスのホスト ルートを改めてアドバタイズし、クライアント ルータは SLB A の使用を開始します。

例：1 台ずつの Web サーバとバックアップ IOS SLB スイッチを使用した 2 つの分散サイトの設定方法

図 22 に、次の特徴を持つルート ヘルス インジェクションを使用して設定した IOS SLB ネットワークを示します。

- 両方の IOS SLB デバイスは、同じ仮想 IP アドレスで設定されます。
- 各 IOS SLB デバイスには、実サーバとしてローカルで接続された Web サーバだけを含むサーバファームがあります。
- 各サイトには、プライマリ IOS SLB デバイスとバックアップ IOS SLB デバイスがあります。
- SLB A へのパスは低い加重です。

図 22　1 台ずつの Web サーバとバックアップ IOS SLB スイッチを使用した 2 つの分散サイト

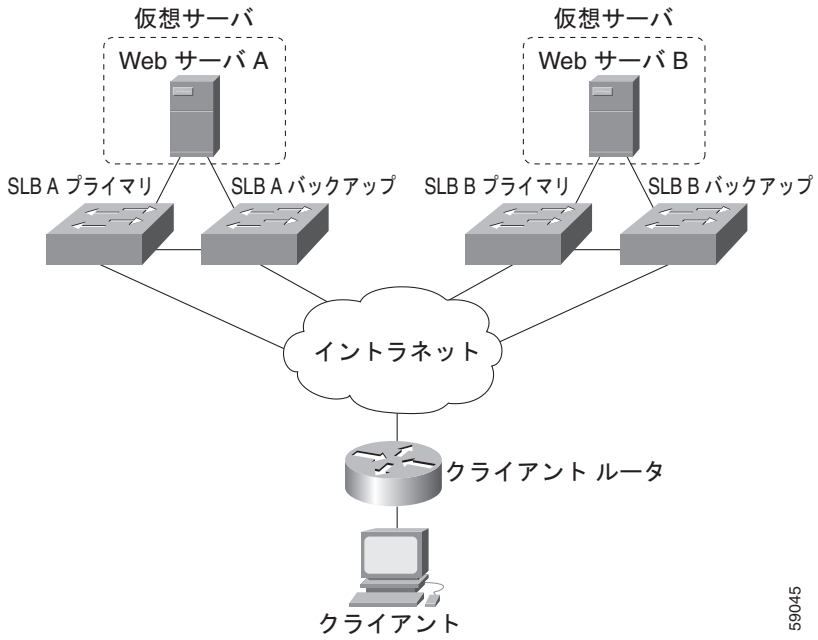


図 22 の両方の Web サーバが動作している場合、クライアント ルータは、SLB A プライマリおよび SLB B プライマリの両方からホスト ルートを受信します。

SLB A プライマリに障害が発生すると、SLB A バックアップは仮想 IP アドレスに対するホスト ルートのアドバタイジングを開始します。SLB A バックアップにも障害が発生すると、SLB A プライマリおよび SLB A バックアップ上にある仮想 IP アドレスの仮想サーバは FAILED 状態になり、仮想 IP アドレスのホスト ルートのアドバタイジングを停止します。すると、クライアント ルータは SLB B プライマリ（SLB B プライマリが使用できない場合は、SLB B バックアップ）に対するルートの使用を開始します。

SLB A プライマリまたは SLB A バックアップがまた使用可能になると、仮想サーバは仮想 IP アドレスのホスト ルートを改めてアドバタイズし、クライアント ルータは SLB A プライマリまたは SLB A バックアップの使用を開始します。

例：GPRS ロード バランシングを使用した IOS SLB の設定方法

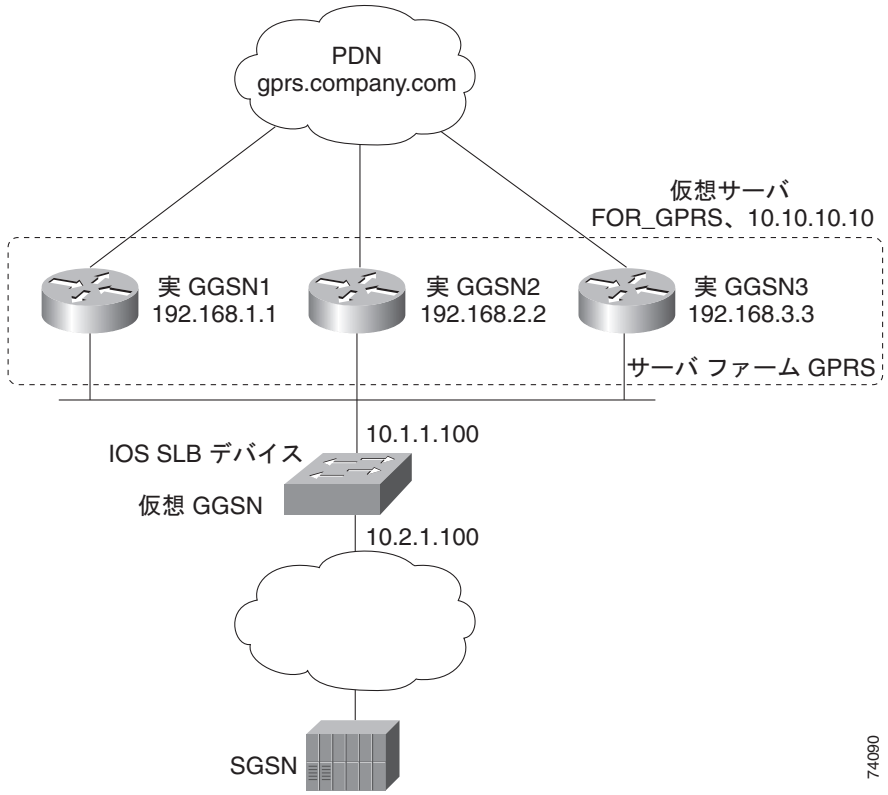
ここでは次の例を紹介し、冗長性を使用するさまざまな IOS SLB 設定を示します。

例：GTP Cause Code Inspection がイネーブルになっていない GPRS ロード バランシングを使用した IOS SLB の設定方法

図 23 に、GTP Cause Code Inspection をイネーブルにしない一般的な GPRS ロード バランシング設定を示します。この設定の場合：

- IOS SLB は、複数の実 GGSN について GPRS フローの負荷を分散できます。SGSN からは、実 GGSN が 1 つの仮想 GGSN に見えます。この設定では、実 GGSN のフロー処理能力を増やし、信頼性と可用性を向上しています。
- SGSN の仮想テンプレート アドレスは 10.111.111.111 です。
- GGSN1 の仮想テンプレート アドレスは 192.168.1.1 です。
- GGSN2 の仮想テンプレート アドレスは 192.168.2.2 です。
- GGSN3 の仮想テンプレート アドレスは 192.168.3.3 です。

図 23　GPRS ロード バランシングを使用した IOS SLB



次に、図 23 の設定の設定文を示します。

- 「IOS SLB の設定文」（P.164）
- 「GGSN1 の設定文」（P.165）
- 「GGSN2 の設定文」（P.166）
- 「GGSN3 の設定文」（P.167）

詳細な GGSN 設定例については、『*Cisco IOS Mobile Wireless Configuration Guide*』を参照してください。

IOS SLB の設定文

```
hostname GTP_SLB
!
ip domain-name gprs.com
!
ip slb serverfarm GPRS
 real 192.168.1.1
  weight 1
  faildetect numconns 1 numclients 1
  inservice
!
 real 192.168.2.2
  weight 1
  faildetect numconns 1 numclients 1
  inservice
!
```

```
 real 192.168.3.3
  weight 1
  faildetect numconns 1 numclients 1
  inservice
!
ip slb vserver FOR_GPRS
 virtual 10.10.10.10 udp 3386 service gtp
 serverfarm GPRS
 inservice
!
ip slb dfp password Password1 0
 agent 10.1.1.201 1111 30 0 10
 agent 10.1.1.202 1111 30 0 10
 agent 10.1.1.203 1111 30 0 10
!
interface FastEthernet1/0
 description TO SERVERFARM GPRS
 ip address 10.1.1.100 255.255.255.0
 no ip redirects
 duplex half
!
interface FastEthernet3/0
 description TO SGSN
 ip address 10.2.1.100 255.255.255.0
 no ip mroute-cache
 duplex half
!
ip route 10.111.111.111 255.255.255.255 FastEthernet1/0
ip route 192.168.1.1 255.255.255.255 10.1.1.201
ip route 192.168.2.2 255.255.255.255 10.1.1.202
ip route 192.168.3.3 255.255.255.255 10.1.1.203
```

GGSN1 の設定文

```
service gprs ggsn
!
hostname GGSN1
!
ip dfp agent gprs
 port 1111
 password Password1 0
 inservice
!
ip domain-name gprs.com
!
interface loopback 1
 description LOOPBACK SAME AS IOS SLB VSERVER ADDRESS
 ip address 10.10.10.10 255.255.255.255
 no ip route-cache
 no ip mroute-cache
!
interface FastEthernet1/0
 description TO SLB
 ip address 10.1.1.201 255.255.255.0
 ip directed-broadcast
 no ip mroute-cache
 duplex half
!
interface Virtual-Template1
 description GTP VIRTUAL TEMPLATE
 ip address 192.168.1.1 255.255.255.0
 encapsulation gtp
 gprs access-point-list gprs1
```

```
!
ip route 10.111.111.111 255.255.255.255 FastEthernet1/0
!
gprs access-point-list gprs1
  access-point 1
   access-point-name gprs.company.com
   access-mode non-transparent
   ip-address-pool dhcp-proxy-client
   dhcp-server 10.100.0.5 10.100.0.6
   dhcp-gateway-address 10.27.3.1
   exit
!
gprs maximum-pdp-context-allowed 45000
gprs qos map canonical-qos
gprs gtp path-echo-interval 0
gprs dfp max-weight 32
gprs slb cef 10.10.10.10
```

GGSN2 の設定文

```
service gprs ggsn
!
hostname GGSN2
!
ip dfp agent gprs
 port 1111
 password Password1 0
 inservice
!
ip domain-name gprs.com
!
interface loopback 1
 description LOOPBACK SAME AS IOS SLB VSERVER ADDRESS
 ip address 10.10.10.10 255.255.255.255
 no ip route-cache
 no ip mroute-cache
!
interface FastEthernet1/0
 description TO SLB
 ip address 10.1.1.202 255.255.255.0
 ip directed-broadcast
 no ip mroute-cache
 duplex half
!
interface Virtual-Template1
 description GTP VIRTUAL TEMPLATE
 ip address 192.168.2.2 255.255.255.0
 encapsulation gtp
 gprs access-point-list gprs1
!
ip route 10.111.111.111 255.255.255.255 FastEthernet1/0
!
gprs access-point-list gprs1
  access-point 1
   access-point-name gprs.company.com
   access-mode non-transparent
   ip-address-pool dhcp-proxy-client
   dhcp-server 10.100.0.5 10.100.0.6
   dhcp-gateway-address 10.27.3.1
   exit
!
gprs maximum-pdp-context-allowed 45000
gprs qos map canonical-qos
```

```
gprs gtp path-echo-interval 0
gprs dfp max-weight 32
gprs slb cef 10.10.10.10
```

GGSN3 の設定文

```
service gprs ggsn
!
hostname GGSN3
!
ip dfp agent gprs
 port 1111
 password Password1 0
 inservice
!
ip domain-name gprs.com
!
interface loopback 1
 description LOOPBACK SAME AS IOS SLB VSERVER ADDRESS
 ip address 10.10.10.10 255.255.255.255
 no ip route-cache
 no ip mroute-cache
!
interface FastEthernet1/0
 description TO SLB
 ip address 10.1.1.203 255.255.255.0
 ip directed-broadcast
 no ip mroute-cache
 duplex half
!
interface Virtual-Template1
 description GTP VIRTUAL TEMPLATE
 ip address 192.168.3.3 255.255.255.0
 encapsulation gtp
 gprs access-point-list gprs1
!
ip route 10.111.111.111 255.255.255.255 FastEthernet1/0
!
gprs access-point-list gprs1
  access-point 1
   access-point-name gprs.company.com
   access-mode non-transparent
   ip-address-pool dhcp-proxy-client
   dhcp-server 10.100.0.5 10.100.0.6
   dhcp-gateway-address 10.27.3.1
   exit
!
gprs maximum-pdp-context-allowed 45000
gprs qos map canonical-qos
gprs gtp path-echo-interval 0
gprs dfp max-weight 32
gprs slb cef 10.10.10.10
```

例：GPRS ロード バランシングと NAT を使用した IOS SLB の設定方法

次の例では、図 23 のネットワークを含め、「例：GTP Cause Code Inspection がイネーブルになっていない GPRS ロード バランシングを使用した IOS SLB の設定方法」（P.163）と同じ基本設定を使用しますが、NAT を追加します。

- 「IOS SLB の設定文」（P.168）
- 「GGSN1 の設定文」（P.169）
- 「GGSN2 の設定文」（P.169）
- 「GGSN3 の設定文」（P.170）

詳細な GGSN 設定例については、『*Cisco IOS Mobile Wireless Configuration Guide*』を参照してください。

IOS SLB の設定文

```
hostname GTP_SLB
!
ip domain-name gprs.com
!
ip slb serverfarm GPRS
 nat server
 real 192.168.1.1
  weight 1
  faildetect numconns 1 numclients 1
  inservice
!
 real 192.168.2.2
  weight 1
  faildetect numconns 1 numclients 1
  inservice
!
 real 192.168.3.3
  weight 1
  faildetect numconns 1 numclients 1
  inservice
!
ip slb vserver FOR_GPRS
 virtual 10.10.10.10 udp 3386 service gtp
 serverfarm GPRS
 inservice
!
ip slb dfp password Password1 0
 agent 10.1.1.201 1111 30 0 10
 agent 10.1.1.202 1111 30 0 10
 agent 10.1.1.203 1111 30 0 10
!
interface FastEthernet1/0
 description TO SERVERFARM GPRS
 ip address 10.1.1.100 255.255.255.0
 no ip redirects
 duplex half
!
interface FastEthernet3/0
 description TO SGSN
 ip address 10.2.1.100 255.255.255.0
 no ip mroute-cache
 duplex half
!
```

```
ip route 10.111.111.111 255.255.255.255 FastEthernet1/0
ip route 192.168.1.1 255.255.255.255 10.1.1.201
ip route 192.168.2.2 255.255.255.255 10.1.1.202
ip route 192.168.3.3 255.255.255.255 10.1.1.203
```

GGSN1 の設定文

```
service gprs ggsn
!
hostname GGSN1
!
ip dfp agent gprs
 port 1111
 password Password1 0
 inservice
!
ip domain-name gprs.com
!
interface FastEthernet1/0
 description TO SLB
 ip address 10.1.1.201 255.255.255.0
 ip directed-broadcast
 no ip mroute-cache
 duplex half
!
interface Virtual-Template1
 description GTP VIRTUAL TEMPLATE
 ip address 192.168.1.1 255.255.255.0
 encapsulation gtp
 gprs access-point-list gprs1
!
ip route 10.111.111.111 255.255.255.255 FastEthernet1/0
!
gprs access-point-list gprs1
  access-point 1
   access-point-name gprs.company.com
   access-mode non-transparent
   ip-address-pool dhcp-proxy-client
   dhcp-server 10.100.0.5 10.100.0.6
   dhcp-gateway-address 10.27.3.1
   exit
!
gprs maximum-pdp-context-allowed 45000
gprs qos map canonical-qos
gprs gtp path-echo-interval 0
gprs dfp max-weight 32
```

GGSN2 の設定文

```
service gprs ggsn
!
hostname GGSN2
!
ip dfp agent gprs
 port 1111
 password Password1 0
 inservice
!
ip domain-name gprs.com
!
interface FastEthernet1/0
 description TO SLB
 ip address 10.1.1.202 255.255.255.0
```

```
 ip directed-broadcast
 no ip mroute-cache
 duplex half
interface Virtual-Template1
 description GTP VIRTUAL TEMPLATE
 ip address 192.168.2.2 255.255.255.0
 encapsulation gtp
 gprs access-point-list gprs1
!
ip route 10.111.111.111 255.255.255.255 FastEthernet1/0
!
gprs access-point-list gprs1
  access-point 1
   access-point-name gprs.company.com
   access-mode non-transparent
   ip-address-pool dhcp-proxy-client
   dhcp-server 10.100.0.5 10.100.0.6
   dhcp-gateway-address 10.27.3.1
   exit
!
gprs maximum-pdp-context-allowed 45000
gprs qos map canonical-qos
gprs gtp path-echo-interval 0
gprs dfp max-weight 32
```

GGSN3 の設定文

```
service gprs ggsn
!
hostname GGSN3
!
ip dfp agent gprs
 port 1111
 password Password1 0
 inservice
!
ip domain-name gprs.com
!
interface FastEthernet1/0
 description TO SLB
 ip address 10.1.1.203 255.255.255.0
 ip directed-broadcast
 no ip mroute-cache
 duplex half
!

interface Virtual-Template1
 description GTP VIRTUAL TEMPLATE
 ip address 192.168.3.3 255.255.255.0
 encapsulation gtp
 gprs access-point-list gprs1
!
ip route 10.111.111.111 255.255.255.255 FastEthernet1/0
!
gprs access-point-list gprs1
  access-point 1
   access-point-name gprs.company.com
   access-mode non-transparent
   ip-address-pool dhcp-proxy-client
   dhcp-server 10.100.0.5 10.100.0.6
   dhcp-gateway-address 10.27.3.1
   exit
!
```

```
gprs maximum-pdp-context-allowed 45000
gprs qos map canonical-qos
gprs gtp path-echo-interval 0
gprs dfp max-weight 32
```

