



## サーバ ロード バランシングの設定

---

このマニュアルでは、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ドキュメントを探すには、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。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、仮想サーバの IP アドレスにセット属性するようにクライアントを設定します。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。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、IOS SLB 機能によって接続の実サーバが設定されます。

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、アカウントティング)、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。

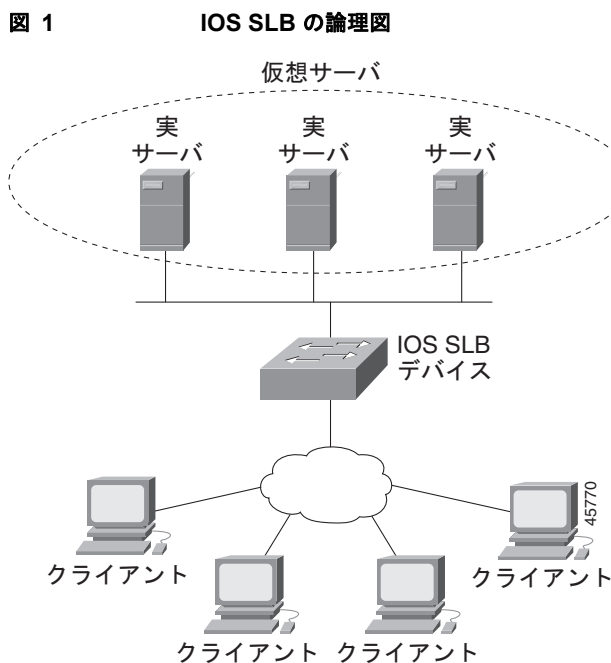
- mobile Service Exchange Framework (mSEF) コンポーネント：
  - Cisco Content Services Gateway (CSG)  
Supervisor Engine 32 (SUP32-MSFC2A) とともに実行している場合、CSG リリース 3.1(3)C7(1) 以降が必要です。
  - Cisco Gateway GPRS サポート ノード (GGSN)
  - Cisco Service Selection Gateway (SSG)
  - Cisco Home Agent
- モバイル、Public Wireless LAN (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ト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。

- Catalyst 6500 ファミリー スイッチおよび Cisco 7600 シリーズ ルータの mSEF 内の単一シャーシの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、簡易 IOS SLB ネットワークの論理図を示します。



## 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.184)を参照してください。

プラットフォームサポートと Cisco IOS および Catalyst OS 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

- 「IOS SLB に関する制約事項」 (P.3)
- 「IOS SLB に関する情報」 (P.9)
- 「IOS SLB の設定方法」 (P.37)
- 「IOS SLB の設定例」 (P.112)
- 「その他の参考資料」 (P.179)
- 「IOS SLB の機能情報」 (P.184)

## 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 packets 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** サーバで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にある IOS SLB の仮想 IP アドレスは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** モードで実行する場合、実サーバはレイヤ 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 スイッチとは別に複数のレイヤ 3 ホップをサーバに配置できるため、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。

- クライアント NAT およびサーバポート変換は、TCP および UDP の仮想サーバでのみサポートされます。
- IOS インターフェイス IP アドレスの 1 つと同じ仮想 IP アドレスに対するバランシング ストリームの場合（ループバック、イーサネットなど）、IOS SLB は、そのアドレスに対するすべての 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」の ICMP パケットで応答します。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。
- Catalyst 6500 ファミリ スイッチで IOS SLB および Web Cache Communication Protocol (WCCP) の両方を設定し、IOS SLB を使用して WCCP Input Redirection を設定している場合、ルータとキャッシュ間にレイヤ 2 WCCP の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。
- フローが 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）を介して送信される「サンドイッチ」設定の場合、その IOS SLB インスタンスは、異なる 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) に存在する必要があります。
- 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。

### スタティック NAT

- 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、実サーバがサーバ NAT に特定の仮想 IP アドレスを使用しており、サーバファームをその同じ仮想 IP アドレスに関連付けている場合、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はできません。
- 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。

### バックアップサーバファームのサポート

- 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

- 各ロードバランシングデバイスで、単一のファイアウォールファームに制限されなくなりました。
- 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できます。または、すべてのデバイスで VLAN を共有し、単一のインターフェイスを使用して接続できます。
- 各ファイアウォールロードバランシングデバイスと各ファイアウォール間には、イーサネットが必要です。
- 各ファイアウォールロードバランシングデバイスでは、各レイヤ 2 ファイアウォールを単一のレイヤ 3 (IP) インターフェイスに接続する必要があります。
- 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。
  - Network Address Translation (NAT; ネットワーク アドレス変換)
  - 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

#### GTP Cause Code Inspection をイネーブルにしない GPRS ロードバランシング

- 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。
- ステイック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されません。
- 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
  - 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 をイネーブルにした GPRS ロードバランシング

- 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

### GPRS トンネリング プロトコル v2 (GTP v2)

- 次の機能はサポートされません。
  - クライアント NAT

### VPN サーバロードバランシング

- 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

- 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 関連付けを使用する場合、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。
- 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

- 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。Cisco VSA は、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

- 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

- 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）。
- 各 User-Name アトリビュートは単一の加入者、または最大限でも非常に少数の加入者に対応付ける必要があります。そうしないと、予定外に大きな負荷が単一の 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。各加入者の User-Name アトリビュート値は、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-Requests 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。
  - その加入者セッションについて、PDSN および HA は、User-Name アトリビュートを指定した RADIUS Access-Request パケットおよび 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。
  - その加入者セッションについて、PDSN および HA は、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の発信元 IP アドレスと同じ Framed-ip-address アトリビュートを指定した 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

- ロードバランシングのために、Registration Request (RRQ) には Network Access Identifier (NAI) を含める必要があります。

- ロードバランシングのために、RRQ には 0.0.0.0 または 255.255.255.255 というホームエージェントの 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 が 96 バイトを超える場合、IOS SLB はプロセスレベルでパケットを処理します。
- 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
  - ステイッキ接続
  - 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

- 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

- 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 環境の場合、クライアントは 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。
- Catalyst 6500 ファミリースイッチおよび Cisco 7600 シリーズルータの場合：
  - Native IOS だけがサポートされます (c6sup イメージ)。Native IOS には、MSFC および 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 ファミリースイッチで冗長 MSFC を実行する場合、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、特に区別している場合を除き、MSFC1、MSFC2、または MSFC3 を指します。  
「PFC」という用語は、特に区別している場合を除き、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 フローの設定方法の詳細については、『*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は PFC ではなく MSFC によって処理されます)。
- Supervisor Engine 2 の場合、ファイアウォール ロードバランシングを必要とする「サンドイッチ」設定はサポートされません。このような設定には VRF が必要であり、VRF は Supervisor Engine 2 でサポートされないためです。

#### Access Service Network (ASN) R6 ロードバランシング

- dispatched または directed サーバ NAT モードでだけ動作します。directed モードの場合、IOS SLB は、Mobile Station (MS) Pre-Attachment 要求の宛先 IP アドレスを、選択した 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 (MS Pre-Attachment 要求用)
- IOS SLB をバイパスして、MS Pre-Attachment ACK パケットを ASN ゲートウェイに直接送信するようにベースステーションを設定する場合、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。

## 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.10)
- 「[一般的な IOS SLB 機能](#)」(P.10) : 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.29) : 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 機能は単一プラットフォームに固有であり、機能に関するドキュメント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ドキュメント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、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。IOS SLB は、SLB テクノロジーを従来のシスコ製スイッチおよびルータに完全に統合したいお客様に推奨します。

Cisco Catalyst 6500 ファミリースイッチで 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 によって、実績のある技術でコンテンツとアプリケーションの継続的な高可用性が確保されるため、分散環境のサーバおよび接続を積極的に管理できます。IOS SLB はユーザ要求をサーバクラスタに分散することで、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、アプリケーションサービスの提供コストを大幅に削減します。

IOS SLB はスケーラビリティ、可用性、およびメンテナンスの容易さを向上します。

- 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。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によって、新しいサーバの負荷を徐々に上げることができます。それによって、サーバに対する新規接続の割り当てが多すぎたり、早すぎたりすることで発生する障害を回避できます。
- 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。

サーバアプリケーションの管理が容易になります。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。

実サーバのアドレスは外部ネットワークに公表されないため、実サーバのセキュリティは確保されます。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。

## 一般的な IOS SLB 機能

IOS SLB には次の機能があります。

- 「ルーティング機能」(P.11)
- 「セキュリティ機能」(P.21)
- 「サーバ障害の検出機能および回復機能」(P.22)
- 「プロトコルサポート機能」(P.27)
- 「冗長機能」(P.28)

## 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」 (P.11)
- 「バインディング ID のサポート」 (P.13)
- 「Client-Assigned ロードバランシング」 (P.13)
- 「接続のレート制限」 (P.13)
- 「コンテンツフローモニタのサポート」 (P.13)
- 「TCP 接続コンテキストの遅延削除」 (P.14)
- 「ファイアウォールロードバランシング」 (P.14)
- 「GTP IMSI スティッキデータベース」 (P.15)
- 「Home Agent Director」 (P.15)
- 「インターフェイス認識」 (P.16)
- 「最大接続」 (P.16)
- 「複数ファイアウォールファームのサポート」 (P.16)
- 「Network Address Translation (NAT; ネットワークアドレス変換)」 (P.16)
- 「ポートバインドサーバ」 (P.19)
- 「ルートヘルスインジェクション」 (P.20)
- 「スティッキ接続」 (P.20)
- 「TCP セッションの再割り当て」 (P.21)
- 「透過的 Web キャッシュロードバランシング」 (P.21)