例：GPRS ロード バランシング、NAT、および GTP Cause Code Inspection を使用した IOS SLB の設定方法

次の例では、図 23 のネットワークを含め、「例：GPRS ロード バランシングと NAT を使用した IOS SLB の設定方法」（P.168）と同じ基本設定を使用しますが、GTP Cause Code Inspection をイネーブルにします。この設定の場合：

- GSN アイドル タイマーは 20 秒に設定されます。
- GTP 要求のアイドル タイマーは 15 秒に設定されます。
- 仮想サーバは、キャリア コード **mcc 222 mnc 22** の International Mobile Subscriber ID（IMSI）からの PDP コンテキスト作成を受け入れます。

次に、図 23 の設定に、NAT と GTP Cause Code Inspection のサポートを追加した設定文を示します。

- 「IOS SLB の設定文」（P.171）
- 「GGSN1 の設定文」（P.169）（GTP Cause Code Inspection に変更はありません）
- 「GGSN2 の設定文」（P.169）（GTP Cause Code Inspection に変更はありません）
- 「GGSN3 の設定文」（P.170）（GTP Cause Code Inspection に変更はありません）

詳細な GGSN 設定例については、『*Cisco IOS Mobile Wireless Configuration Guide*』を参照してください。

IOS SLB の設定文

```
hostname GTP_SLB
!
ip domain-name gprs.com
!
ip slb timers gtp gsn 20
!
ip slb serverfarm GPRS
 nat server
 real 192.168.1.1
  weight 1
  faildetect numconns 1 numclients 1
  inservice
!
 real 192.168.2.2
  weight 1
  faildetect numconns 1 numclients 1
  inservice
!
 real 192.168.3.3
  weight 1
  faildetect numconns 1 numclients 1
  inservice
!
ip slb vserver FOR_GPRS
 virtual 10.10.10.10 udp 0 service gtp-inspect
 idle gtp request 15
 client gtp carrier-code mcc 222 mnc 22
 serverfarm GPRS
 inservice
```

```
!
ip slb dfp password Password1 0
 agent 10.1.1.201 1111 30 0 10
 agent 10.1.1.202 1111 30 0 10
 agent 10.1.1.203 1111 30 0 10
!
interface FastEthernet1/0
 description TO SERVERFARM GPRS
 ip address 10.1.1.100 255.255.255.0
 no ip redirects
 duplex half
!
interface FastEthernet3/0
 description TO SGSN
 ip address 10.2.1.100 255.255.255.0
 no ip mroute-cache
 duplex half
!
ip route 10.111.111.111 255.255.255.255 FastEthernet1/0
ip route 192.168.1.1 255.255.255.255 10.1.1.201
ip route 192.168.2.2 255.255.255.255 10.1.1.202
ip route 192.168.3.3 255.255.255.255 10.1.1.203
```

例：GPRS ロード バランシング マップを使用した IOS SLB の設定方法

次の設定例では、アクセス ポイント ネーム（APN）を使用してサーバ ファームを選択し、GPRS ロード バランシング仮想サーバの背後で、IOS SLB が複数のサーバ ファームをサポートできるようにします。サーバ ファーム **farm6** は関連マップなしで設定されているため、デフォルト サーバ ファームとして動作します。IOS SLB が他のサーバ ファーム マップのいずれもマッチングできない場合、IOS SLB はデフォルト サーバ ファームに GPRS 要求を送信します。

```
ip slb map 1 gtp
 apn cisco*
ip slb map 4 gtp
 apn abc.microsoft.com
 apn xyz.intel.com
ip slb map 5 gtp
 apn yahoo.com
!
ip slb serverfarm farm1
 real 10.0.0.1
 inservice
 real 10.0.0.2
 inservice
ip slb serverfarm farm2
 real 10.0.0.3
 inservice
 real 10.0.0.4
 inservice
ip slb serverfarm farm3
 real 10.0.0.5
 inservice
 real 10.0.0.6
 inservice
ip slb serverfarm farm4
 real 10.0.0.7
 inservice
 real 10.0.0.8
 inservice
ip slb serverfarm farm5
 real 10.0.0.9
 inservice
```

```
 real 10.0.0.10
 inservice
ip slb serverfarm farm6
 real 10.0.0.11
 inservice
!
ip slb map 1 gtp
 apn cisco*
ip slb map 4 gtp
 apn abc.microsoft.com
 apn xyz.intel.com
ip slb map 5 gtp
 apn yahoo.com
!
ip slb vserver GGSN_SERVER
 virtual 10.10.10.10 udp 0 service gtp
 serverfarm farm1 backup farm2 map 1 priority 3
 serverfarm farm4 map 4 priority 1
 serverfarm farm5 map 5 priority 4
 serverfarm farm6
 inservice
```

例：GTP ロード バランシング用のデュアルスタック アドレスを使用した IOS SLB の設定方法

次の設定例を使用すれば、IOS SLB で GTP ロード バランシング用のデュアルスタック アドレスをサポートすることができます。

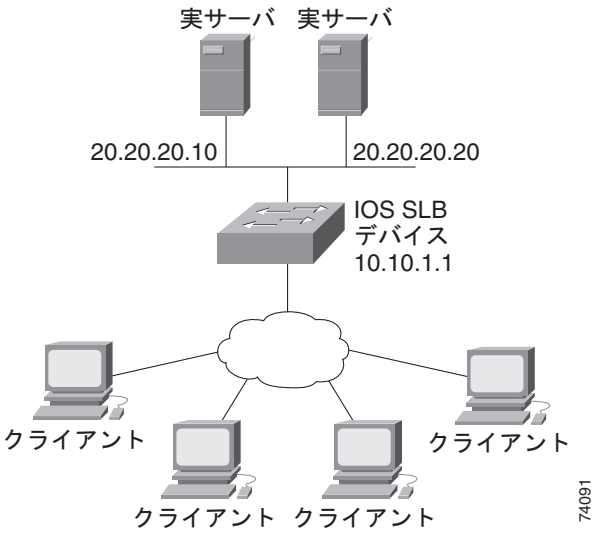
```
ip slb serverfarm SF1
 real 172.16.88.5
  weight 1
  inservice
!
ip slb serverfarm SF2
 real 172.16.88.6
  weight 1
  inservice
!
ip slb serverfarm SF3
 real 172.16.88.7 ipv6 2342:2342:2343:FF04:2388:BB03:3329:8612
  weight 1
  inservice
!
ip slb serverfarm SF4
 real 172.16.88.8 ipv6 2342:2342:2343:FF04:2388:BB03:3423:8912
  weight 1
  inservice
!
ip slb vserver VS2
 virtual 4.3.2.1 ipv6 2342:2342:2343:FF04:2341:AA03:2323:8912 udp 0 service gtp
 serverfarm sf1 backup sf2 ipv6-primary sf3 ipv6-backup sf4
 idle gtp request 90
 idle gtp imsi 10000000
 sticky gtp imsi group 1
 gtp notification cac 3
 inservice
```

例：VPN サーバ ロード バランシングを使用した IOS SLB の設定方法

図 24 に、一般的な VPN サーバ ロード バランシング設定を示します。この設定の場合：

- VPN フローの負荷は、実サーバ 20.20.20.10 および 20.20.20.20 の間で分散されます。
- クライアントは、IOS SLB 仮想サーバ アドレス 10.10.1.1 に接続します。
- ESP 仮想サーバと UDP 仮想サーバの間にはスティッキ接続があります。
- 暗号キーの交換は IKE（ISAKMP、ポート 500）経由で行われます。

図 24　　VPN サーバ ロード バランシングを使用した IOS SLB



次に、図 24 の設定の IOS SLB 設定文を示します。

```
ip slb serverfarm VPN
 nat server
 real 20.20.20.10
  inservice
 real 20.20.20.20
  inservice
 failaction purge
!
ip slb vserver ESP
 virtual 10.10.1.1 ESP
 serverfarm VPN
 sticky 3600 group 69
 inservice
!
ip slb vserver UDP
 virtual 10.10.1.1 UDP isakmp
 serverfarm VPN
 sticky 3600 group 69
 inservice
```

例：RADIUS ロード バランシングを使用した IOS SLB の設定方法

ここでは次の例を紹介し、さまざまな IOS SLB RADIUS ロード バランシング設定を示します。

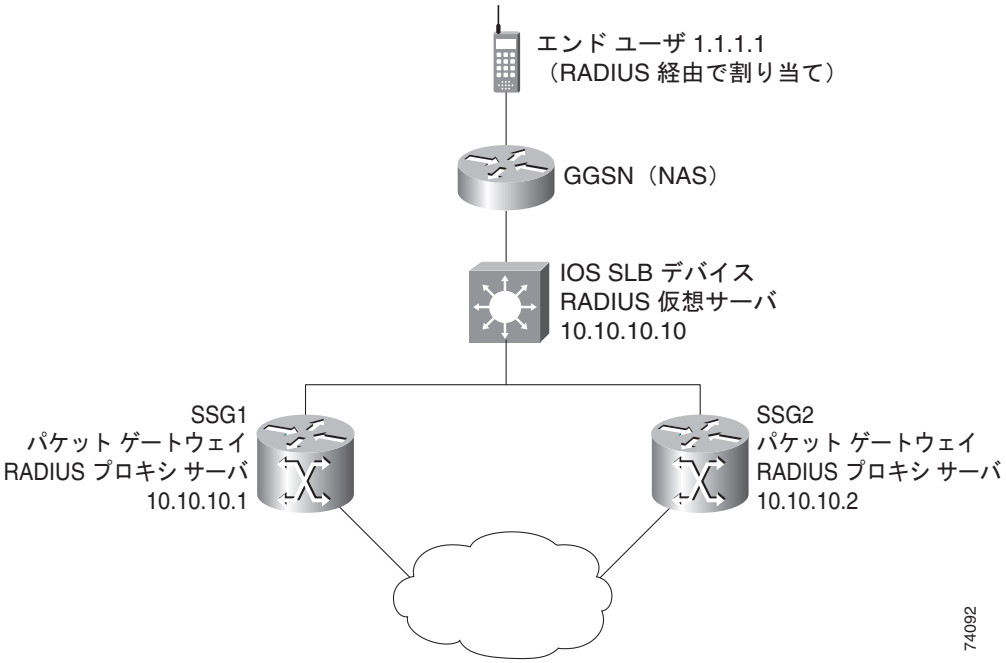
- 「例：GPRS ネットワーク用の RADIUS ロード バランシングを使用した IOS SLB の設定方法」（P.175）
- 「例：簡易 IP CDMA2000 ネットワーク用の RADIUS ロード バランシングを使用した IOS SLB の設定方法」（P.177）
- 「例：Mobile IP CDMA2000 ネットワーク用の RADIUS ロード バランシングを使用した IOS SLB の設定方法」（P.178）
- 「例：複数のサービス ゲートウェイ サーバ ファーム用の RADIUS ロード バランシングを使用した IOS SLB の設定方法」（P.179）
- 「例：RADIUS ロード バランシング/ファイアウォール ロード バランシング「サンドイッチ」を使用した IOS SLB の設定方法」（P.180）
- 「例：RADIUS ロード バランシング マップを使用した IOS SLB の設定方法」（P.182）
- 「例：RADIUS ロード バランシング加速データ プレーン フォワーディングを使用した IOS SLB の設定方法」（P.182）

例：GPRS ネットワーク用の RADIUS ロード バランシングを使用した IOS SLB の設定方法

図 25 に、GPRS ネットワークの一般的な IOS SLB RADIUS ロード バランシング設定を示します。この設定の場合：

- RADIUS 要求の負荷は、SSG RADIUS プロキシ サーバ 10.10.10.1 および 10.10.10.2 の間で分散されます。
- エンドユーザ データ パケットは、IOS SLB デバイスにルーティングされます。
- 1.1.1.0 サブネットからのエンドユーザ データ パケットは、IOS SLB から SSG1 に送信されます。
- 1.1.2.0 サブネットからのエンドユーザ データ パケットは、IOS SLB から SSG2 に送信されます。

図 25　GPRS ネットワーク用の RADIUS ロード バランシングを使用した IOS SLB



次に、図 25 の設定の IOS SLB 設定文を示します。

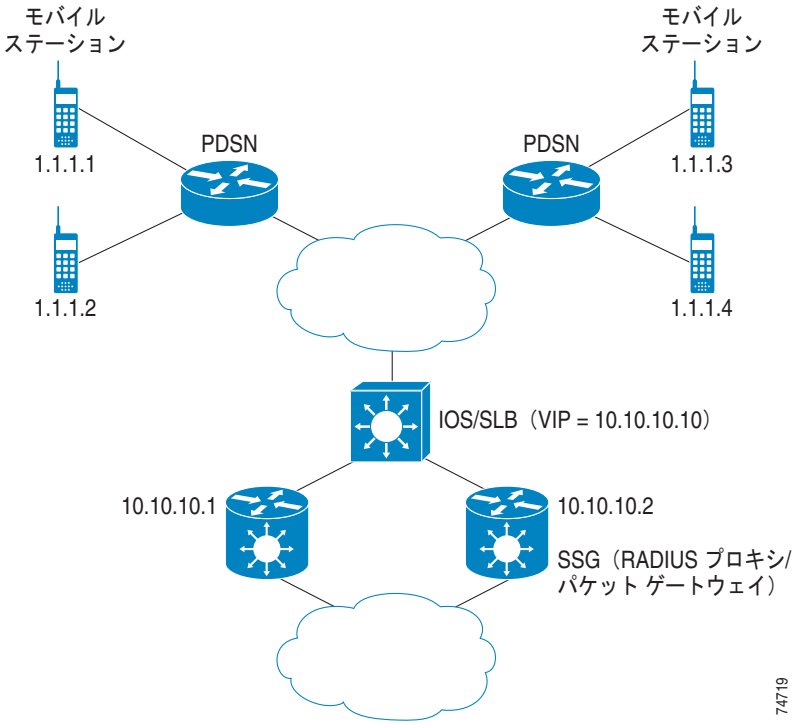
```
ip slb route 1.1.0.0 255.255.0.0 framed-ip
!
ip slb serverfarm SSGFARM
 nat server
 real 10.10.10.1
  inservice
 real 10.10.10.2
  inservice
!
ip slb vserver RADIUS_ACCT
 virtual 10.10.10.10 udp 1813 service radius
 serverfarm SSGFARM
 idle radius request 20
 idle radius framed-ip 7200
 sticky radius framed-ip group 1
 inservice
!
ip slb vserver RADIUS_AUTH
 virtual 10.10.10.10 udp 1812 service radius
 serverfarm SSGFARM
 idle radius request 20
 idle radius framed-ip 7200
 sticky radius framed-ip group 1
 inservice
```

例：簡易 IP CDMA2000 ネットワーク用の RADIUS ロード バランシングを使用した IOS SLB の設定方法

図 26 に、簡易 IP サービスを使用する CDMA2000 ネットワークの一般的な IOS SLB RADIUS ロード バランシング設定を示します。この設定の場合：

- PDSN の RADIUS 仮想サーバの IP アドレスは 10.10.10.10 です。
- RADIUS 要求の負荷は、SSG RADIUS プロキシ サーバ 10.10.10.1 および 10.10.10.2 の間で分散されます。
- エンドユーザ データ パケットは、IOS SLB デバイスにルーティングされます。
- 1.1.0.0 ネットワークからのエンドユーザ データ パケットは、SSG にルーティングされます。

図 26　簡易 IP CDMA2000 ネットワーク用の RADIUS ロード バランシングを使用した IOS SLB



次に、図 26 の設定の IOS SLB 設定文を示します。

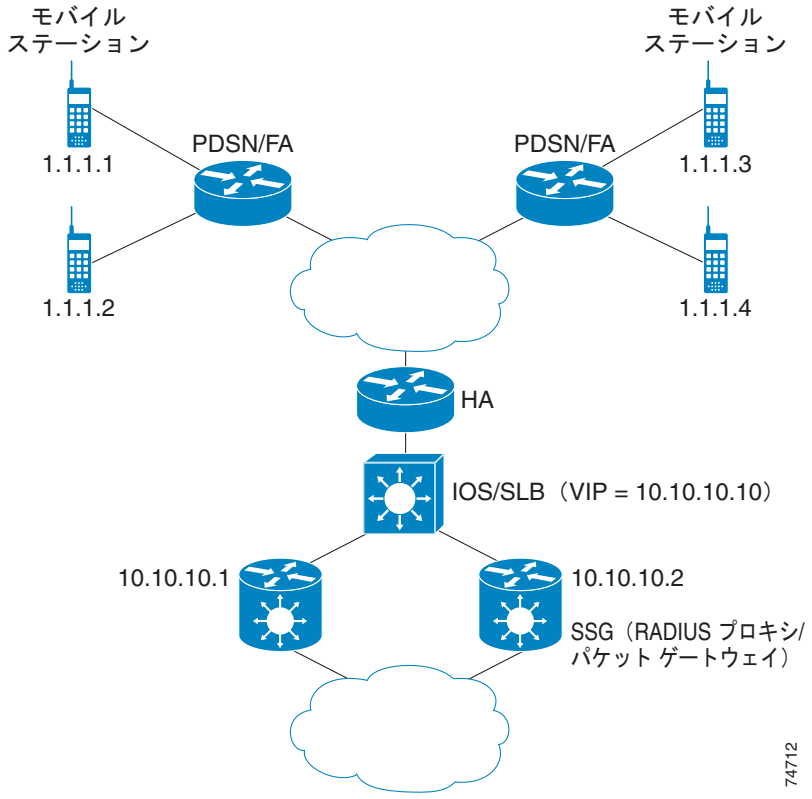
```
ip slb route 1.1.0.0 255.255.0.0 framed-ip
!
ip slb serverfarm SSGFARM
  nat server
  real 10.10.10.1
    inservice
  real 10.10.10.2
    inservice
!
ip slb vserver RADIUS_SIP
  virtual 10.10.10.10 udp 0 service radius
  serverfarm SSGFARM
  idle radius framed-ip 3600
  sticky radius username
  sticky radius framed-ip
  inservice
```