## 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。

- 「加重ラウンドロビン」 (P.11)
- 「加重最小接続」 (P.12)
- 「ルートマップ」 (P.13)

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。

各アルゴリズムについて、終了状態の接続は、実サーバに割り当てられた接続数に継続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に影響が及びます。最小接続アルゴリズムは接続数の影響を受け、接続数が増えるほど影響が大きくなるためです。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

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。各実サーバには加重  $n$  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ている他の実サーバと比較して、接続を処理できる容量を示します。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)

サーバファームのすべてのサーバに  $n=1$  という加重を割り当てると、IOS SLB デバイスは簡易なラウンドロビンアルゴリズムを使用するように設定されます。

GPRS Tunneling Protocol (GTP; GPRS トンネリングプロトコル) Cause Code Inspection をイネーブルにしない General Packet Radio Service (GPRS) ロードバランシングの場合、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は、GTP Cause Code Inspection をイネーブルにせずに 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できますが、仮想サーバを INSERVICE に変更できません。変更しようとする、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は、Home Agent Director 仮想サーバにバインドできますが、仮想サーバを INSERVICE に変更できません。変更しようとする、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では、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

加重最小接続アルゴリズムでは、仮想サーバへの新しい接続について、サーバファームから選択される次の実サーバが、アクティブな接続数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、 $n_1/(n_1+n_2+n_3\dots)$  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)

サーバファームのすべてのサーバに  $n=1$  という加重を割り当てると、IOS SLB デバイスは簡易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 をイネーブルにしない GPRS ロードバランシングの場合、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 をイネーブルにした GPRS ロードバランシングの場合、加重最小接続アルゴリズムをサポートします。

Access Service Network (ASN) R6 ロードバランシング (MS 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では、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

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、加入者のデータプレーントラフィックを処理する高パフォーマンスの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、ペイロードが検査され、framed-IP アトリビュートが抽出され、ルートマップがその IP アドレスに適用され、加入者を処理する CSG が決定されます。

機能、使用するタイミング、設定方法、イネーブルにする方法など、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」および「Configuring Policy-Based Routing」の項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 を使用すると、単一の物理サーバを複数の仮想サーバにバインドし、それぞれについて異なる加重をレポートできます。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。

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 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 パケットは順序どおりに到達しないため、IOS SLB の視点では、TCP 接続の終了 (finish [FIN] または reset [RST]) 後に、接続の他のパケットが到達することがあります。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達するパケットを適切にリダイレクトするために、IOS SLB は、特定の期間、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

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。

各ロード バランシング デバイ스에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 ファイアウォールには IP アドレス指定可能なインターフェイスがあります。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、固有の MAC アドレスを持っている場合、レイヤ 3 ファイアウォールは IOS SLB のファイアウォール 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 ファイアウォールには IP アドレスがなく、IOS SLB ファイアウォール ロード バランシングからは認識されません。IOS SLB がレイヤ 2 ファイアウォールをサポートするには、IP アドレス指定可能なインターフェイス間にファイアウォールを配置します。

ロード バランシング デバイス (たとえば、単一の LAN) 上の単一のレイヤ 3 インターフェイスから離れて多数のレイヤ 3 ファイアウォールを配置できますが、各インターフェイスから離れて配置できるレイヤ 2 ファイアウォールは 1 つだけです。

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 バランシングでは、ハッシュ アルゴリズムをルート検索に適用し、最適なファイアウォールを選択して接続要求を処理します。



(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。Catalyst 6500 ファミリー スイッチでは、さらにいくつかからのパケットを確認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 パフォーマンスに影響があるため、全体的な設計として考慮する必要があります。

複数のファイアウォールを備えるネットワークで可用性と復元力を最大限にするために、ファイアウォールの 1 つだけに単一のルートを設定するのではなく、個別の均等な加重のルートを各ファイアウォールに設定します。

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、「スティッキー」にすることができます。
- source-IP、destination-IP、および source-destination-IP のスティッキー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 スティッキー データベース

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。

この機能をイネーブルにするために、IOS SLB では GPRS Tunneling Protocol (GTP) IMSI スティッキー データベースを使用します。このデータベースによって、各 IMSI は、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されます。

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ー データベース オブジェクトが作成されます。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、スティッキー オブジェクトが削除されます。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 にスティッキー オブジェクトを削除するように通知されます。

### 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.29) 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](#)」(P.11) 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

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、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対してパケットをマッピングする場合、IOS SLB では入力インターフェイスを考慮に入れる必要があります。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)。