例：Mobile IP CDMA2000 ネットワーク用の RADIUS ロード バランシングを使用した IOS SLB の設定方法

図 27 に、Mobile IP サービスを使用する CDMA2000 ネットワークの一般的な IOS SLB RADIUS ロード バランシング設定を示します。この設定の場合：

- PDSN および HA の RADIUS 仮想サーバの IP アドレスは 10.10.10.10 です。
- RADIUS 要求の負荷は、SSG RADIUS プロキシ サーバ 10.10.10.1 および 10.10.10.2 の間で分散されます。
- エンドユーザ データ パケットは、IOS SLB デバイスにルーティングされます。
- 1.1.0.0 ネットワークからのエンドユーザ データ パケットは、SSG にルーティングされます。

図 27　Mobile IP CDMA2000 ネットワーク用の RADIUS ロード バランシングを使用した IOS SLB



次に、図 27 の設定の IOS SLB 設定文を示します。

```
ip slb route 1.1.0.0 255.255.0.0 framed-ip
!
ip slb serverfarm SSGFARM
  nat server
  real 10.10.10.1
    inservice
  real 10.10.10.2
    inservice
!
ip slb vserver RADIUS_SIP
  virtual 10.10.10.10 udp 0 service radius
  serverfarm SSGFARM
  idle radius framed-ip 3600
```

```
 sticky radius username
 sticky radius framed-ip
 inservice
```

例：複数のサービス ゲートウェイ サーバ ファーム用の RADIUS ロード バランシングを使用した IOS SLB の設定方法

IOS SLB は、次の設定例で複数のサービス ゲートウェイ サーバ ファーム（この例では、SSG のサーバ ファームと CSG のサーバ ファーム）のセットに対するパケット フローの負荷を分散できるようになります。

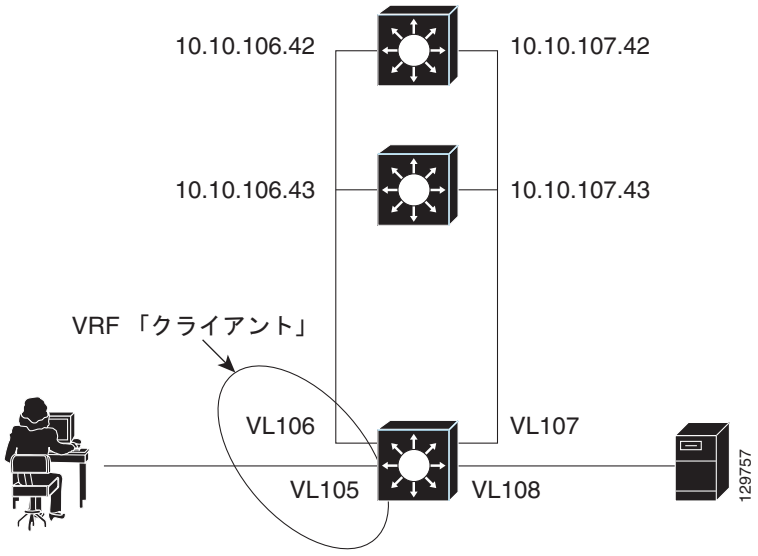
```
ip slb route 1.1.0.0 255.255.0.0 framed-ip
!
ip slb serverfarm SSGFARM
 nat server
 real 10.10.10.1
  inservice
 real 10.10.10.2
  inservice
!
ip slb serverfarm CSGFARM
 nat server
 real 20.20.20.1
  inservice
 real 20.20.20.2
  inservice
!
ip slb vserver SSG_AUTH
 virtual 10.10.10.10 udp 1812 service radius
 serverfarm SSGFARM
 idle radius request 20
 idle radius framed-ip 7200
 sticky radius framed-ip group 1
 access Vlan20 route framed-ip
 inservice
!
ip slb vserver SSG_ACCT
 virtual 10.10.10.10 udp 1813 service radius
 serverfarm SSGFARM
 idle radius request 20
 idle radius framed-ip 7200
 sticky radius framed-ip group 1
 access Vlan20 route framed-ip
 inservice
!
ip slb vserver CSG_ACCT
 virtual 20.20.20.20 udp 1813 service radius
 serverfarm CSGFARM
 idle radius request 25
 idle radius framed-ip 0
 sticky radius framed-ip
 access Vlan30 route framed-ip
 inservice
```

例：RADIUS ロード バランシング/ファイアウォール ロード バランシング「サンドイッチ」を使用した IOS SLB の設定方法

図 28 に、1 台の IOS SLB デバイス上の RADIUS ロード バランシング/ファイアウォール ロード バランシング「サンドイッチ」を示します。この設定例の場合：

- RADIUS ロード バランシングの仮想 IP アドレスは 5.5.5.5 です。
- 加入者の framed-IP ネットワークは 1.0.0.0/255.0.0.0 です。
- VL105、VL106、VL107、および VL108 は VLAN です。
- VLAN VL105 に到達する RADIUS 要求の負荷は、10.10.106.42 と 10.10.106.43 の間で分散されます。
- ユーザ トラフィックは、1.0.0.0 サブネットの framed-IP アドレスの割り当てに基づいて、スティッキ接続されます。
- 相手側（10.10.107.42/43）のファイアウォール ロード バランシングによって、加入者へのリターン パス トラフィックは、適切なゲートウェイに配信されます。

図 28　RADIUS ロード バランシング/ファイアウォール ロード バランシング「サンドイッチ」を使用した IOS SLB



次に、図 28 の設定の IOS SLB 設定文を示します。

```
ip vrf client
 rd 0:1
!
ip slb probe P742 ping
 address 10.10.107.42
 interval 120
!
ip slb probe P743 ping
 address 10.10.107.43
 interval 120
!
ip slb route 1.0.0.0 255.0.0.0 framed-ip
ip slb route framed-ip deny
!
ip slb firewallfarm SERVER
```

```
 access inbound Vlan108
 access outbound Vlan107
 inservice
 real 10.10.107.42
  probe P742
  inservice
 real 10.10.107.43
  probe P743
  inservice
 protocol tcp
  sticky 180 destination
 protocol datagram
  sticky 180 destination
 predictor hash address port
!

ip slb serverfarm SF1
 nat server
 access Vlan106
!
 real 10.10.106.42
  inservice
 real 10.10.106.43
  inservice
!
ip slb vserver VS1
 virtual 5.5.5.5 udp 0 service radius
 serverfarm SF1
 sticky radius framed-ip
 access Vlan105 route framed-ip
 access Vlan105
 inservice
!
mls flow ip interface-full
!
!************************************************
!* Switchports, port channels and trunks         *
!* added to vlans 105-108 (left out for brevity) *
!************************************************
!
interface Vlan105
 ip vrf forwarding client
 ip address 10.10.105.2 255.255.255.0
!
interface Vlan106
 ip vrf forwarding client
 ip address 10.10.106.2 255.255.255.0
!
interface Vlan107
 ip address 10.10.107.2 255.255.255.0
!
interface Vlan108
 ip address 10.10.108.2 255.255.255.0
!
ip route 10.10.105.0 255.255.255.0 10.10.107.42
ip route vrf client 10.10.108.0 255.255.255.0 10.10.106.42
```

例：RADIUS ロード バランシング マップを使用した IOS SLB の設定方法

次の設定例では、RADIUS 発信ステーション ID およびユーザ名を使用してサーバ ファームを選択し、RADIUS ロード バランシング仮想サーバの背後で、IOS SLB が複数のサーバ ファームをサポートできるようにします。サーバ ファーム **farm3** は関連マップなしで設定されているため、デフォルト サーバ ファームとして動作します。IOS SLB が他のサーバ ファーム マップのいずれもマッチングできない場合、IOS SLB はデフォルト サーバ ファームに RADIUS 要求を送信します。

```
ip slb serverfarm CSGFARM
 predictor route-map rlb-pbr
ip slb serverfarm AAAFARM
 nat server
 real 10.10.10.1
  inservice
 real 10.10.10.2
  inservice

ip slb vserver RADIUS_ACCT
 virtual 10.10.10.10 udp 1813 service radius
 serverfarm CSGFARM

 radius inject acct 1 key 0 cisco
 inservice

ip slb vserver RADIUS_AUTH
 virtual 10.10.10.10 udp 1812 service radius
 serverfarm AAAFARM
 radius inject auth 1 calling-station-id
 radius inject auth timer 45
 radius inject auth vsa cisco
 inservice

!
interface vlan 100
 ip policy route-map rlb-pbr
!
access-list 1 permit 0.0.0.1 255.255.255.254
access-list 2 permit 0.0.0.0 255.255.255.254
!
route-map rlb-pbr permit 10
 match ip address 1
 set ip next-hop 10.10.10.1
!
route-map rlb-pbr permit 20
 match ip address 2
 set ip next-hop 10.10.10.2
```

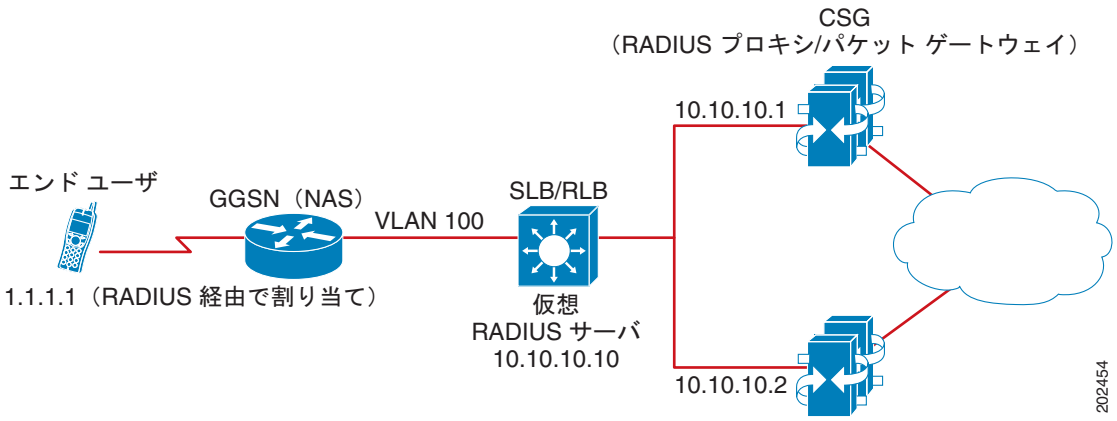
例：RADIUS ロード バランシング加速データ プレーン フォワーディングを使用した IOS SLB の設定方法

この IOS SLB 設定には、次の特徴があります。

- Network Access Server（NAS）デバイスを管理する IP アドレス 10.10.10.10 の仮想 RADIUS サーバが存在します。
- IP アドレス 10.10.10.1 および 10.10.10.2 という 2 つのパケット ゲートウェイがあります。
- 仮想 RADIUS サーバ宛ての RADIUS トラフィックは、ルート マップ **rlb-pbr** に従い、マップ済み framed-IP アドレスに基づいて、パケット ゲートウェイ間で分散されます。

- サーバ ファーム CSGFARM は、ルート マップ **rlb-pbr** の可能な結果に一致する実 IP アドレスを使用して設定されます。
- VLAN 100 に到達するエンドユーザ トラフィックは、アクセス コントロール リスト（ACL）に基づいて、適切な Cisco Content Services Gateway（CSG）にルーティングされます。
  - ACL 1 は、末尾が奇数の IP アドレスを、パケット ゲートウェイ 10.10.10.1 の背後にある CSG に送信します。
  - ACL 2 は、末尾が偶数の IP アドレスを、パケット ゲートウェイ 10.10.10.2 の背後にある CSG に送信します。

図 29　RADIUS ロード バランシング加速データ プレーン フォワーディングを使用した IOS SLB



次に、図 29 の設定の IOS SLB 設定文を示します。

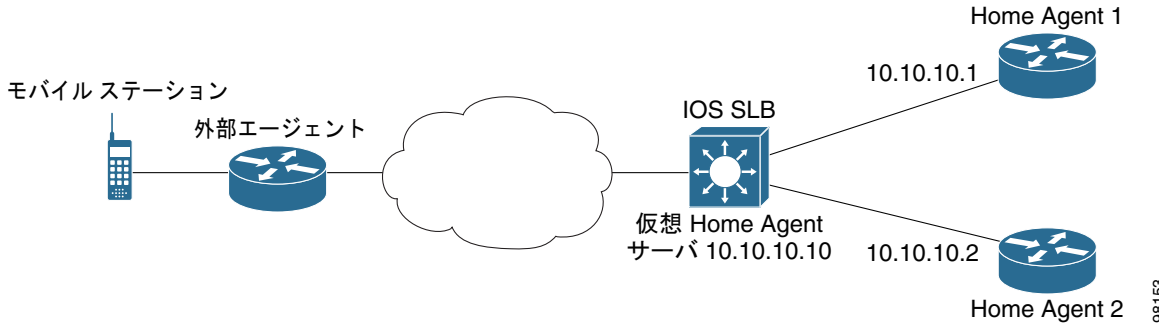
```
ip slb serverfarm CSGFARM
 predictor route-map rlb-pbr
ip slb serverfarm AAAFARM
 nat server
 real 10.10.10.1
  inservice
 real 10.10.10.2
  inservice
!
ip slb vserver RADIUS_ACCT
 virtual 10.10.10.10 udp 1813 service radius
 serverfarm CSGFARM
 radius inject acct 1 key 0 cisco
 inservice
!
ip slb vserver RADIUS_AUTH
 virtual 10.10.10.10 udp 1812 service radius
 serverfarm AAAFARM
 radius inject auth 1 calling-station-id
 radius inject auth timer 45
 radius inject auth vsa cisco
 inservice
!
interface vlan 100
 ip policy route-map rlb-pbr
!
access-list 1 permit 0.0.0.1 255.255.255.254
access-list 2 permit 0.0.0.0 255.255.255.254
!
route-map rlb-pbr permit 10
```

```
 match ip address 1
 set ip next-hop 10.10.10.1
!
route-map rlb-pbr permit 20
 match ip address 2
 set ip next-hop 10.10.10.2
```

例：Home Agent Director を使用した IOS SLB の設定方法

次の設定例では、IOS SLB が複数のホーム エージェントに Mobile IP RRQ の負荷を分散できるようにします。

図 30　　Home Agent Director を使用した IOS SLB



次に、図 30 の設定の IOS SLB 設定文を示します。

```
ip slb serverfarm HA_FARM
 nat server
 real 10.10.10.1
  inservice
 real 10.10.10.2
  inservice

ip slb vserver VIRTUAL_HA
 virtual 10.10.10.10 udp 434 service ipmobile
 serverfarm HA_FARM
 inservice
```

例：スティッキ接続を使用した IOS SLB の設定方法

次の設定例では、サブネットからのすべての HTTP 接続を、サーバ ファーム PUBLIC の同じ実サーバに割り当てます。

```
ip slb vserver http
  serverfarm PUBLIC
  sticky 30 group 1 netmask 255.255.255.248
  virtual 20.20.20.20 tcp 80
  inservice
```

次の設定例では、HTTP 接続を上記の設定に追加します。上記と同じスティッキ情報を使用しますが、仮想サーバは異なります。

```
ip slb vserver https
  serverfarm PUBLIC
  sticky 30 group 1 netmask 255.255.255.248
```

```
  virtual 20.20.20.20 tcp 443
  inservice
```

この例では、サブネットからのすべての HTTP 接続および HTTPS 接続は、同じ実サーバに割り当てられます。たとえば、あるユーザが HTTP に接続する場合、次のユーザは HTTPS に接続し、両方の接続は同じ実サーバに割り当てられます。

例：GTP IMSI スティッキ データベースを使用した IOS SLB の設定方法

次の設定例で、IOS SLB GTP IMSI スティッキ データベースをイネーブルにする方法を示します。

```
ip slb serverfarm GGSN_FARM
 failaction gtp purge
 real 10.20.10.1
  weight 1
  faildetect numconns 255 numclients 8
  inservice
!
 real 10.20.10.2
  weight 1
  faildetect numconns 255 numclients 8
  inservice
!
 real 10.20.10.3
  weight 1
  faildetect numconns 255 numclients 8
  inservice
!
ip slb vserver GGSN_SERVER1
 virtual 10.10.10.10 udp 3386 service gtp
 serverfarm GGSN_FARM backup GGSN_FARM
 idle gtp request 90
 idle gtp imsi 10000000
 sticky gtp imsi group 1
 gtp notification cac 3
 inservice
!
ip slb vserver GGSN_SERVER2
 virtual 10.10.10.10 udp 2123 service gtp
 serverfarm GGSN_FARM backup GGSN_FARM
 idle gtp request 90
 idle gtp imsi 10000000
 sticky gtp imsi group 1
 gtp notification cac 3
 inservice
```

例：ASN IMSI スティッキ データベースを使用した IOS SLB の設定方法

次の設定例は、IOS SLB ASN スティッキ データベースをイネーブルにする方法を示しています。

```
ip slb entries sticky 15000 800000
ip slb serverfarm ASNLB_FARM
 failaction asn purge
!
 real 10.20.10.1
  weight 1
  faildetect numconns 255 numclients 8
  inservice
!
```

```
 real 10.20.10.2
  weight 1
  faildetect numconns 255 numclients 8
  inservice
!
 real 10.20.10.3
  weight 1
  faildetect numconns 255 numclients 8
  inservice
!
ip slb vserver ASNLB_SERVER
 virtual 10.10.10.10 udp 0 service asn
 serverfarm ASNLB_FARM
 idle asn request 90
 idle asn msid 100000
 sticky asn msid group 1
 gw port 63082
 replicate casa 100.100.100.102 100.100.100.101 1024 password hello
 inservice
```

例：透過的 Web キャッシュ ロード バランシングを使用した IOS SLB の設定方法

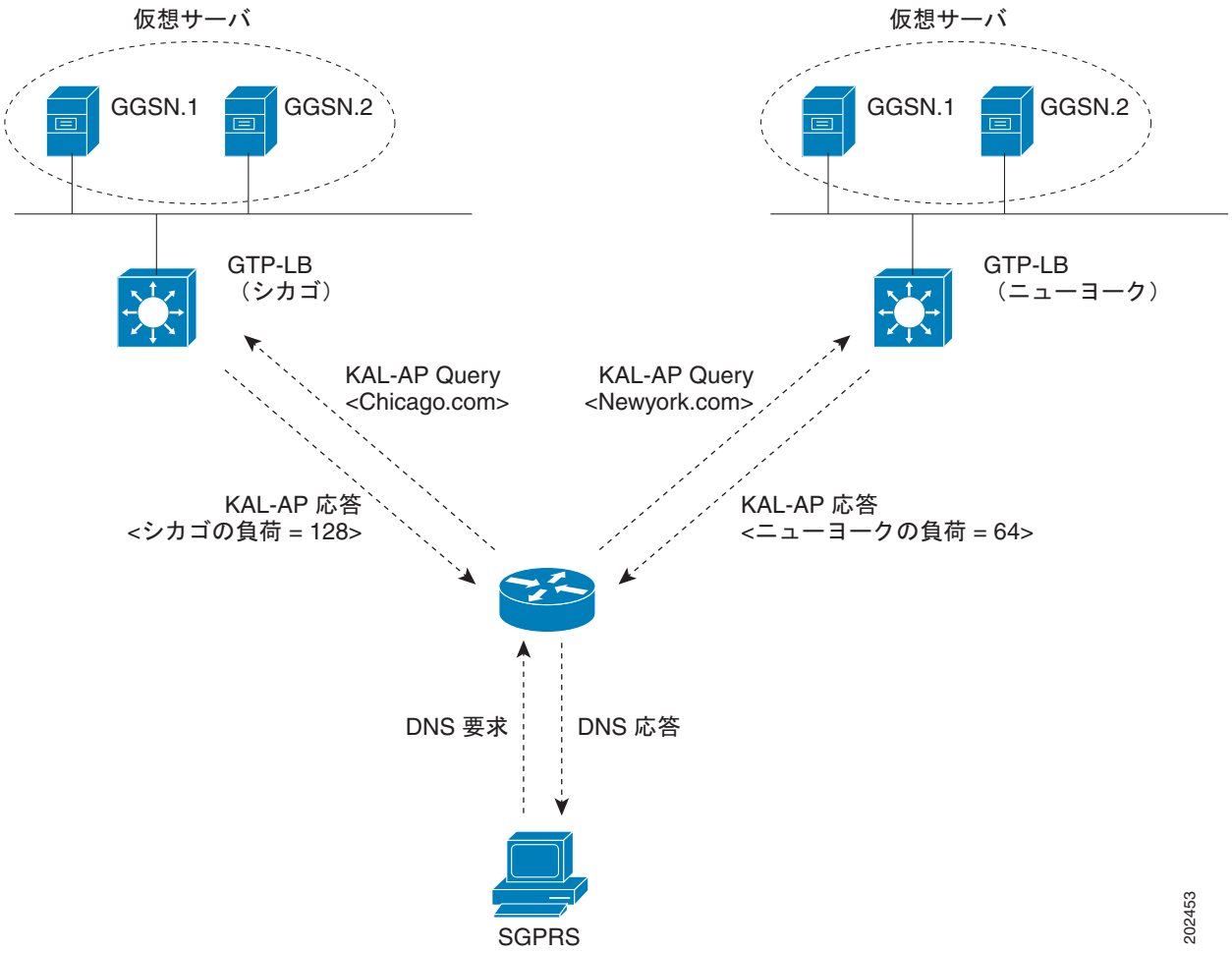
次の設定例では、仮想サーバ WEBCACHE によって、ロード バランシング デバイスを経由するすべての Web フローを確認し、サーバ ファーム WEBCACHE-FARM に送出します。**client exclude** 文によってサブネット 80.80.7.0 から発信されたフローを無視し、実サーバ 80.80.7.188 および 80.80.7.189 が必要に応じてインターネットと通信できるようにします。

```
ip slb serverfarm WEBCACHE-FARM
  real 80.80.7.188
   inservice
  real 80.80.7.189
   inservice
ip slb vserver WEBCACHE
  virtual 0.0.0.0 0.0.0.0 tcp www
  serverfarm WEBCACHE-FARM
  client 80.80.7.0 255.255.255.0 exclude
  inservice
```

例：KAL-AP エージェントを使用した IOS SLB の設定方法

次の設定例では、ドメイン ネーム システム（DNS）クエリー **abcd.com** を GSS に送信するようにクライアントを設定します。DUBLIN サイトの Global Site Selector（GSS）は、クライアントから要求を受信します。GSS は、仮想サーバからレポートされる負荷に基づき、CHICAGO（10.0.0.100）または NEWYORK（10.0.0.200）の仮想 IP アドレスを使用して DNS クエリーに応答します。

図 31　KAL-AP エージェントを使用した IOS SLB



次に、図 31 の設定の IOS SLB 設定文を示します。

GSS

```
shared-keepalive kalap 192.168.1.1 capp-secure enable key kap
shared-keepalive kalap 192.168.2.1 capp-secure enable key kap
!
answer vip 10.0.0.100 name CHICAGO activate
 keepalive type kalap tag 192.168.1.1 chicao.com
answer vip 10.0.0.200 name NEWYORK activate
 keepalive type kalap tag 192.168.2.1 newyork.com
!

answer-group ABCD owner System type vip
answer-add 10.0.0.100 name CHICAGO weight 1 order 0 load-threshold 254 activate
answer-add 10.0.0.200 name NEWYORK weight 1 order 0 load-threshold 254 activate
dns rule ABCDGPRS owner System source-address-list Anywhere domain-list abcd.com query a
 clause 1 vip-group method least-loaded ttl 20 count 1 sticky disable
```

サイト 1：IOS SLB - CHICAGO

```
ip slb capp udp
 peer port 6000 secret 0 kap
!
ip slb serverfarm SF
 kal-ap domain chicago.com
 farm-weight 200
 real 10.10.10.1
  inservice
 real 10.10.10.2
  inservice
!
ip slb vserver chicago
 virtual 10.0.0.100 udp 0
 serverfarm SF
 inservice
!
ip slb dfp
 agent 10.10.10.1 5000 30 0 10
 agent 10.10.10.2 5000 30 0 10
!
int vlan100
 ip address 192.168.1.1 255.255.255.0
```

GGSN-1

```
gprs dfp max-weight 100
gprs maximum-pdp-context-allowed 20000
!
ip dfp agent gprs
 port 5000
 inservice
```

GGSN-2

```
gprs dfp max-weight 100
gprs maximum-pdp-context-allowed 20000
!
ip dfp agent gprs
 port 5000
 inservice
```

サイト 2：IOS SLB - NEWYORK

```
ip slb capp udp
 peer port 6000
 peer 192.1.1.1 secret 0 test
 peer 10.100.100.100 port 1234
!
ip slb serverfarm SF
 kal-ap domain newyork.com
 farm-weight 6200
 real 10.20.20.1
  inservice
 real 10.20.20.2
  inservice
 real 10.20.20.3
  inservice
 real 10.20.20.4
  inservice
```

```
!
ip slb vserver chicago
 virtual 10.0.0.200 udp 0
 serverfarm SF
 inservice
!
ip slb dfp
 agent 10.10.10.1 5000 30 0 10
 agent 10.10.10.2 5000 30 0 10
!
int vlan200
 ip address 192.168.2.1 255.255.255.0
```

GGSN-1

```
gprs dfp max-weight 100
gprs maximum-pdp-context-allowed 20000
!
ip dfp agent gprs
 port 5000
 inservice
```

GGSN-2

```
gprs dfp max-weight 100
gprs maximum-pdp-context-allowed 20000
!
ip dfp agent gprs
 port 5000
 inservice
```

関連情報

次のセクションで、IOS SLB に関するその他の情報を提供します。

- 「トラブルシューティング」（P.190）
- 「サポートされているプラットフォーム」（P.192）

トラブルシューティング

質問	回答
IOS SLB を使用して、同じ LAN または VLAN 上にあるクライアントおよび実サーバの負荷を分散できますか。	**いいえ。** **IOS SLB は、同じ LAN または VLAN 上にあるクライアントおよび実サーバ間のフローのロード バランシングをサポートしていません。同じインターフェイス上のロード バランシング デバイスには、ロード バランシング対象のパケットを入出力できません。**
データを転送しているのに、IOS SLB で接続が ESTABLISHED とマークされないのはなぜですか。	dispatched モードを使用している場合、発信フローが IOS SLB をバイパスできる代替パスがないようにします。また、クライアントと実サーバが同じ IP サブネット上にない（つまり、同じ LAN または VLAN 上にない）ようにします。
実サーバに直接接続できるのに、仮想サーバに接続できないのはなぜですか。	仮想 IP アドレスが、各実サーバでループバックとして設定されていることを確認します（dispatched モードで実行している場合）。
ネットワークから実サーバの接続を解除しても、IOS SLB で実サーバが FAILED とマークされないのはなぜですか。	**numclients**、**numconns**、および **delay** の各キーワードの値を調整します。 クライアント数がごく少数の場合（たとえば、テスト環境）、**numclients** キーワードを使用すると問題が発生する可能性があります。これは、IOS SLB が少数のクライアントの障害を実サーバの障害と取り違えないようにするパラメータです。
実サーバを終了したり、物理的に接続を解除しても、IOS SLB で INSERVICE とマークされないのはなぜですか。	INSERVICE 状態および OUTOFSERVICE 状態は、ネットワーク管理者が、実サーバの動作時にその実サーバを使用する*意図*があるかどうかを示します。INSERVICE 状態で、IOS SLB の自動障害検出によって動的に選択リストから削除された実サーバは、FAILED とマークされます。これらの実サーバを表示するには、**show ip slb reals detail** コマンドを使用します。 リリース 12.1(1)E 以降、サーバ動作の実態を反映するために、INSERVICE は OPERATIONAL に変更されました。
IOS SLB スティッキ接続が適切に動作していることは、どのように確認できますか。	次の手順を使用します。 **1.** スティッキ接続を設定します。 **2.** クライアント接続を開始します。 **3.** **show ip slb reals detail** および **show ip slb conns** コマンドを入力します。 **4.** 実サーバの接続カウントを確認します。カウントが増える実サーバは、クライアント接続が割り当てられた実サーバです。 **5.** **show ip slb sticky** コマンドを入力して、IOS SLB に格納されているスティッキの関係を表示します。 **6.** 接続を終了します。 **7.** 実サーバの接続カウントが減ることを確認します。 **8.** スティッキ タイムアウト値の間待ってから、接続を再開します。 **9.** もう一度 **show ip slb conns** コマンドを入力します。 **10.** 実サーバの接続カウントをもう一度調べて、スティッキ接続は以前と同じ実サーバに割り当てられていることを確認します。

質問	回答
サーバ障害が適切に検出されていることは、どのように確認できますか。	次の手順を使用します。 1. 大量のクライアント数を使用します。クライアント数がごく少数の場合、サーバが FAILED と表示されないように、**faildetect numconns**（実サーバ）コマンドで **numclients** キーワードを調整します。 2. **show ip slb reals detail** コマンドを入力して、実サーバのステータスを表示します。 3. 実サーバのステータスと接続カウントを確認します。 – 障害が発生したサーバは、コマンドの送信時にサーバがバックアップになったことを確認するかどうかに基づいて、FAILED、TESTING、または READY_TO_TEST のステータスを示します。 – 実サーバに障害が発生すると、割り当て済みで確立していない（SYN または ACK を受信していない）接続は、**reassign** しきい値に達した後、最初に受信した SYN で、別の実サーバに再割り当てされます。ただし、確立済みの接続は同じ実サーバに転送されます。これは、新しい接続を受け入れない可能性があり、さらに既存の接続を提供している可能性があるためです。 – 加重最小接続の場合、サービスが開始されたばかりの実サーバは、新しい接続で過負荷にならないように、低速で開始されます（詳細については、「スロー スタート」（P.23）を参照してください）。そのため、新しい実サーバについて表示される接続カウントは、（新しい実サーバの低いカウントに関係なく）他の実サーバに送信される接続を示します。また、接続カウントは、新しい実サーバに対して「ダミー接続」を示します。ダミー接続は、スロー スタート期間に、IOS SLB が実サーバの接続数を意図的につり上げるために使用されます。
no inservice コマンドで、リソースは直ちにアウト オブ サービスになりますか。	**inservice** コマンドの **no** 形式を使用して、ファイアウォール、ファイアウォール ファーム、実サーバ、または仮想サーバをサービスから削除すると、各リソースは通常の手順で削除を実行します。新しい接続が割り当てられなければ、既存の接続は完了できます。 ファイアウォール ファームまたは仮想サーバ全体について、すべての既存の接続を直ちに停止するには、**clear ip slb connections** コマンドを使用します。
同じ Catalyst 6500 ファミリ スイッチに IOS SLB と入力 ACL の両方を設定すると、「TCAM Capacity Exceeded」メッセージが表示されます。なぜですか。	1 台の Catalyst 6500 ファミリ スイッチ上で IOS SLB と、入力 ACL またはファイアウォール ロード バランシングのどちらかを設定すると、ポリシー フィーチャ カード（PFC）上の Telecommunications Access Method（TCAM）の容量を超える可能性があります。この問題を解決するには、**mls ip slb search wildcard rp** コマンドを使用して、IOS SLB で使用される TCAM スペースの量を減らします。ただし、このコマンドを使用すると、ルート プロセッサの使用率が若干増加する可能性があります。
IOS SLB VRF をサポートする IOS リリースおよびプラットフォームはどれですか。	IOS SLB の Virtual Private Network（VPN）Routing and Forwarding（VRF）は、Cisco 7600 シリーズ ルータ用の MSFC3（SUP720-MSFC3）を搭載した Supervisor Engine 720 上の IOS リリース 12.2(18)SXE 以降でサポートされます。

質問	回答
スーパーバイザで表示される IOS SLB out-of-sync メッセージによって何が起こる可能性がありますか。	**replicate slave** が設定された 1 つのスーパーバイザ エンジンを使用している場合は、そのスーパーバイザで out-of-sync メッセージを受信する可能性があります。
IOS SLB は、同じスーパーバイザにファイアウォール ロード バランシングと RADIUS ロード バランシングの両方を提供できますか。	IOS SLB は、同じ Supervisor Engine 720（SUP720-MSFC3）にファイアウォール ロード バランシングと RADIUS ロード バランシングの両方を提供できます。

サポートされているプラットフォーム

スイッチまたはルータ	サポートされているプラットフォーム
Cisco 7600 シリーズ ルータ	• MSFC2A を搭載した Supervisor Engine 32（SUP32-MSFC2A） • MSFC3 を搭載した Supervisor Engine 720（SUP720-MSFC3） • 2 つのギガビット イーサネット ポートを搭載した Distributed Forwarding Card DFC3CXL 付きの Cisco Route Switch Processor 720（RSP720-3CXL-GE）

その他の参考資料

ここでは、IOS SLB に関する参考資料について説明します。

- 「関連資料」（P.193）
- 「規格」（P.193）
- 「MIB」（P.193）
- 「RFC」（P.193）
- 「シスコのテクニカル サポート」（P.194）

関連資料

内容	参照先
Cisco IOS コマンド	『*Cisco IOS Master Commands List, All Releases*』
Cisco IOS 設定の基礎	『*Cisco IOS Configuration Fundamentals Configuration Guide*』
Cisco IOS IP 設定情報	『*Cisco IOS IP Addressing Configuration Guide*』 『*Cisco IOS IP Addressing Command Reference*』 『*Cisco IOS IP Application Services Configuration Guide*』 『*Cisco IOS IP Application Services Command Reference*』
Cisco IOS モバイル ワイヤレス設定情報	『*Cisco IOS IP Mobility Configuration Guide*』 『*Cisco IOS IP Mobility Command Reference*』
DFP 設定情報	『*Dynamic Feedback Protocol Support in Distributed Director*』
CFM 設定情報	『*Using Content Flow Monitor*』

規格

規格	タイトル
この機能がサポートする新しい規格または変更された規格はありません。また、この機能による既存規格のサポートに変更はありません。	—

MIB

MIB	MIB リンク
CISCO-SLB-MIB CISCO-SLB-CAPABILITY **（注）** これらの MIB のオブジェクトは *read-create* と定義されていますが、SNMP SET コマンドを使用して変更することはできません。代わりに、コマンド ラインを使用して関連するコマンド ライン キーワードを設定します。その後に、新しい値が SNMP で反映されます。	選択されたプラットフォーム、シスコ ソフトウェア リリース、およびフィーチャ セットの MIB を検索してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
RFC 1631	「*The IP Network Address Translator (NAT)*」

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 ・テクニカル サポートを受ける ・ソフトウェアをダウンロードする ・セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける ・ツールおよびリソースへアクセスする - Product Alert の受信登録 - Field Notice の受信登録 - Bug Toolkit を使用した既知の問題の検索 ・Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する ・トレーニング リソースへアクセスする ・TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

IOS SLB の機能情報

表 2 に、この章に記載されている機能および具体的な設定情報へのリンクを示します。この表には、Cisco IOS Release 12.2(1) 以降のリリースで導入または変更された機能だけを示します。

ご使用の Cisco IOS ソフトウェア リリースによっては、コマンドの中に一部使用できないものがあります。特定のコマンドのリリース情報については、『*Cisco IOS IP Application Services Command Reference*』を参照してください。