## 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。

## Network Address Translation (NAT; ネットワークアドレス変換)

Cisco IOS NAT (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.16)
- 「dispatched モード」(P.17)
- 「directed モード」(P.17)
- 「サーバ NAT」(P.17)
- 「クライアント NAT」(P.18)
- 「スタティック NAT」(P.18)
- 「サーバポート変換」(P.19)

### 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には、パケットを実サーバにリダイレクトする処理があります。

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 モードのいずれでも、IOS SLB では常に接続が追跡されます。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 モードの場合、仮想サーバのアドレスは実サーバに認識されます。各実サーバで、仮想サーバの IP アドレスは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 モードの場合、仮想サーバの IP アドレスは変更されないため、実サーバは IOS SLB に対してレイヤ 2 隣接にする必要があります。そうしないと、仲介ルータは選択した実サーバにルーティングできない可能性があります。

Catalyst 6500 ファミリースイッチの場合、ハードウェア データパケット アクセラレーションを使用した dispatched モードは 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 응답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 モードでは、任意の実サーバから認識される 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.17)
- 「クライアント NAT」(P.18)
- 「スタティック NAT」(P.18)
- 「サーバポート変換」(P.19)



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

directed モードの場合、IOS SLB は FTP またはファイアウォールの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のロードバランシングは NAT を使用できません。

TCP および UDP の仮想サーバの場合、TCP IOS SLB はクライアント NAT だけをサポートします。

Encapsulation Security Payload (ESP) 仮想サーバまたは Generic Routing Encapsulation (GRE) 仮想サーバの場合、IOS SLB はサーバ NAT だけをサポートします (ただし、サーバポートの変換は行われません)。

### 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的ポートを使用できるため、一時的クライアント 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 を使用すると、一部のユーザは NAT を利用し、同じイーサネット インターフェイスの他のユーザは、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 にスタティック NAT は必要ありませんが、実サーバの 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] : アドレスの変換時に、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 プロローブを使用します。
- [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ー 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ー 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ー オブジェクトを検出すると、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、IOS SLB はそのパケットを通常どおりに処理します。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** ステイタック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 は一致するステイタック 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 は一致するステイタック 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

仮想サーバを定義する場合、その仮想サーバで処理する TCP または UDP の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。

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

(**inserve** 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 アドレスは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。

## スティッキ接続

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。

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。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 **MAXCONNNS\_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。

**sticky** コマンドでサブネットマスクを指定すると、クライアントサブネットのスティッキが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。

スティッキ接続では、複数の仮想サーバまたはファイアウォール ファームによって処理されるサービスのカップリングも設定できます。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

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。

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。

キャッシュに必要なページが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に対して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」 (P.21)
- 「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.22)
- 「スロー スタート」 (P.22)
- 「SynGuard」 (P.22)

## 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、高度にセキュリティなサイトであれば、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

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。

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、仮想サーバが処理する TCP start-of-connection パケットのレート (SYNchronize Sequence Number (SYN)) を制限することで、SYN フラッドサービス拒絶攻撃と呼ばれる種類のネットワークの問題を回避します。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、仮想サーバが処理する SYN 数を特定の間隔で監視し、設定した SYN しきい値を超える数の SYN を許可しません。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.23)
- 「自動アンフェイル」 (P.23)
- 「バックアップサーバファーム」 (P.23)
- 「DFP Agent Subsystem のサポート」 (P.24)

- 「IOS SLB 用 Dynamic Feedback Protocol」 (P.24)
- 「GGSN-IOS SLB メッセージング」 (P.25)
- 「仮想サーバの INOP\_REAL 状態」 (P.25)
- 「プローブ」 (P.25)

## 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する場合、1 つまたは複数のプローブを設定することを強く推奨します。

**no faildetect inband** コマンドを指定する場合、**faildetect numconns** コマンドを指定しても無視されます。

## 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、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。

## 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。

## 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 リリース 12.2(18)SXD の *DFP Agent Subsystem* 機能に関するドキュメントを参照してください。

## IOS SLB 用 Dynamic Feedback Protocol

ロードバランシング環境の DFP マネージャが IOS SLB Dynamic Feedback Protocol (DFP) をサポートしている場合、DFP エージェントを使用して TCP 接続を開始できます。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、DFP 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レポートに加え、実サーバのステータスに急な変化があった場合に DFP エージェントから初期のレポートが送信されます。

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静的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 は静的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、以下の項を参照してください。

- 「[DFP および GPRS ロードバランシング](#)」 (P.24)
- 「[DFP および Home Agent Director](#)」 (P.25)

### 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 エージェントでは、CPU 使用率、プロセッサメモリ、および各 GGSN でアクティブ化できる 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 の加重が算出されます。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。

$$(\text{既存の PDP コンテキスト数}) / (\text{最大 PDP コンテキスト数})$$

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。

$$(\text{既存の PDP コンテキスト}) / 10000 = \text{低い GGSN 加重}$$

**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する場合、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 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 エージェントでは、CPU 使用率、プロセッサメモリ、および各ホームエージェントで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が算出されます。

$(\text{バインディングの最大数} - \text{現在のバインディング数}) / \text{バインディングの最大数} \times (\text{CPU 使用率} + \text{メモリ使用率}) / 32 \times \text{最大 DFP 加重} = \text{レポートされる加重}$

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。

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

IOS SLB 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。

また、HTTP プローブを使用して、サーバロードバランシング処理されたアプリケーションを監視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](#)』の **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。

あるプローブに対して実サーバが失敗すると、すべてのプローブに失敗したことになります。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)

ステートフルバックアップのためにプローブを設定し、フェールオーバーが発生した場合、ステータスの変更(バックアップからアクティブへ)は、新しいアクティブ IOS SLB デバイスに正確に反映されます。ただし、(フェールオーバー前はアクティブデバイスだった)新しいバックアップ IOS SLB デバイスのプローブのステータスは、アクティブと表示されます。

### 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。

パスワードの問題を解消するために、ステータスコード 401 を受け入れるように HTTP プローブを設定します。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*』の **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.27)
- 「AAA ロードバランシング」 (P.28)
- 「オーディオおよびビデオのロードバランシング」 (P.28)
- 「VPN サーバロードバランシング」 (P.28)

## 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) R6
- ドメインネームシステム (DNS)
- Encapsulation Security Payload (ESP; カプセル化セキュリティペイロード)
- ファイル転送プロトコル (FTP)
- Generic Routing Encapsulation (GRE)
- GPRS トンネリングプロトコル v0 (GTP v0)
- GPRS トンネリングプロトコル v1 (GTP v1)
- GPRS トンネリングプロトコル v2 (GTP v2)
- ハイパーテキスト転送プロトコル (HTTP)
- 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)
- RealAudio/RealVideo via RTSP
- Remote Authentication Dial-In User Service (RADIUS)

- Simple Mail Transport Protocol (SMTP)
- Telnet
- トランスミッション制御プロトコル (TCP) および標準の TCP プロトコル
- ユーザ データグラム プロトコル (UDP) 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 の認証、認可、アカウントिंग (AAA) 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トング 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.34) 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するサーバについて、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) を介する RealAudio および RealVideo ストリームの負荷を分散できます。

### 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

IOS SLB デバイスはシングル ポイント障害を示すことがあり、次のいずれかの状況になると、サーバは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스에 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.29)
  - 「ステートフル バックアップ」 (P.29)
  - 「アクティブ スタンバイ」 (P.29)

### 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、シングル レイヤ 3 スイッチの可用性に依存することなく、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で、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う場合は特に、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。フェールオーバーを迅速に検出する方法を設定するには、HSRP を使用します。

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)

ステートフル バックアップのためにプローブを設定し、フェールオーバーが発生した場合、ステータスの変更 (バックアップからアクティブへ) は、新しいアクティブ IOS SLB デバイスに正確に反映されます。ただし、(フェールオーバー前はアクティブ デバイスだった) 新しいバックアップ IOS SLB デバイスのプローブのステータスは、アクティブと表示されます。

### 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、Catalyst 6500 ファミリー スイッチおよび Catalyst 7600 シリーズ スイッチ用の mobile Service Exchange Framework (mSEF) の場合、Exchange Director をサポートします。Exchange Director には次の機能があります。

- 「ASN R6 ロードバランシング」 (P.30)
- 「GPRS ロードバランシング」 (P.30)
- 「GTP Cause Code Inspection なしの GPRS ロードバランシング」 (P.31)
- 「GTP Cause Code Inspection ありの GPRS ロードバランシング」 (P.31)
- 「Home Agent Director」 (P.32)
- 「KeepAlive Application Protocol (KAL-AP) エージェントのサポート」 (P.32)
- 「RADIUS ロードバランシング」 (P.34)
- 「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.35)
- 「WAP ロードバランシング」 (P.36)
- 「冗長ルートプロセッサのステートフルバックアップ」 (P.37)
- 「フローの永続性」 (P.37)

## ASN R6 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単一の ASN ゲートウェイのように見えます。

Mobile Subscriber Station (MSS) はネットワークに参加するとき、ベースステーションから Mobile Station (MS; モバイルステーション) 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 MS Pre-Attachment 応答でベースステーションに直接応答します。設定に従い、ベースステーションから IOS SLB に MS Pre-Attachment ACK を返します。その ACK は選択し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。