プラットフォーム サポートとソフトウェア イメージ サポートに関する情報を入手するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator を使用すると、特定のソフトウェア リリース、フィーチャ セット、またはプラットフォームをサポートするソフトウェア イメージを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 表 2 に、特定のソフトウェア リリース トレイン内の機能に対するサポートが導入されたソフトウェア リリースだけを示します。特に断りのないかぎり、そのソフトウェア リリース トレイン以降のリリースでもその機能がサポートされます。

表 2　IOS SLB の機能情報

機能名	リリース	機能情報
IOS SLB、12.2 の最初のリリース	12.2(1) 12.2(14)S 12.2(14)ZA2 12.2(14)ZA4 12.2(14)ZA5 12.2(14)ZA6 12.2(17d)SXB 12.2(17d)SXB1 12.2(17d)SXD 12.2(17d)SXE 12.2(18)SXF 12.2(18)SXF5 12.2(18)SXF7 12.2(33)SRB 12.2(33)SRC 12.2(33)SRC1 12.2(33)SRE 15.0(1)S	IOS SLB 機能は、多様なネットワーク デバイスおよびサービスに適したロード バランシングが用意されている IOS ベースのソリューションです。
AAA ロード バランシング	12.2(14)S 12.2(14)ZA2 12.2(14)ZA4 12.2(14)ZA5 12.2(14)ZA6 12.2(17d)SXB 12.2(17d)SXB1 12.2(17d)SXD 12.2(17d)SXE 12.2(18)SXF 12.2(18)SXF5 12.2(18)SXF7 12.2(33)SRB 12.2(33)SRC 12.2(33)SRC1 12.2(33)SRE 15.0(1)S	IOS SLB には、RADIUS の Authentication, Authorization, and Accounting（AAA; 認証、認可、アカウンティング）サーバ用の RADIUS ロード バランシング機能があります。 この機能については、次の項に説明があります。 • 「AAA ロード バランシング」（P.29）

表 2　IOS SLB の機能情報 （続き）

機能名	リリース	機能情報
アクティブ スタンバイ	12.2(1) 12.2(14)S 12.2(14)ZA2 12.2(14)ZA4 12.2(14)ZA5 12.2(14)ZA6 12.2(17d)SXB 12.2(17d)SXB1 12.2(17d)SXD 12.2(17d)SXE 12.2(18)SXF 12.2(18)SXF5 12.2(18)SXF7 12.2(33)SRB 12.2(33)SRC 12.2(33)SRC1 12.2(33)SRE 15.0(1)S	アクティブ スタンバイによって、2 つの IOS SLB は同じ仮想 IP アドレスの負荷を分散すると同時に、相互にバックアップとして動作できます。 この機能に関する詳細については、次の各項を参照してください。 • 「アクティブ スタンバイ」（P.31） • 「ステートレス バックアップの設定作業リスト」（P.106） • 「例：アクティブ スタンバイを使用した IOS SLB の設定方法」（P.153）
サーバ ロード バランシングのアルゴリズム	12.2(1) 12.2(14)S 12.2(14)ZA2 12.2(14)ZA4 12.2(14)ZA5 12.2(14)ZA6 12.2(17d)SXB 12.2(17d)SXB1 12.2(17d)SXD 12.2(17d)SXE 12.2(18)SXF 12.2(18)SXF5 12.2(18)SXF7 12.2(33)SRB 12.2(33)SRC 12.2(33)SRC1 12.2(33)SRE 15.0(1)S	IOS SLB には次のロード バランシング アルゴリズムがあります。 • 「加重ラウンド ロビン アルゴリズム」（P.13） • 「加重最小接続アルゴリズム」（P.13） • 「ルート マップ アルゴリズム」（P.14） この機能に関する詳細については、次の各項を参照してください。 • 「サーバ ロード バランシングのアルゴリズム」（P.12） • 「サーバ ファームと実サーバの設定方法」（P.41）

表 2　IOS SLB の機能情報 （続き）

機能名	リリース	機能情報
代替 IP アドレス	12.2(1) 12.2(14)S 12.2(14)ZA2 12.2(14)ZA4 12.2(14)ZA5 12.2(14)ZA6 12.2(17d)SXB 12.2(17d)SXB1 12.2(17d)SXD 12.2(17d)SXE 12.2(18)SXF 12.2(18)SXF5 12.2(18)SXF7 12.2(33)SRB 12.2(33)SRC 12.2(33)SRC1 12.2(33)SRE 15.0(1)S	IOS SLB を使用すると、代替 IP アドレスを使用して、ロード バランシング デバイスに Telnet を使用できます。 この機能については、次の項に説明があります。 • 「代替 IP アドレス」（P.23）
ASN ロード バランシング	12.2(33)SRC1 12.2(33)SRE 15.0(1)S	IOS SLB は、ASN ゲートウェイのセット全体にロード バランシングを提供します。ゲートウェイのクラスタが、ベース ステーションからは 1 つの ASN ゲートウェイとして見えます。 この機能に関する詳細については、次の各項を参照してください。 • 「Cisco IOS SLB に関する制約事項」（P.3） • 「ASN ロード バランシング」（P.31） • 「ASN ロード バランシングの設定作業リスト」（P.101） この機能によって、次のコマンドが変更されました。 **debug ip slb、idle（仮想サーバ）、show ip slb sessions、show ip slb stats、show ip slb vservers、virtual**
ASN ロード バランシング：ステートフルとスティッキのサポート	12.2(33)SRE 15.0(1)S	ASN ロード バランシングは、ステートフル冗長性とスティッキ接続をサポートします。 この機能に関する詳細については、次の各項を参照してください。 • 「Cisco IOS SLB に関する制約事項」（P.3） • 「ASN ロード バランシング」（P.31） • 「ASN ロード バランシングの設定作業リスト」（P.101） この機能に関連して、次の新しいコマンドが追加されています。 **clear ip slb sticky asn msid、gw port、show ip slb sticky** この機能によって、次のコマンドが変更されました。 **debug ip slb、failaction（サーバ ファーム）、idle（仮想サーバ）、show ip slb sticky、sticky（仮想サーバ）**

表 2　IOS SLB の機能情報 （続き）

機能名	リリース	機能情報
オーディオおよびビデオのロード バランシング	12.2(1) 12.2(14)S 12.2(14)ZA2 12.2(14)ZA4 12.2(14)ZA5 12.2(14)ZA6 12.2(17d)SXB 12.2(17d)SXB1 12.2(17d)SXD 12.2(17d)SXE 12.2(18)SXF 12.2(18)SXF5 12.2(18)SXF7 12.2(33)SRB 12.2(33)SRC 12.2(33)SRC1 12.2(33)SRE 15.0(1)S	IOS SLB は、RealNetworks アプリケーションを実行しているサーバに対して、Real-Time Streaming Protocol（RTSP; リアルタイム トランスポート ストリーミング プロトコル）経由の RealAudio ストリームと RealVideo ストリームのバランスを取ることができます。 この機能については、次の項に説明があります。 • 「オーディオおよびビデオのロード バランシング」（P.29）
自動サーバ障害検出	12.2(1) 12.2(14)S 12.2(14)ZA2 12.2(14)ZA4 12.2(14)ZA5 12.2(14)ZA6 12.2(17d)SXB 12.2(17d)SXB1 12.2(17d)SXD 12.2(17d)SXE 12.2(18)SXF 12.2(18)SXF5 12.2(18)SXF7 12.2(33)SRB 12.2(33)SRC 12.2(33)SRC1 12.2(33)SRE 15.0(1)S	IOS SLB は、実サーバに対して失敗した各 TCP 接続試行を自動的に検出し、そのサーバの障害カウンタを増加します。サーバの障害カウンタが設定可能な障害しきい値を超えると、サーバはアウト オブ サービスと見なされ、アクティブな実サーバ リストから削除されます。 この機能に関する詳細については、次の各項を参照してください。 • 「自動サーバ障害検出」（P.24） • 「自動サーバ障害検出のディセーブル方法」（P.115）

表 2　IOS SLB の機能情報 （続き）

機能名	リリース	機能情報
自動サーバ障害検出：自動サーバ障害検出のディセーブル化	12.2(14)ZA4 12.2(14)ZA5 12.2(14)ZA6 12.2(17d)SXB 12.2(17d)SXB1 12.2(17d)SXD 12.2(17d)SXE 12.2(18)SXF 12.2(18)SXF5 12.2(18)SXF7 12.2(33)SRB 12.2(33)SRC 12.2(33)SRC1 12.2(33)SRE 15.0(1)S	IOS SLB は、実サーバに対して失敗した各 TCP 接続試行を自動的に検出し、そのサーバの障害カウンタを増加します。サーバの障害カウンタが設定可能な障害しきい値を超えると、サーバはアウト オブ サービスと見なされ、アクティブな実サーバ リストから削除されます。 この機能に関する詳細については、次の各項を参照してください。 • 「自動サーバ障害検出」（P.24） • 「自動サーバ障害検出のディセーブル方法」（P.115）
自動アンフェイル	12.2(1) 12.2(14)S 12.2(14)ZA2 12.2(14)ZA4 12.2(14)ZA5 12.2(14)ZA6 12.2(17d)SXB 12.2(17d)SXB1 12.2(17d)SXD 12.2(17d)SXE 12.2(18)SXF 12.2(18)SXF5 12.2(18)SXF7 12.2(33)SRB 12.2(33)SRC 12.2(33)SRC1 12.2(33)SRE 15.0(1)S	実サーバに障害が発生し、アクティブなサーバのリストから削除されると、設定可能な再試行タイマーに指定された期間、新しい接続は割り当てられません。タイマーの期限が切れると、そのサーバには新しい仮想サーバ接続を受ける資格ができ、IOS SLB から次の適格性確認の接続がサーバに送信されます。その接続が成功すると、失敗したサーバはアクティブな実サーバのリストに戻されます。接続に失敗すると、サーバはアウト オブ サービスのままで、再試行タイマーがリセットされます。失敗した接続は少なくとも 1 回は再試行が実行されます。実行されていない場合、次の適格性確認の接続もその失敗したサーバに送信されます。 この機能については、次の項に説明があります。 • 「自動アンフェイル」（P.25）

表 2　IOS SLB の機能情報 （続き）

機能名	リリース	機能情報
サーバ ファームおよびファイアウォール ファームに対する攻撃の回避	12.2(1) 12.2(14)S 12.2(14)ZA2 12.2(14)ZA4 12.2(14)ZA5 12.2(14)ZA6 12.2(17d)SXB 12.2(17d)SXB1 12.2(17d)SXD 12.2(17d)SXE 12.2(18)SXF 12.2(18)SXF5 12.2(18)SXF7 12.2(33)SRB 12.2(33)SRC 12.2(33)SRC1 12.2(33)SRE 15.0(1)S	高度なセキュア サイトであれば、特定の手順を使用して、サーバ ファームおよびファイアウォール ファームを攻撃から保護できます。 この機能については、次の項に説明があります。 • 「サーバ ファームおよびファイアウォール ファームに対する攻撃の回避」（P.23）
バックアップ サーバ ファーム	12.2(14)S 12.2(14)ZA2 12.2(14)ZA4 12.2(14)ZA5 12.2(14)ZA6 12.2(17d)SXB 12.2(17d)SXB1 12.2(17d)SXD 12.2(17d)SXE 12.2(18)SXF 12.2(18)SXF5 12.2(18)SXF7 12.2(33)SRB 12.2(33)SRC 12.2(33)SRC1 12.2(33)SRE 15.0(1)S	バックアップ サーバ ファームは、プライマリ サーバ ファームに定義されている実サーバで新しい接続を受け入れることができないときに使用できるサーバ ファームです。 この機能に関する詳細については、次の各項を参照してください。 • 「バックアップ サーバ ファーム」（P.25） • 「仮想サーバの設定方法」（P.45）

表 2　IOS SLB の機能情報 （続き）

機能名	リリース	機能情報
バインディング ID のサポート	12.2(1) 12.2(14)S 12.2(14)ZA2 12.2(14)ZA4 12.2(14)ZA5 12.2(14)ZA6 12.2(17d)SXB 12.2(17d)SXB1 12.2(17d)SXD 12.2(17d)SXE 12.2(18)SXF 12.2(18)SXF5 12.2(18)SXF7 12.2(33)SRB 12.2(33)SRC 12.2(33)SRC1 12.2(33)SRE 15.0(1)S	バインド ID を使用すれば、1 台の物理サーバを複数の仮想サーバにバインドして、サーバごとに加重を報告させることができます。したがって、単一の実サーバは、自身の複数インスタンスとして表現され、それぞれに異なるバインド ID が割り当てられます。Dynamic Feedback Protocol（DFP）はバインド ID を使用して、特定の加重が指定された実サーバのインスタンスを識別します。バインド ID が必要なのは、DFP を使用している場合だけです。 この機能に関する詳細については、次の各項を参照してください。 • 「バインディング ID のサポート」（P.14） • 「Cisco IOS SLB 用の DFP」（P.25） • 「サーバ ファームと実サーバの設定方法」（P.41）
Client-Assigned ロード バランシング	12.2(1) 12.2(14)S 12.2(14)ZA2 12.2(14)ZA4 12.2(14)ZA5 12.2(14)ZA6 12.2(17d)SXB 12.2(17d)SXB1 12.2(17d)SXD 12.2(17d)SXE 12.2(18)SXF 12.2(18)SXF5 12.2(18)SXF7 12.2(33)SRB 12.2(33)SRC 12.2(33)SRC1 12.2(33)SRE 15.0(1)S	Client-Assigned ロード バランシングでは、仮想サーバを使用する権限を持つクライアント IP サブネットのリストを指定することで、仮想サーバに対するアクセスを制限できます。この機能を使用すると、仮想 IP アドレスに接続する 1 セットのクライアント IP サブネット（内部サブネットなど）を、1 つのサーバ ファームまたはファイアウォール ファームに割り当て、別のクライアント セット（外部クライアントなど）を別のサーバ ファームまたはファイアウォール ファームに割り当てることができます。 この機能については、次の項に説明があります。 • 「Client-Assigned ロード バランシング」（P.14）
接続のレート制限	12.2(33)SRC 12.2(33)SRC1 12.2(33)SRE 15.0(1)S	IOS SLB を使用すると、サーバ ファームの 1 つの実サーバに許可する最大接続レートを指定できます。 この機能に関する詳細については、次の各項を参照してください。 • 「接続のレート制限」（P.14） • 「サーバ ファームと実サーバの設定方法」（P.41）

表 2　IOS SLB の機能情報 （続き）

機能名	リリース	機能情報
コンテンツ フロー モニタのサポート	12.2(1) 12.2(14)S 12.2(14)ZA2 12.2(14)ZA4 12.2(14)ZA5 12.2(14)ZA6 12.2(17d)SXB 12.2(17d)SXB1 12.2(17d)SXD 12.2(17d)SXE 12.2(18)SXF 12.2(18)SXF5 12.2(18)SXF7 12.2(33)SRB 12.2(33)SRC 12.2(33)SRC1 12.2(33)SRE 15.0(1)S	IOS SLB は Cisco Content Flow Monitor（CFM）をサポートします。CFM は、CiscoWorks2000 製品ファミリ内の Web ベース ステータス モニタリング アプリケーションです。CFM を使用すると、Cisco サーバ ロード バランシング デバイスを管理できます。CFM は Windows NT および Solaris ワークステーション上で動作します。CFM には Web ブラウザを使用してアクセスします。 この機能については、次の項に説明があります。 • 「コンテンツ フロー モニタのサポート」（P.15）
TCP 接続コンテキストの遅延削除	12.2(1) 12.2(14)S 12.2(14)ZA2 12.2(14)ZA4 12.2(14)ZA5 12.2(14)ZA6 12.2(17d)SXB 12.2(17d)SXB1 12.2(17d)SXD 12.2(17d)SXE 12.2(18)SXF 12.2(18)SXF5 12.2(18)SXF7 12.2(33)SRB 12.2(33)SRC 12.2(33)SRC1 12.2(33)SRE 15.0(1)S	IP パケットの順序異常が原因で、IOS SLB が、TCP 接続の終了（finish [FIN] または reset [RST]）後に、接続用の他のパケットが続いているのを検出する場合があります。一般的に、この問題は TCP 接続パケットがたどるパスが複数あるときに発生します。接続が終了した後に到着するパケットを適切にリダイレクトするために、IOS SLB が、指定された期間、TCP 接続情報（つまり、コンテキスト）を保持します。接続の終了後にコンテキストを保持する期間は、設定可能な遅延タイマーで制御されます。 この機能に関する詳細については、次の各項を参照してください。 • 「TCP 接続コンテキストの遅延削除」（P.15） • 「サーバ ファームと実サーバの設定方法」（P.41）