## GPRS ロードバランシング

General Packet Radio Service (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、GPRS Tunneling Protocol (GTP; GPRS トンネリングプロトコル) を使用して Serving GPRS Support Node (SGSN) と接続します。結果として、トランスポートに UDP を使用します。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)、バージョン 1 (GTP v1)、およびバージョン 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 対応」になるため、IOS SLB の認識をレイヤ 5 まで拡張できます。

- 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.31)
- 「[GTP Cause Code Inspection ありの GPRS ロードバランシング](#)」 (P.31)

### 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。
- ステイ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.29) 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](#)」 (P.11) 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監視できます。それによって、GTP 障害の原因コードを監視し、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 作成応答の原因コードと対応する IOS SLB のアクション

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

表 1 PDP 作成応答の原因コードと対応する IOS SLB のアクション (続き)

原因コード	IOS SLB のアクション
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 \(P.29\)](#)」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 \(P.12\)](#)」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。

## 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 \(P.29\)](#)」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 \(P.11\)](#)」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。



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。

$$\text{KAL-AP 負荷} = 256 - (\text{アクティブな実サーバの数} \times 256 / \text{サービスに参加している実サーバの数})$$

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。

$$\text{KAL-AP 負荷} = 256 - (1 \times 256 / 2) = 256 - 128 = 128$$

### 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。

$$\text{KAL-AP 負荷} = 256 - (\text{実サーバの最大 DFP 加重の合計} \times 256 / \text{ファームの加重})$$



(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 加重で GGSN を設定し、GGSN の負荷は 50% の場合、50 の最大 DFP 加重が KAL-AP にレポートされます。

実サーバに対する DFP 接続がダウン状態の場合、KAL-AP では、SLB 実サーバ コンフィギュレーション モードで **weight** コマンドの設定が使用されます。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 には 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 加重がレポートされます)。
- GGSN-2 には 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 加重がレポートされます)。

このサイトの KAL-AP 負荷値は次のようになります。

$$\text{KAL-AP 負荷} = 256 - [(100 + 50) \times 256 / 200] = 256 - 192 = 64$$

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トリング 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、およびアカウントリングに関して、RADIUS メッセージの負荷を AAA サーバに分散できます。データプレーンの RADIUS ロード バランシングでは、特定の加入者のデータ フローに、宛先ネットワーク デバイスに対する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 アカウントリング メッセージを承認し、ステイック 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](#)」(P.11) を参照してください。
- RADIUS プロトコルを介して SSG シングル サインオンが容易になります。
- 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 アカウンティングのローカル ACK によって、IOS SLB は RADIUS アカウンティング パケットに ACK で応答し、さらに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 アカウンティングのローカル ACK は、RADIUS ロードバランシング マップと Turbo RADIUS ロードバランシングと同時に使用できません。
- 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ます) は、CSG 環境でポリシーベース ルーティング (PBR) ルート マップを使用し、加入者のデータプレーン トラフィックを処理する高パフォーマンスの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、ペイロードが検査され、framed-IP アトリビュートが抽出され、ルート マップがその IP アドレスに適用され、加入者を処理する CSG が決定されます。

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。

機能、使用するタイミング、設定方法、イネーブルにする方法など、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」および「Configuring Policy-Based Routing」の項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は、RADIUS ロードバランシング マップおよび 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。

Turbo RADIUS ロードバランシングは、Virtual Private Network (VPN) Routing and Forwarding (VRF) と同時に使用できません。

Turbo RADIUS ロードバランシングは、簡易な 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。

Turbo RADIUS ロードバランシングは、オプションの ACL ログイング ファシリティと同時に使用できません。Turbo RADIUS ロードバランシングを使用するには、まずログイング 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。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 モードの場合、WSP は簡易な 1 要求/1 応答プロトコルであり、単一のサーババインド パケットによって、1 つまたは複数のパケットのサーバ応答が返されます。
- Connection-oriented WSP モード (IP/UDP [9201]/WTP/WSP)。Connection-oriented WSP モードの場合、WDP イベントの再送信は WTP によって処理され、WSP は定義済みのセッション起動/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 でのみ動作します。この WSP セッションは暗号化されていないため、WTP によって再送信が処理されます。
- 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

Catalyst 6500 ファミリー スイッチおよび 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高可用性を維持できます。

## 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 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.112) 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ドキュメントについては、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。