表 2　IOS SLB の機能情報 （続き）

機能名	リリース	機能情報
DFP のサポート	12.2(1) 12.2(14)S 12.2(14)ZA2 12.2(14)ZA4 12.2(14)ZA5 12.2(14)ZA6 12.2(17d)SXB 12.2(17d)SXB1 12.2(17d)SXD 12.2(17d)SXE 12.2(18)SXF 12.2(18)SXF5 12.2(18)SXF7 12.2(33)SRB 12.2(33)SRC 12.2(33)SRC1 12.2(33)SRE 15.0(1)S	IOS SLB は Dynamic Feedback Protocol（DFP）をサポートします。 この機能に関する詳細については、次の各項を参照してください。 • 「Cisco IOS SLB 用の DFP」（P.25） • 「DFP の設定方法」（P.70） • 「例 : GPRS ロード バランシングを使用した IOS SLB の設定方法」（P.163） • 「例 : KAL-AP エージェントを使用した IOS SLB の設定方法」（P.186）
DFP Agent Subsystem のサポート	12.2(14)S 12.2(14)ZA2 12.2(14)ZA4 12.2(14)ZA5 12.2(14)ZA6 12.2(17d)SXB 12.2(17d)SXB1 12.2(17d)SXD 12.2(17d)SXE 12.2(18)SXF 12.2(18)SXF5 12.2(18)SXF7 12.2(33)SRB 12.2(33)SRC 12.2(33)SRC1 12.2(33)SRE 15.0(1)S	IOS SLB は DFP Agent Subsystem 機能（グローバル ロード バランシングとも呼ばれます）をサポートします。そのため、IOS SLB 以外のクライアント サブシステムも DFP エージェントとして実行できます。DFP Agent Subsystem を利用すると、複数のクライアント サブシステムの複数の DFP エージェントを同時に使用できます。 この機能に関する詳細については、次の各項を参照してください。 • 「Dynamic Feedback Protocol（DFP）Agent Subsystem のサポート」（P.25） • 「DFP の設定方法」（P.70） • 「例 : GTP Cause Code Inspection がイネーブルになっていない GPRS ロード バランシングを使用した IOS SLB の設定方法」（P.163） • 「例 : GPRS ロード バランシングと NAT を使用した IOS SLB の設定方法」（P.168） • 「例 : KAL-AP エージェントを使用した IOS SLB の設定方法」（P.186）

表 2　IOS SLB の機能情報 （続き）

機能名	リリース	機能情報
DFP および Home Agent Director	12.2(17d)SXD 12.2(17d)SXE 12.2(18)SXF 12.2(18)SXF5 12.2(18)SXF7 12.2(33)SRB 12.2(33)SRC 12.2(33)SRC1 12.2(33)SRE 15.0(1)S	Home Agent Director の場合、DFP マネージャとして IOS SLB を定義し、サーバ ファームの各ホーム エージェントに DFP エージェントを定義できます。また、DFP エージェントから、ホーム エージェントの加重をレポートできます。DFP エージェントは、CPU 使用率、プロセッサ メモリ、およびホーム エージェントごとにアクティブ化できるバインディングの最大数に基づいて、各ホーム エージェントの加重を計算します この機能に関する詳細については、次の各項を参照してください。 • 「Cisco IOS SLB 用の DFP」（P.25） • 「DFP および Home Agent Director」（P.26） • 「Home Agent Director」（P.34） • 「DFP の設定方法」（P.70） • 「Home Agent Director の設定作業リスト」（P.102） • 「例：GPRS ロード バランシングを使用した IOS SLB の設定方法」（P.163） • 「例：Home Agent Director を使用した IOS SLB の設定方法」（P.184） • 「例：KAL-AP エージェントを使用した IOS SLB の設定方法」（P.186）
Exchange Director 機能	12.2(14)ZA5 12.2(14)ZA6 12.2(17d)SXB 12.2(17d)SXB1 12.2(17d)SXD 12.2(17d)SXE 12.2(18)SXF 12.2(18)SXF5 12.2(18)SXF7 12.2(33)SRB 12.2(33)SRC 12.2(33)SRC1 12.2(33)SRE 15.0(1)S	IOS SLB は、Catalyst 7600 シリーズ ルータ用の mobile Service Exchange Framework（mSEF）の場合、Exchange Director をサポートします。 この機能については、次の項に説明があります。 • 「Exchange Director 機能」（P.31）

表 2　IOS SLB の機能情報 （続き）

機能名	リリース	機能情報
ファイアウォール ロード バランシング	12.2(1) 12.2(14)S 12.2(14)ZA2 12.2(14)ZA4 12.2(14)ZA5 12.2(14)ZA6 12.2(17d)SXB 12.2(17d)SXB1 12.2(17d)SXD 12.2(17d)SXE 12.2(18)SXF 12.2(18)SXF5 12.2(18)SXF7 12.2(33)SRB 12.2(33)SRC 12.2(33)SRC1 12.2(33)SRE 15.0(1)S	この名前が示すように、ファイアウォール ロード バランシングを使用すると、IOS SLB はフローの負荷をファイアウォールに分散します。ファイアウォール ロード バランシングでは、ファイアウォール グループ（ファイアウォール ファームと呼ばれます）の両側にあるロード バランシング デバイスを使用して、各フローのトラフィックが同じファイアウォールに送信されるように確保しているため、セキュリティ ポリシーは保護されます。 この機能に関する詳細については、次の各項を参照してください。 • 「ファイアウォール ロード バランシング」（P.15） • 「ファイアウォール ロード バランシングの設定方法」（P.53） • 「例：ファイアウォール ロード バランシングを使用した IOS SLB の設定方法」（P.124）
ファイアウォール ロード バランシング：複数のファイアウォール ファームのサポート	12.2(14)S 12.2(14)ZA2 12.2(14)ZA4 12.2(14)ZA5 12.2(14)ZA6 12.2(17d)SXB 12.2(17d)SXB1 12.2(17d)SXD 12.2(17d)SXE 12.2(18)SXF 12.2(18)SXF5 12.2(18)SXF7 12.2(33)SRB 12.2(33)SRC 12.2(33)SRC1 12.2(33)SRE 15.0(1)S	各ロード バランシング デバイスに複数のファイアウォール ファームを設定できます。 この機能に関する詳細については、次の各項を参照してください。 • 「複数ファイアウォール ファームのサポート」（P.17） • 「ファイアウォール ロード バランシングの設定方法」（P.53） • 「例：複数のファイアウォール ファームを使用した IOS SLB の設定方法」（P.129）

表 2　IOS SLB の機能情報 （続き）

機能名	リリース	機能情報
ファイアウォール ロード バランシング：性能の向上	12.2(33)SRE 15.0(1)S	IOS SLB ファイアウォールのロード バランシングによって、CPU 使用率が高くなる可能性がある、特定の条件を回避できます。 この機能に関する詳細については、次の各項を参照してください。 • 「ファイアウォール ロード バランシングの設定方法」（P.53） • 「MLS エントリのプロトコル レベル消去の設定方法」（P.98） • 「接続消去要求動作の設定方法」（P.98） • 「スティッキ接続消去要求動作の設定方法」（P.99） この機能に関連して、次の新しいコマンドが追加されています。 **purge connection**、**purge sticky** この機能により次のコマンドが変更されました。 **access**（ファイアウォール ファーム）
フローの永続性	12.2(14)ZA5 12.2(14)ZA6 12.2(17d)SXB 12.2(17d)SXB1 12.2(17d)SXD 12.2(17d)SXE 12.2(18)SXF 12.2(18)SXF5 12.2(18)SXF7 12.2(33)SRB 12.2(33)SRC 12.2(33)SRC1 12.2(33)SRE 15.0(1)S	フローの永続性には、負荷分散された IP フローを適切なノードに返す、高度なリターン ルーティング機能があります。負荷分散されたデータ パスの両側でハッシュ メカニズムを調整する必要はありません。また、ネットワーク アドレス変換（NAT）やプロキシを使用して、クライアントまたはサーバの IP アドレスを変更する必要もありません。 この機能については、次の項に説明があります。 • 「フローの永続性」（P.39）

表 2　IOS SLB の機能情報 （続き）

機能名	リリース	機能情報
GPRS ロード バランシング：GTP ロード バランシングに対するデュアルスタック サポート	15.0(1)S	IPv6 サポートによって、IOS SLB ですべてのバージョンの GTP（v0、v1、v2）に対する GTP ロード バランシング用の IPv6 アドレスを管理することができます。 デュアルスタック サポートを使用すれば、IOS SLB で GTP ロード バランシング用のデュアルスタック実装を管理することができます。デュアルスタック実装とは、IPv4 アドレスと IPv6 アドレスの両方を使用する実装です。 この機能に関する詳細については、次の各項を参照してください。 • 「GTP ロード バランシングに対するデュアルスタック サポート」（P.34） • 「GPRS ロード バランシングの設定作業リスト」（P.71） • 「例：GTP ロード バランシング用のデュアルスタック アドレスを使用した IOS SLB の設定方法」（P.173） この機能では、次のコマンドが追加されました。 **show ip slb wildcard** この機能によって、次のコマンドが変更されました。 **client（仮想サーバ）、real（サーバ ファーム）、serverfarm、show ip slb reals、show ip slb serverfarms、show ip slb sessions、show ip slb sticky、show ip slb vservers、show ip slb wildcard**
GPRS ロード バランシング：GGSN-IOS SLB メッセージング	12.2(17d)SXB1 12.2(17d)SXD 12.2(17d)SXE 12.2(18)SXF 12.2(18)SXF5 12.2(18)SXF7 12.2(33)SRB 12.2(33)SRC 12.2(33)SRC1 12.2(33)SRE 15.0(1)S	特定の状況が発生した場合、GGSN ではこの機能を使用して IOS SLB に通知できます。IOS SLB では通知によって適切な判断を下すことができます。結果として、GPRS ロード バランシングと障害検出が改善されます。 この機能に関する詳細については、次の各項を参照してください。 • 「GGSN-IOS SLB メッセージング」（P.26） • 「GGSN-IOS SLB メッセージング作業リスト」（P.74）

表 2　IOS SLB の機能情報 （続き）

機能名	リリース	機能情報
GPRS ロード バランシング：GTP Cause Code Inspection	12.2(14)ZA2 12.2(14)ZA4 12.2(14)ZA5 12.2(14)ZA6 12.2(17d)SXB 12.2(17d)SXB1 12.2(17d)SXD 12.2(17d)SXE 12.2(18)SXF 12.2(18)SXF5 12.2(18)SXF7 12.2(33)SRB 12.2(33)SRC 12.2(33)SRC1 12.2(33)SRE 15.0(1)S	GTP Cause Code Inspection をイネーブルにした GPRS ロード バランシングを使用すると、IOS SLB は、GGSN サーバ ファームとの間で送受信するすべての PDP コンテキスト シグナリング フローをモニタできます。それによって、GTP 障害の原因コードをモニタし、Cisco GGSN と非 Cisco GGSN の両方について、システムレベルの問題を検出できます。 この機能に関する詳細については、次の各項を参照してください。 • 「GTP Cause Code Inspection ありの GPRS ロード バランシング」（P.33） • 「GPRS ロード バランシングの設定作業リスト」（P.71） • 「例：GPRS ロード バランシング、NAT、および GTP Cause Code Inspection を使用した IOS SLB の設定方法」（P.171）
GPRS ロード バランシング：GTP IMSI スティッキ データベース	12.2(17d)SXE 12.2(18)SXF 12.2(18)SXF5 12.2(18)SXF7 12.2(33)SRB 12.2(33)SRC 12.2(33)SRC1 12.2(33)SRE 15.0(1)S	IOS SLB では、特定の International Mobile Subscriber ID（IMSI）に Gateway General Packet Radio Service（GPRS）Support Node（GGSN）を選択し、同じ IMSI から送信される以降の Packet Data Protocol（PDP）作成要求すべてを、選択した GGSN に転送できます。 この機能に関する詳細については、次の各項を参照してください。 • 「GTP IMSI スティッキ データベース」（P.16） • 「例：GTP IMSI スティッキ データベースを使用した IOS SLB の設定方法」（P.185）
GPRS ロード バランシング：GTP Sticky-Only のサポート	12.2(33)SRE 15.0(1)S	IOS SLB は、すべてのバージョンの GTP（v0、v1、v2）に対して sticky-only をサポートします。 この機能については、次の項に説明があります。 • 「仮想サーバの設定方法」（P.45） この機能では、次のコマンドが追加されました。 **gtp session (virtual server)** この機能により次のコマンドが変更されました。 **show ip slb sticky**

表 2　IOS SLB の機能情報 （続き）

機能名	リリース	機能情報
GPRS ロード バランシング：GTP v0 のサポート	12.2(14)S 12.2(14)ZA2 12.2(14)ZA4 12.2(14)ZA5 12.2(14)ZA6 12.2(17d)SXB 12.2(17d)SXB1 12.2(17d)SXD 12.2(17d)SXE 12.2(18)SXF 12.2(18)SXF5 12.2(18)SXF7 12.2(33)SRB 12.2(33)SRC 12.2(33)SRC1 12.2(33)SRE 15.0(1)S	IOS SLB は GTP version 0（GTP v0）をサポートします。GTP のサポートによって、IOS SLB は、「GTP 認識」になり、レイヤ 5 に対する知識を拡張することができます。 この機能に関する詳細については、次の各項を参照してください。 • 「GPRS ロード バランシング」（P.32） • 「仮想サーバの設定方法」（P.45） • 「GPRS ロード バランシングの設定作業リスト」（P.71） • 「例：GPRS ロード バランシングを使用した IOS SLB の設定方法」（P.163）
GPRS ロード バランシング：GTP v1 のサポート	12.2(14)ZA2 12.2(14)ZA4 12.2(14)ZA5 12.2(14)ZA6 12.2(17d)SXB 12.2(17d)SXB1 12.2(17d)SXD 12.2(17d)SXE 12.2(18)SXF 12.2(18)SXF5 12.2(18)SXF7 12.2(33)SRB 12.2(33)SRC 12.2(33)SRC1 12.2(33)SRE 15.0(1)S	IOS SLB は、GTP version 0（GTP v0）および GTP version 1（GTP v1）の両方をサポートします。GTP のサポートによって、IOS SLB は、「GTP 認識」になり、レイヤ 5 に対する知識を拡張することができます。 この機能に関する詳細については、次の各項を参照してください。 • 「GPRS ロード バランシング」（P.32） • 「仮想サーバの設定方法」（P.45） • 「GPRS ロード バランシングの設定作業リスト」（P.71） • 「例：GPRS ロード バランシングを使用した IOS SLB の設定方法」（P.163）
GPRS ロード バランシング：GTP v2 のサポート	12.2(33)SRE 15.0(1)S	IOS SLB は GTP version 2（GTP v2）をサポートします。 この機能に関する詳細については、次の各項を参照してください。 • 「Cisco IOS SLB に関する制約事項」（P.3） • 「プロトコル サポート」（P.28） • 「仮想サーバの設定方法」（P.45） • 「GPRS ロード バランシングの設定作業リスト」（P.71）

表 2　IOS SLB の機能情報 （続き）

機能名	リリース	機能情報
GPRS ロード バランシング：マップ	12.2(33)SRB 12.2(33)SRC 12.2(33)SRC1 12.2(33)SRE 15.0(1)S	GPRS ロード バランシング マップによって、IOS SLB は Access Point Name（APN）に基づいてユーザ トラフィックを分類し、ルーティングできます。 この機能に関する詳細については、次の各項を参照してください。 • 「GPRS ロード バランシング」（P.32） • 「GPRS ロード バランシング マップの設定方法」（P.75） • 「例：GPRS ロード バランシング マップを使用した IOS SLB の設定方法」（P.172）
Home Agent Director	12.2(14)ZA2 12.2(14)ZA4 12.2(14)ZA5 12.2(14)ZA6 12.2(17d)SXB 12.2(17d)SXB1 12.2(17d)SXD 12.2(17d)SXE 12.2(18)SXF 12.2(18)SXF5 12.2(18)SXF7 12.2(33)SRB 12.2(33)SRC 12.2(33)SRC1 12.2(33)SRE 15.0(1)S	Home Agent Director は、ホーム エージェント セット（サーバ ファームの実サーバとして設定されます）の中で、Mobile IP Registration Request（RRQ）のロード バランシングを実行します。ホーム エージェントは、モバイル ノードのアンカー ポイントです。ホーム エージェントは、モバイル ノードのフローを現在の外部エージェント（接続ポイント）にルーティングします。 この機能に関する詳細については、次の各項を参照してください。 • 「Home Agent Director」（P.34） • 「Home Agent Director の設定作業リスト」（P.102） • 「例：Home Agent Director を使用した IOS SLB の設定方法」（P.184）
Hot ICE 準拠	12.2(33)SRE 15.0(1)S	すべての IOS SLB コマンドが Hot ICE 準拠です。Hot ICE は、Cisco IOS 設定管理の運用堅牢性、スケーラビリティ、およびプログラム可能性を向上させるように設計された Cisco IOS 設定機能強化のセットです。
仮想サーバの INOP_REAL 状態	12.2(33)SRC 12.2(33)SRC1 12.2(33)SRE 15.0(1)S	仮想サーバに関連付けられているすべての実サーバが非アクティブの場合、次のアクションを実行するように、仮想サーバを設定できます。 • 仮想サーバを INOP_REAL 状態に設定します。 • 仮想サーバの状態遷移について SNMP トラップを生成します。 • 仮想サーバは ICMP 要求に対する応答を停止します。 この機能に関する詳細については、次の各項を参照してください。 • 「仮想サーバの INOP_REAL 状態」（P.26） • 「仮想サーバの設定方法」（P.45）

表 2　IOS SLB の機能情報 （続き）

機能名	リリース	機能情報
インターフェイス認識	12.2(17d)SXE 12.2(18)SXF 12.2(18)SXF5 12.2(18)SXF7 12.2(33)SRB 12.2(33)SRC 12.2(33)SRC1 12.2(33)SRE 15.0(1)S	環境によっては、CSG、SSG、またはファイアウォールのファームの両側に IOS SLB が必要です。たとえば、ファームの一方で RADIUS ロード バランシングを実行し、もう一方でファイアウォール ロード バランシングを実行できます。また、ファイアウォール ファームの両側でファイアウォール ロード バランシングを実行することもできます。 このような「サンドイッチ」環境では、仮想サーバ、ファイアウォール ファーム、接続、およびセッションにパケットをマッピングするときに、IOS SLB で入力インターフェイスを考慮する必要があります。IOS SLB では、この機能はインターフェイス認識と呼ばれます。インターフェイス認識を設定すると、設定したアクセス インターフェイスに到達したトラフィックのみが処理されます（アクセス インターフェイスは任意のレイヤ 3 インターフェイスです）。 この機能に関する詳細については、次の各項を参照してください。 • 「インターフェイス認識」（P.17） • 「例：二重ファイアウォール ロード バランシング「サンドイッチ」を使用した IOS SLB の設定方法」（P.130） • 「例：RADIUS ロード バランシング/ファイアウォール ロード バランシング「サンドイッチ」を使用した IOS SLB の設定方法」（P.180）
KAL-AP エージェントのサポート	12.2(33)SRC 12.2(33)SRC1 12.2(33)SRE 15.0(1)S	KAL-AP エージェントのサポートによって、IOS SLB は Global Server Load Balancing（GSLB; グローバル サーバ ロード バランシング）環境でロード バランシングを実行できます。KAL-AP は、負荷情報とキープアライブ応答メッセージを KAL-AP マネージャまたは GSLB デバイス（Global Site Selector（GSS）など）に提供します。また、GSLB デバイスが、最も負荷が少ない IOS SLB デバイスにクライアント要求の負荷を分散できるように支援します。 この機能に関する詳細については、次の各項を参照してください。 • 「KeepAlive Application Protocol（KAL-AP）エージェントのサポート」（P.35） • 「KAL-AP エージェント サポートの設定方法」（P.77） • 「例：KAL-AP エージェントを使用した IOS SLB の設定方法」（P.186）

表 2　IOS SLB の機能情報 （続き）

機能名	リリース	機能情報
最大接続	12.2(1) 12.2(14)S 12.2(14)ZA2 12.2(14)ZA4 12.2(14)ZA5 12.2(14)ZA6 12.2(17d)SXB 12.2(17d)SXB1 12.2(17d)SXD 12.2(17d)SXE 12.2(18)SXF 12.2(18)SXF5 12.2(18)SXF7 12.2(33)SRB 12.2(33)SRC 12.2(33)SRC1 12.2(33)SRE 15.0(1)S	IOS SLB では、サーバおよびファイアウォール ロード バランシングの最大接続数を設定できます。この機能に関する詳細については、次の各項を参照してください。 • 「最大接続」（P.17） • 「サーバ ファームと実サーバの設定方法」（P.41） • 「ファイアウォール ファームの設定方法」（P.54） • 「例：包括的な IOS SLB ネットワークの設定方法」（P.123）
NAT：クライアント NAT	12.2(1) 12.2(14)S 12.2(14)ZA2 12.2(14)ZA4 12.2(14)ZA5 12.2(14)ZA6 12.2(17d)SXB 12.2(17d)SXB1 12.2(17d)SXD 12.2(17d)SXE 12.2(18)SXF 12.2(18)SXF5 12.2(18)SXF7 12.2(33)SRB 12.2(33)SRC 12.2(33)SRC1 12.2(33)SRE 15.0(1)S	ネットワークで複数のロード バランシング デバイスを使用している場合、クライアント IP アドレスを、デバイスのいずれかに関連付けられている IP アドレスで置換することで、発信フローが適切なデバイスにルーティングされます。また、クライアント NAT の場合、多数のクライアントが同じ一時ポートを使用できるため、一時クライアント ポートを変更する必要があります。複数のロード バランシング デバイスを使用しない場合でも、負荷が分散された接続のパケットがデバイス中をルーティングされないようにするには、クライアント NAT が便利です。 この機能に関する詳細については、次の各項を参照してください。 • 「クライアント NAT」（P.19） • 「NAT の設定方法」（P.104） • 「例：NAT とスタティック NAT を使用した IOS SLB の設定方法」（P.137）

表 2　IOS SLB の機能情報 （続き）

機能名	リリース	機能情報
NAT：サーバ NAT	12.2(1) 12.2(14)S 12.2(14)ZA2 12.2(14)ZA4 12.2(14)ZA5 12.2(14)ZA6 12.2(17d)SXB 12.2(17d)SXB1 12.2(17d)SXD 12.2(17d)SXE 12.2(18)SXF 12.2(18)SXF5 12.2(18)SXF7 12.2(33)SRB 12.2(33)SRC 12.2(33)SRC1 12.2(33)SRE 15.0(1)S	サーバ NAT には、仮想サーバの IP アドレスを実サーバの IP アドレスに置換する処理（およびその逆の処理）があります。 この機能に関する詳細については、次の各項を参照してください。 • 「サーバ NAT」（P.19） • 「NAT の設定方法」（P.104） • 「例：NAT とスタティック NAT を使用した IOS SLB の設定方法」（P.137）
NAT：スタティック NAT	12.2(14)S 12.2(14)ZA2 12.2(14)ZA4 12.2(14)ZA5 12.2(14)ZA6 12.2(17d)SXB 12.2(17d)SXB1 12.2(17d)SXD 12.2(17d)SXE 12.2(18)SXF 12.2(18)SXF5 12.2(18)SXF7 12.2(33)SRB 12.2(33)SRC 12.2(33)SRC1 12.2(33)SRE 15.0(1)S	スタティック NAT の場合、スタティック NAT コマンドを設定すると、アドレス変換は NAT 変換テーブルに登録され、スタティック NAT コマンドを削除するまで変換テーブルに保存されます。 この機能に関する詳細については、次の各項を参照してください。 • 「スタティック NAT」（P.19） • 「NAT の設定方法」（P.104） • 「例：スタティック NAT を使用した IOS SLB の設定方法」（P.140）

表 2　IOS SLB の機能情報 （続き）

機能名	リリース	機能情報
ポートバインド サーバ	12.2(1) 12.2(14)S 12.2(14)ZA2 12.2(14)ZA4 12.2(14)ZA5 12.2(14)ZA6 12.2(17d)SXB 12.2(17d)SXB1 12.2(17d)SXD 12.2(17d)SXE 12.2(18)SXF 12.2(18)SXF5 12.2(18)SXF7 12.2(33)SRB 12.2(33)SRC 12.2(33)SRC1 12.2(33)SRE 15.0(1)S	仮想サーバを定義するときに、そのサーバで管理する TCP ポートまたは UDP ポートを指定する必要があります。ただし、サーバ ファームで NAT を設定する場合、ポートバインド サーバを設定することもできます。ポートバインド サーバを使用すると、1 つの仮想サーバの IP アドレスで、HTTP などのサービス用の実サーバ セットと、Telnet などのサービス用の実サーバ セットを表現できます。 この機能に関する詳細については、次の各項を参照してください。 • 「ポートバインド サーバ」（P.21） • 「仮想サーバの設定方法」（P.45）
プローブ：カスタム UDP プローブ	12.2(14)ZA2 12.2(14)ZA4 12.2(14)ZA5 12.2(14)ZA6 12.2(17d)SXB 12.2(17d)SXB1 12.2(17d)SXD 12.2(17d)SXE 12.2(18)SXF 12.2(18)SXF5 12.2(18)SXF7 12.2(33)SRB 12.2(33)SRC 12.2(33)SRC1 12.2(33)SRE 15.0(1)S	IOS SLB プローブで、サーバ ファーム内の各実サーバのステータスと、ファイアウォール ファーム内の各ファイアウォールを判断します。 この機能に関する詳細については、次の各項を参照してください。 • 「プローブ」（P.27） • 「プローブの設定方法」（P.60） • 「例：プローブを使用した IOS SLB の設定方法」（P.132）

表 2　IOS SLB の機能情報 （続き）

機能名	リリース	機能情報
プローブ：DNS プローブ、Routed プローブ、および TCP プローブ	12.2(14)S 12.2(14)ZA2 12.2(14)ZA4 12.2(14)ZA5 12.2(14)ZA6 12.2(17d)SXB 12.2(17d)SXB1 12.2(17d)SXD 12.2(17d)SXE 12.2(18)SXF 12.2(18)SXF5 12.2(18)SXF7 12.2(33)SRB 12.2(33)SRC 12.2(33)SRC1 12.2(33)SRE 15.0(1)S	IOS SLB プローブで、サーバ ファーム内の各実サーバのステータスと、ファイアウォール ファーム内の各ファイアウォールを判断します。 この機能に関する詳細については、次の各項を参照してください。 • 「プローブ」（P.27） • 「プローブの設定方法」（P.60） • 「例：プローブを使用した IOS SLB の設定方法」（P.132）
プローブ：HTTP プローブ、ping プローブ、および WSP プローブ	12.2(1) 12.2(14)S 12.2(14)ZA2 12.2(14)ZA4 12.2(14)ZA5 12.2(14)ZA6 12.2(17d)SXB 12.2(17d)SXB1 12.2(17d)SXD 12.2(17d)SXE 12.2(18)SXF 12.2(18)SXF5 12.2(18)SXF7 12.2(33)SRB 12.2(33)SRC 12.2(33)SRC1 12.2(33)SRE 15.0(1)S	IOS SLB プローブで、サーバ ファーム内の各実サーバのステータスと、ファイアウォール ファーム内の各ファイアウォールを判断します。 この機能に関する詳細については、次の各項を参照してください。 • 「プローブ」（P.27） • 「プローブの設定方法」（P.60） • 「例：プローブを使用した IOS SLB の設定方法」（P.132）

表 2　IOS SLB の機能情報 （続き）

機能名	リリース	機能情報
プロトコル サポート	12.2(1) 12.2(14)S 12.2(14)ZA2 12.2(14)ZA4 12.2(14)ZA5 12.2(14)ZA6 12.2(17d)SXB 12.2(17d)SXB1 12.2(17d)SXD 12.2(17d)SXE 12.2(18)SXF 12.2(18)SXF5 12.2(18)SXF7 12.2(33)SRB 12.2(33)SRC 12.2(33)SRC1 12.2(33)SRE 15.0(1)S	IOS SLB がサポートするプロトコル セットは固定です。 この機能については、次の項に説明があります。 • 「プロトコル サポート」（P.28）
RADIUS ロード バランシング：加速データ プレーン フォワーディング	12.2(33)SRC 12.2(33)SRC1 12.2(33)SRE 15.0(1)S	RADIUS ロード バランシング加速データ プレーン フォワーディング（Turbo RADIUS ロード バランシングとも呼ばれる）は、CSG 環境で基本的な Policy-Based Routing（PBR; ポリシーベース ルーティング）ルート マップを使用して加入者のデータプレーン トラフィックを管理する高性能ソリューションです。Turbo RADIUS ロード バランシングが RADIUS ペイロードを受信すると、そのペイロードを検査して、framed-IP アトリビュートを抽出し、ルート マップを IP アドレスに適用してから、加入者を管理する CSG を決定します。 この機能に関する詳細については、次の各項を参照してください。 • 「RADIUS ロード バランシング加速データ プレーン フォワーディング」（P.38） • 「RADIUS ロード バランシング加速データ プレーン フォワーディングの設定方法」（P.86） • 「例：RADIUS ロード バランシング加速データ プレーン フォワーディングを使用した IOS SLB の設定方法」（P.182）

表 2　IOS SLB の機能情報 （続き）

機能名	リリース	機能情報
RADIUS ロード バランシング：CDMA2000	12.2(14)S 12.2(14)ZA2 12.2(14)ZA4 12.2(14)ZA5 12.2(14)ZA6 12.2(17d)SXB 12.2(17d)SXB1 12.2(17d)SXD 12.2(17d)SXE 12.2(18)SXF 12.2(18)SXF5 12.2(18)SXF7 12.2(33)SRB 12.2(33)SRC 12.2(33)SRC1 12.2(33)SRE 15.0(1)S	IOS SLB は、サービス ゲートウェイ（Cisco Service Selection Gateway（SSG）または Cisco Content Services Gateway（CSG））を使用するモバイル ワイヤレス ネットワークに RADIUS ロード バランシング機能を提供します。IOS SLB は、次の CDMA2000 モバイル ワイヤレス ネットワークについて RADIUS ロード バランシングをサポートします。 • 簡易 IP CDMA2000 ネットワーク。CDMA2000 は Third-Generation（3-G; 第 3 世代）バージョンの Code Division Multiple Access（CDMA; 符号分割多重接続）です。簡易 IP CDMA2000 モバイル ワイヤレス ネットワークの場合、RADIUS クライアントは Packet Data Service Node（PDSN）です。 • Mobile IP CDMA2000 ネットワーク。Mobile IP CDMA2000 モバイル ワイヤレス ネットワークの場合、Home Agent（HA）および PDSN/Foreign Agent（PDSN/FA）の両方が RADIUS クライアントです。 この機能に関する詳細については、次の各項を参照してください。 • 「RADIUS ロード バランシング」（P.36） • 「RADIUS ロード バランシングの設定作業リスト」（P.79） • 「例：簡易 IP CDMA2000 ネットワーク用の RADIUS ロード バランシングを使用した IOS SLB の設定方法」（P.177） • 「例：Mobile IP CDMA2000 ネットワーク用の RADIUS ロード バランシングを使用した IOS SLB の設定方法」（P.178）
RADIUS ロード バランシング：GPRS ネットワーク	12.2(14)S 12.2(14)ZA2 12.2(14)ZA4 12.2(14)ZA5 12.2(14)ZA6 12.2(17d)SXB 12.2(17d)SXB1 12.2(17d)SXD 12.2(17d)SXE 12.2(18)SXF 12.2(18)SXF5 12.2(18)SXF7 12.2(33)SRB 12.2(33)SRC 12.2(33)SRC1 12.2(33)SRE 15.0(1)S	IOS SLB は、サービス ゲートウェイ（Cisco Service Selection Gateway（SSG）または Cisco Content Services Gateway（CSG））を使用するモバイル ワイヤレス ネットワークに RADIUS ロード バランシング機能を提供します。IOS SLB は、GPRS ネットワークの場合、RADIUS ロード バランシングをサポートします。GPRS モバイル ワイヤレス ネットワークでは、RADIUS クライアントは通常 GGSN です。 この機能に関する詳細については、次の各項を参照してください。 • 「RADIUS ロード バランシング」（P.36） • 「RADIUS ロード バランシングの設定作業リスト」（P.79） • 「例：GPRS ネットワーク用の RADIUS ロード バランシングを使用した IOS SLB の設定方法」（P.175）

表 2　IOS SLB の機能情報 （続き）

機能名	リリース	機能情報
RADIUS ロード バランシング：マップ	12.2(33)SRB 12.2(33)SRC 12.2(33)SRC1 12.2(33)SRE 15.0(1)S	RADIUS ロード バランシング マップによって、IOS SLB は RADIUS 発信側ステーション ID とユーザ名に基づいてユーザ トラフィックを分類し、ルーティングすることができます。RADIUS ロード バランシング マップは、Turbo RADIUS ロード バランシングおよび RADIUS ロード バランシング アカウンティングのローカル ACK と同時に使用できません。 この機能に関する詳細については、次の各項を参照してください。 • 「RADIUS ロード バランシング」（P.36） • 「RADIUS ロード バランシング マップの設定方法」（P.84） • 「例：RADIUS ロード バランシング マップを使用した IOS SLB の設定方法」（P.182）
RADIUS ロード バランシング：複数のサービス ゲートウェイ サーバ ファーム	12.2(14)S 12.2(14)ZA2 12.2(14)ZA4 12.2(14)ZA5 12.2(14)ZA6 12.2(17d)SXB 12.2(17d)SXB1 12.2(17d)SXD 12.2(17d)SXE 12.2(18)SXF 12.2(18)SXF5 12.2(18)SXF7 12.2(33)SRB 12.2(33)SRC 12.2(33)SRC1 12.2(33)SRE 15.0(1)S	IOS SLB は、サービス ゲートウェイ（Cisco Service Selection Gateway（SSG）または Cisco Content Services Gateway（CSG））を使用するモバイル ワイヤレス ネットワークに RADIUS ロード バランシング機能を提供します。IOS SLB は、複数のサービス ゲートウェイ サーバ ファームの場合に RADIUS ロード バランシングをサポートします（たとえば、SSG ファームと CSG ファーム）。 この機能に関する詳細については、次の各項を参照してください。 • 「RADIUS ロード バランシング」（P.36） • 「RADIUS ロード バランシングの設定作業リスト」（P.79） • 「例：複数のサービス ゲートウェイ サーバ ファーム用の RADIUS ロード バランシングを使用した IOS SLB の設定方法」（P.179）
RADIUS ロード バランシング：RADIUS IMSI スティッキ データベース	12.2(17d)SXE 12.2(18)SXF 12.2(18)SXF5 12.2(18)SXF7 12.2(33)SRB 12.2(33)SRC 12.2(33)SRC1 12.2(33)SRE 15.0(1)S	IOS SLB RADIUS International Mobile Subscriber ID（IMSI）は、各ユーザの IMSI アドレスを対応するゲートウェイにルーティングします。その結果、同じユーザに対する以降のすべてのフローを同じゲートウェイに転送できるようになります。 この機能に関する詳細については、次の各項を参照してください。 • 「RADIUS ロード バランシング」（P.36） • 「RADIUS ロード バランシングの設定作業リスト」（P.79）