- 「[必須および任意の IOS SLB 機能の設定](#)」(P.38) (必須)
- 「[ファイアウォールロードバランシングの設定](#)」(P.50) (任意)
- 「[プローブの設定](#)」(P.56) (任意)
- 「[DFP の設定](#)」(P.65) (任意)
- 「[GPRS ロードバランシングの設定作業リスト](#)」(P.66) (任意)
- 「[GGSN-IOS SLB のメッセージング作業リスト](#)」(P.68) (任意)
- 「[GPRS ロードバランシングマップの設定](#)」(P.69) (任意)
- 「[KeepAlive Application Protocol \(KAL-AP\) エージェントのサポートの設定](#)」(P.72) (任意)
- 「[RADIUS ロードバランシングの設定作業リスト](#)」(P.73) (任意)
- 「[mSEF 用 Exchange Director の設定作業リスト](#)」(P.83) (任意)
- 「[VPN サーバロードバランシングの設定作業リスト](#)」(P.93) (任意)
- 「[ASN R6 ロードバランシングの設定作業リスト](#)」(P.95) (任意)
- 「[Home Agent Director の設定作業リスト](#)」(P.95) (任意)
- 「[NAT の設定](#)」(P.97) (任意)
- 「[スタティック NAT の設定](#)」(P.97) (任意)
- 「[ステートレスバックアップの設定作業リスト](#)」(P.98) (任意)
- 「[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.100) (任意)
- 「[データベースエントリの設定](#)」(P.101) (任意)
- 「[フラグメントデータベースのバッファの設定](#)」(P.102) (任意)

- 「データベースおよびカウンタのクリア」(P.102) (任意)
- 「ワイルドカード検索の設定」(P.103) (任意)
- 「接続の消去および再割り当て」(P.105) (任意)
- 「自動サーバ障害検出のディセーブル化」(P.106) (任意)
- 「IOS SLB のモニタおよびメンテナンス」(P.107) (任意)

## 必須および任意の IOS SLB 機能の設定

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。

- 「サーバファームおよび実サーバの設定」(P.38) (必須)
- 「仮想サーバの設定」(P.42) (必須)
- 「サーバファームの確認」(P.48) (任意)
- 「仮想サーバの確認」(P.48) (任意)
- 「クライアントの確認」(P.49) (任意)
- 「IOS SLB 接続の確認」(P.49) (任意)

## サーバファームおよび実サーバの設定

サーバファームおよび実サーバを設定するには、この作業を実行します。



(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. **bindid [*bind-id*]**
5. **nat {*client pool* | *server*}**
6. **predictor [*roundrobin* | *leastconns* | *route-map mapname*]**
7. **probe *probe***
8. **real *ip-address* [*port*]**
9. **faildetect *numconns number-of-conns* [*numclients number-of-clients*]**
10. **maxclients *number-of-conns***
11. **maxconns *number-of-conns* [*sticky-override*]**
12. **reassign *threshold***
13. **retry *retry-value***
14. **weight *setting***
15. **inservice**

## 手順の詳細

	コマンド	説明
ステップ1	<code>enable</code>  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	<code>configure terminal</code>  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	<code>ip slb serverfarm server-farm</code>  例: Router(config)# ip slb serverfarm PUBLIC	サーバファームの定義を IOS SLB ロードバランシング (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	<code>bindid [bind-id]</code>  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。  <b>(注)</b> 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5	<code>nat {client pool   server}</code>  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。

コマンド	説明
<p><b>ステップ 6</b> <code>predictor [roundrobin   leastconns   route-map mapname]</code></p> <p>例： Router(config-slb-sfarm)# predictor leastconns</p>	<p>(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。</p> <p><b>(注)</b> RADIUS ロードバランシングの場合、デフォルト設定 (加重ラウンドロビンアルゴリズム) が必須です。</p> <p>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、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。</p> <p>Home Agent Director の場合、デフォルト設定 (加重ラウンドロビンアルゴリズム) が必須です。</p> <p>SLB サーバファーム コンフィギュレーション モードで <code>predictor route-map</code> 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 モードでその他のコマンドを使用できません。</p> <p>詳細については、次の項を参照してください。</p> <ul style="list-style-type: none"> <li>• 「加重ラウンドロビン」 (P.11)</li> <li>• 「加重最小接続」 (P.12)</li> <li>• 「ルートマップ」 (P.13)</li> </ul>
<p><b>ステップ 7</b> <code>probe probe</code></p> <p>例： Router(config-slb-sfarm)# probe PROBE1</p>	<p>(任意) プローブを実サーバに関連付けます。</p>
<p><b>ステップ 8</b> <code>real ip-address [port]</code></p> <p>例： Router(config-slb-sfarm)# real 10.1.1.1</p>	<p>サーバファームのメンバとして、実サーバを IP アドレスとオプションのポート番号で指定し、実サーバ コンフィギュレーション モードを開始します。</p> <p><b>(注)</b> GPRS ロードバランシングの場合、GGSN 機能を実行する実サーバの IP アドレス (Cisco GGSN の場合、仮想プレートアドレス) を指定します。</p> <p>VPN サーバロードバランシングの場合、VPN ターミネータとして動作する実サーバの IP アドレスを指定します。</p> <p>Home Agent Director の場合、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。</p>