表 2　IOS SLB の機能情報 （続き）

機能名	リリース	機能情報
ルート ヘルス インジェクション	12.2(14)S 12.2(14)ZA2 12.2(14)ZA4 12.2(14)ZA5 12.2(14)ZA6 12.2(17d)SXB 12.2(17d)SXB1 12.2(17d)SXD 12.2(17d)SXE 12.2(18)SXF 12.2(18)SXF5 12.2(18)SXF7 12.2(33)SRB 12.2(33)SRC 12.2(33)SRC1 12.2(33)SRE 15.0(1)S	（**inservice** コマンドを使用して）仮想サーバをサービスに登録すると、デフォルトで、仮想サーバの IP アドレスがアドバタイズされます（ルーティング テーブルに追加されます）。Web サイトの仮想 IP アドレスに対して希望のホスト ルートがある場合、そのホスト ルートをアドバタイズできますが、その IP アドレスを使用できるという保証はありません。ただし、IP アドレスを使用できると IOS SLB で検証された場合にだけ、ホスト ルートをアドバタイズするように、**advertise** コマンドで IOS SLB を設定できます。IP アドレスを使用できなくなると、IOS SLB はアドバタイズメントを撤回します。この機能はルート ヘルス インジェクションと呼ばれます。 この機能に関する詳細については、次の各項を参照してください。 • 「ルート ヘルス インジェクション」（P.21） • 「仮想サーバの設定方法」（P.45） • 「例：ルート ヘルス インジェクションを使用した IOS SLB の設定方法」（P.160）
スロー スタート	12.2(1) 12.2(14)S 12.2(14)ZA2 12.2(14)ZA4 12.2(14)ZA5 12.2(14)ZA6 12.2(17d)SXB 12.2(17d)SXB1 12.2(17d)SXD 12.2(17d)SXE 12.2(18)SXF 12.2(18)SXF5 12.2(18)SXF7 12.2(33)SRB 12.2(33)SRC 12.2(33)SRC1 12.2(33)SRE 15.0(1)S	加重最小接続ロード バランシングを使用する環境では、起動した直後の実サーバには接続がないため、新しい接続が多数割り当てられ、過負荷になる可能性があります。このような過負荷を回避するために、スロー スタートによって、起動した直後の実サーバに割り当てられる新しい接続数を制御します。 この機能については、次の項に説明があります。 • 「スロー スタート」（P.23）

表 2　IOS SLB の機能情報 （続き）

機能名	リリース	機能情報
ステートフル バックアップ	12.2(1) 12.2(14)S 12.2(14)ZA2 12.2(14)ZA4 12.2(14)ZA5 12.2(14)ZA6 12.2(17d)SXB 12.2(17d)SXB1 12.2(17d)SXD 12.2(17d)SXE 12.2(18)SXF 12.2(18)SXF5 12.2(18)SXF7 12.2(33)SRB 12.2(33)SRC 12.2(33)SRC1 12.2(33)SRE 15.0(1)S	ステートフル バックアップを使用すると、ロード バランシングの決定を段階的にバックアップするか、プライマリ スイッチとバックアップ スイッチ間で「状態を維持」できます。バックアップ スイッチは、HSRP がフェールオーバーを検出するまで、仮想サーバを休止状態にしたままにします。検出後、バックアップ（現在はプライマリ）スイッチは、仮想アドレスのアドバタイズとフローの処理を開始します。 この機能に関する詳細については、次の各項を参照してください。 • 「ステートフル バックアップ」（P.30） • 「冗長ルート プロセッサのステートフル バックアップの設定作業リスト」（P.108） • 「例：ステートフル バックアップを使用した IOS SLB の設定方法」（P.150） • 「例：冗長ルート プロセッサのステートフル バックアップを使用した IOS SLB の設定方法」（P.152）
ステートフル バックアップ：冗長ルート プロセッサ	12.2(14)ZA5 12.2(14)ZA6 12.2(17d)SXB 12.2(17d)SXB1 12.2(17d)SXD 12.2(17d)SXE 12.2(18)SXF 12.2(18)SXF5 12.2(18)SXF7 12.2(33)SRB 12.2(33)SRC 12.2(33)SRC1 12.2(33)SRE 15.0(1)S	Cisco 7600 シリーズ ルータで、RPR+ を併用する場合、IOS SLB は mSEF について冗長ルート プロセッサのステートフル バックアップをサポートします。これによって、IOS SLB と同じシャーシに、Cisco Multiprocessor WAN Application Module（MWAN）を配置し、さらにロード バランシング割り当てのハイ アベイラビリティを維持できます。 この機能に関する詳細については、次の各項を参照してください。 • 「冗長ルート プロセッサのステートフル バックアップ」（P.39） • 「冗長ルート プロセッサのステートフル バックアップの設定作業リスト」（P.108） • 「例：冗長ルート プロセッサのステートフル バックアップを使用した IOS SLB の設定方法」（P.152）

表 2　IOS SLB の機能情報 （続き）

機能名	リリース	機能情報
ステートレス バックアップ	12.2(1) 12.2(14)S 12.2(14)ZA2 12.2(14)ZA4 12.2(14)ZA5 12.2(14)ZA6 12.2(17d)SXB 12.2(17d)SXB1 12.2(17d)SXD 12.2(17d)SXE 12.2(18)SXF 12.2(18)SXF5 12.2(18)SXF7 12.2(33)SRB 12.2(33)SRC 12.2(33)SRC1 12.2(33)SRE 15.0(1)S	ステートレス バックアップは、1 台のレイヤ 3 スイッチの可用性に依存せずに、イーサネット ネットワーク上のホストからの IP フローをルーティングすることによって、ネットワークの高可用性を実現します。Router Discovery Protocol（System-to-Intermediate System（IS-IS）Interdomain Routing Protocol（IDRP）など）をサポートしないホストで、新しいレイヤ 3 スイッチにシフトする機能がない場合は特に、ステートレス バックアップが有効です。 この機能に関する詳細については、次の各項を参照してください。 • 「ステートレス バックアップ」（P.30） • 「ステートレス バックアップの設定作業リスト」（P.106） • 「例：ステートレス バックアップを使用した IOS SLB の設定方法」（P.141）
スティッキ接続	12.2(1) 12.2(14)S 12.2(14)ZA2 12.2(14)ZA4 12.2(14)ZA5 12.2(14)ZA6 12.2(17d)SXB 12.2(17d)SXB1 12.2(17d)SXD 12.2(17d)SXE 12.2(18)SXF 12.2(18)SXF5 12.2(18)SXF7 12.2(33)SRB 12.2(33)SRC 12.2(33)SRC1 12.2(33)SRE 15.0(1)S	クライアント トランザクションには、複数の連続する接続が必要なことがあります。つまり、同じクライアントの IP アドレスまたはサブネットからの新しい接続を、同じ実サーバに割り当てる必要があります。オプションの **sticky** コマンドを使用すると、同じクライアントからの発信を、サーバ ファーム内の同じロード バランシング サーバに強制的に接続できます。ファイアウォール ロード バランシングの場合、同じクライアント - サーバ ペア間の接続は、同じファイアウォールに割り当てられます。 この機能に関する詳細については、次の各項を参照してください。 • 「スティッキ接続」（P.21） • 「サーバ ファームと実サーバの設定方法」（P.41） • 「仮想サーバの設定方法」（P.45） • 「ファイアウォール ファームの設定方法」（P.54） • 「例：スティッキ接続を使用した IOS SLB の設定方法」（P.184）
サブインターフェイスのサポート	12.2(33)SRE 15.0(1)S	IOS SLB は、**access** コマンドについてサブインターフェイスのサポートを提供しています。 この機能に関する詳細については、次の各項を参照してください。 • 「サーバ ファームと実サーバの設定方法」（P.41） • 「仮想サーバの設定方法」（P.45） • 「ファイアウォール ファームの設定方法」（P.54） この機能によって、次のコマンドが変更されました。 **access（ファイアウォール ファーム）**、**access（サーバ ファーム）**、**access（仮想サーバ）**

表 2　IOS SLB の機能情報 （続き）

機能名	リリース	機能情報
12.2(1) と 12.2(14)S に対してサポートされているプラットフォーム	12.2(1) 12.2(14)S	次のプラットフォームに対するサポートのみが含まれる一覧表示されたリリースの IOS SLB： • Cisco 7200 シリーズ ルータ
12.2(14)ZA2、 12.2(14)ZA2、 12.2(14)ZA4、 12.2(14)ZA5、および 12.2(14)ZA6 に対してサポートされているプラットフォーム	12.2(14)ZA2 12.2(14)ZA4 12.2(14)ZA5 12.2(14)ZA6	次のプラットフォームに対するサポートのみが含まれる一覧表示されたリリースの IOS SLB： • Cisco 7100 シリーズ ルータ • Cisco 7200 シリーズ ルータ • Cisco Catalyst 6500 シリーズ スイッチ用の MSFC2 が搭載された Supervisor Engine 1 • Cisco Catalyst 6500 シリーズ スイッチ用の MSFC2 が搭載された Supervisor Engine 2（SUP2-MSFC2） • Cisco 7600 シリーズ ルータ用の MSFC2 搭載の Supervisor Engine 1 • Cisco 7600 シリーズ ルータ用の MSFC2 搭載の Supervisor Engine 2（SUP2-MSFC2）
12.2(17d)SXB と 12.2(17d)SXB1 に対してサポートされているプラットフォーム	12.2(17d)SXB 12.2(17d)SXB1	次のプラットフォームに対するサポートのみが含まれる一覧表示されたリリースの IOS SLB： • Cisco Catalyst 6500 シリーズ スイッチ用の MSFC2 が搭載された Supervisor Engine 2（SUP2-MSFC2） • Cisco 7600 シリーズ ルータ用の MSFC2 搭載の Supervisor Engine 2（SUP2-MSFC2）
12.2(17d)SXD、 12.2(17d)SXE、および 12.2(18)SXF に対してサポートされているプラットフォーム	12.2(17d)SXD 12.2(17d)SXE 12.2(18)SXF	次のプラットフォームに対するサポートのみが含まれる一覧表示されたリリースの IOS SLB： • Cisco Catalyst 6500 シリーズ スイッチ用の MSFC2 が搭載された Supervisor Engine 2（SUP2-MSFC2） • Cisco Catalyst 6500 シリーズ スイッチ用の MSFC3 が搭載された Supervisor Engine 720（SUP720-MSFC3） • Cisco 7600 シリーズ ルータ用の MSFC2 搭載の Supervisor Engine 2（SUP2-MSFC2） • Cisco 7600 シリーズ ルータ用の MSFC3 搭載の Supervisor Engine 720（SUP720-MSFC3）

表 2　IOS SLB の機能情報 （続き）

機能名	リリース	機能情報
12.2(17d)SXF5 と 12.2(18)SXF7 に対してサポートされているプラットフォーム	12.2(18)SXF5 12.2(18)SXF7	次のプラットフォームに対するサポートのみが含まれる一覧表示されたリリースの IOS SLB： • Cisco Catalyst 6500 シリーズ スイッチ用の MSFC2 が搭載された Supervisor Engine 2（SUP2-MSFC2） • Cisco Catalyst 6500 シリーズ スイッチ用の MSFC2A が搭載された Supervisor Engine 32（SUP32-MSFC2A） • Cisco Catalyst 6500 シリーズ スイッチ用の MSFC3 が搭載された Supervisor Engine 720（SUP720-MSFC3） • Cisco 7600 シリーズ ルータ用の MSFC2 搭載の Supervisor Engine 2（SUP2-MSFC2） • Cisco 7600 シリーズ ルータ用の MSFC2A 搭載の Supervisor Engine 32（SUP32-MSFC2A） • Cisco 7600 シリーズ ルータ用の MSFC3 搭載の Supervisor Engine 720（SUP720-MSFC3）
12.2(33)SRB に対してサポートされているプラットフォーム	12.2(33)SRB	次のプラットフォームに対するサポートのみが含まれる一覧表示されたリリースの IOS SLB： • Cisco 7600 シリーズ ルータ用の MSFC2A 搭載の Supervisor Engine 32（SUP32-MSFC2A） • Cisco 7600 シリーズ ルータ用の MSFC3 搭載の Supervisor Engine 720（SUP720-MSFC3）
12.2(33)SRC、12.2(33)SRC1、12.2(33)SRE、および 15.0(1)S に対してサポートされているプラットフォーム	12.2(33)SRC 12.2(33)SRC1 12.2(33)SRE 15.0(1)S	次のプラットフォームに対するサポートのみが含まれる一覧表示されたリリースの IOS SLB： • Cisco 7600 シリーズ ルータ用の MSFC2A 搭載の Supervisor Engine 32（SUP32-MSFC2A） • Cisco 7600 シリーズ ルータ用の MSFC3 搭載の Supervisor Engine 720（SUP720-MSFC3） • 2 つのギガビット イーサネット ポートを搭載した Distributed Forwarding Card DFC3CXL 付きの Cisco Route Switch Processor 720（RSP720-3CXL-GE）

表 2　IOS SLB の機能情報 （続き）

機能名	リリース	機能情報
SynGuard	12.2(1) 12.2(14)S 12.2(14)ZA2 12.2(14)ZA4 12.2(14)ZA5 12.2(14)ZA6 12.2(17d)SXB 12.2(17d)SXB1 12.2(17d)SXD 12.2(17d)SXE 12.2(18)SXF 12.2(18)SXF5 12.2(18)SXF7 12.2(33)SRB 12.2(33)SRC 12.2(33)SRC1 12.2(33)SRE 15.0(1)S	SynGuard は、仮想サーバによって管理される TCP start-of-connection パケット（SYN）のレートを制限して、SYN フラッド サービス拒否攻撃と呼ばれるネットワーク上の問題を阻止します。ユーザが大量の SYN をサーバに送信することもあり、それによってサーバの過負荷やクラッシュが発生し、他のユーザへのサービスが停止する可能性があります。SynGuard によって、IOS SLB または実サーバを停止させる攻撃などを回避します。SynGuard は、仮想サーバによって管理される SYN 数を一定間隔でモニタして、その数が、設定された SYN しきい値を超えないようにします。しきい値に達すると、新しい SYN はドロップされます。 この機能に関する詳細については、次の各項を参照してください。 • 「SynGuard」（P.24） • 「仮想サーバの設定方法」（P.45） • 「例：包括的な IOS SLB ネットワークの設定方法」（P.123）
TCP セッションの再割り当て	12.2(1) 12.2(14)S 12.2(14)ZA2 12.2(14)ZA4 12.2(14)ZA5 12.2(14)ZA6 12.2(17d)SXB 12.2(17d)SXB1 12.2(17d)SXD 12.2(17d)SXE 12.2(18)SXF 12.2(18)SXF5 12.2(18)SXF7 12.2(33)SRB 12.2(33)SRC 12.2(33)SRC1 12.2(33)SRE 15.0(1)S	クライアントが実サーバに対して新しい接続を開こうとしている場合、そのサーバに送信される各 TCP SYN は IOS SLB によって追跡されます。複数の連続する SYN に応答がない場合、または SYN が RST で応答される場合、TCP セッションは新しい実サーバに再割り当てされます。SYN の試行回数は、設定可能な再割り当てしきい値で制御されます。 この機能に関する詳細については、次の各項を参照してください。 • 「TCP セッションの再割り当て」（P.22） • 「サーバ ファームと実サーバの設定方法」（P.41） • 「GPRS ロード バランシングの設定作業リスト」（P.71）

表 2　IOS SLB の機能情報 （続き）

機能名	リリース	機能情報
透過的 Web キャッシュ ロード バランシング	12.2(1) 12.2(14)S 12.2(14)ZA2 12.2(14)ZA4 12.2(14)ZA5 12.2(14)ZA6 12.2(17d)SXB 12.2(17d)SXB1 12.2(17d)SXD 12.2(17d)SXE 12.2(18)SXF 12.2(18)SXF5 12.2(18)SXF7 12.2(33)SRB 12.2(33)SRC 12.2(33)SRC1 12.2(33)SRE 15.0(1)S	IOS SLB は、透過的 Web キャッシュのクラスタ全体で HTTP フローの負荷を分散できます。この機能をセットアップするには、透過的 Web キャッシュで処理するサブネット IP アドレス、または何らかの共通するサブセットを仮想サーバとして設定します。透過的 Web キャッシュ ロード バランシングに使用する仮想サーバは、サブネット IP アドレスの代理で ping に応答しません。また、トレースルートに影響がありません。 この機能に関する詳細については、次の各項を参照してください。 • 「透過的 Web キャッシュ ロード バランシング」（P.22） • 「仮想サーバの設定方法」（P.45） • 「例：透過的 Web キャッシュ ロード バランシングを使用した IOS SLB の設定方法」（P.186）
VPN サーバ ロード バランシング	12.2(14)S 12.2(14)ZA2 12.2(14)ZA4 12.2(14)ZA5 12.2(14)ZA6 12.2(17d)SXB 12.2(17d)SXB1 12.2(17d)SXD 12.2(17d)SXE 12.2(18)SXF 12.2(18)SXF5 12.2(18)SXF7 12.2(33)SRB 12.2(33)SRC 12.2(33)SRC1 12.2(33)SRE 15.0(1)S	IOS SLB は、VPN フローのバランスを取ることができます。 この機能に関する詳細については、次の各項を参照してください。 • 「VPN サーバ ロード バランシング」（P.30） • 「VPN サーバ ロード バランシングの設定作業リスト」（P.99） • 「例 : VPN サーバ ロード バランシングを使用した IOS SLB の設定方法」（P.174）

表 2　IOS SLB の機能情報 （続き）

機能名	リリース	機能情報
WAP ロード バランシング	12.2(1) 12.2(14)S 12.2(14)ZA2 12.2(14)ZA4 12.2(14)ZA5 12.2(14)ZA6 12.2(17d)SXB 12.2(17d)SXB1 12.2(17d)SXD 12.2(17d)SXE 12.2(18)SXF 12.2(18)SXF5 12.2(18)SXF7 12.2(33)SRB 12.2(33)SRC 12.2(33)SRC1 12.2(33)SRE 15.0(1)S	IOS SLB を使用すると、IP ベアラ ネットワークの WAP ゲートウェイまたはサーバのグループ内で、Wireless Session Protocol（WSP）セッションの負荷を分散できます。 この機能に関する詳細については、次の各項を参照してください。 • 「WAP ロード バランシング」（P.39） • 「仮想サーバの設定方法」（P.45） • 「WSP プローブの設定方法」（P.67） • 「例：WAP および UDP ロード バランシングを使用した IOS SLB の設定方法」（P.158）
—	12.2(14)ZA6 12.2(18)SXF 12.2(18)SXF5 12.2(18)SXF7	これらのリリースには、マイナーな修正と明確化が施されているだけです。新しい機能は導入されていません。