コマンド	説明
<b>ステップ 9</b> <code>faildetect numconns number-of-conns</code> <code>[numclients number-of-clients]</code>  <b>例:</b> 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。  <b>GPRS</b> ロードバランシングの場合、環境に 1 つの SGSN しかない場合、値 1 の <b>numclients</b> キーワードを指定します。  <b>RADIUS</b> 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 <b>numclients</b> キーワードを指定します。
<b>ステップ 10</b> <code>maxclients number-of-conns</code>  <b>例:</b> 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 Server Load Balancing (IOS SLB) および GTP ステイキ加入者の最大数を指定します。
<b>ステップ 11</b> <code>maxconns number-of-conns [sticky-override]</code>  <b>例:</b> 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。
<b>ステップ 12</b> <code>reassign threshold</code>  <b>例:</b> 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。  <b>(注)</b> 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 <b>reassign threshold</b> を指定する必要があります。
<b>ステップ 13</b> <code>retry retry-value</code>  <b>例:</b> Router(config-slb-real)# retry 120	(任意) サーバの障害を検出してから、その障害が発生したサーバへの接続を再試行するまでの間隔 (秒) を指定します。
<b>ステップ 14</b> <code>weight setting</code>  <b>例:</b> Router(config-slb-real)# weight 24	(任意) 実サーバの作業負荷容量を指定します。サーバファーム内の他のサーバと相対的な値です。  <b>(注)</b> 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 <b>weight</b> コマンドを使用して定義した静的加重よりも、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 は静的な加重に戻されます。
<b>ステップ 15</b> <code>inservice</code>  <b>例:</b> Router(config-slb-real)# inservice	IOS Server Load Balancing (IOS SLB) が使用する実サーバをイネーブルにします。



(注)

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を Catalyst 6500 ファミリースイッチで実行する場合、PFC 上の TCAM の容量を超える可能性を軽減するには、**mls ip slb wildcard search rp** コマンドを使用します。詳細については、「[ワイルドカード検索の設定](#)」(P.103) を参照してください。

## 仮想サーバの設定

仮想サーバを設定するには、次の作業を実行します。

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 *ip-address* [*netmask* [**group**]] {**esp** | **gre** | *protocol*}**  
 または  
**virtual *ip-address* [*netmask* [**group**]] {**tcp** | **udp**} [*port* | **any**] [**service** *service*]**
5. **serverfarm *primary-farm* [**backup** *backup-farm* [**sticky**]] [**map** *map-id* **priority** *priority*]**
6. **access *interface* [**route** **framed-ip**]**
7. **advertise [**active**]**
8. **client {*ip-address netmask* [**exclude**] | **gtp carrier-code** [*code*]}**
9. **delay {*duration* | **radius framed-ip** *duration*}**
10. **gtp notification cac [*reassign-count*]**
11. **hand-off radius *duration***
12. **idle [**asn r6 request** | **gtp request** | **ipmobile request** | **radius** {**request** | **framed-ip**}] *duration***
13. **purge radius framed-ip acct on-off**
14. **purge radius framed-ip acct stop {*attribute-number* | {**26** | *vsa*} {*vendor-ID* | **3gpp** | **3gpp2**} *sub-attribute-number*}**
15. **radius acct local-ack key [**encrypt**] *secret-string***
16. **radius inject auth *group-number* {**calling-station-id** | **username**}**
17. **radius inject auth timer *seconds***
18. **radius inject auth vsa *vendor-id***
19. **replicate casa *listen-ip remote-ip port* [*interval*] [**password** [**encrypt**] *secret-string* *timeout*]**
20. **replicate interval *interval***
21. **replicate slave**
22. **sticky {*duration* [**group** *group-id*] [**netmask** *netmask*] | **gtp imsi** [**group** *group-id*] | **radius calling-station-id** | **radius framed-ip** [**group** *group-id*] | **radius username** [**msid-cisco**] [**group** *group-id*]}**
23. **synguard *syn-count interval***

## 24. inservice [standby group-name] [active]

## 手順の詳細

	コマンド	説明
ステップ1	<b>enable</b>  例： Router> enable	特権 EXEC モードをイネーブルにします。 <ul style="list-style-type: none"><li>プロンプトが表示されたら、パスワードを入力します。</li></ul>
ステップ2	<b>configure terminal</b>  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	<b>ip slb vserver virtual-server</b>  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。

コマンド	説明
<p><b>ステップ 4</b> <code>virtual ip-address [netmask [group]]</code>  <code>{esp   gre   protocol}</code></p> <p>または</p> <p><code>virtual ip-address [netmask [group]] {tcp   udp}</code>  <code>[port   any] [service service]</code></p> <p>例：  Router(config-slb-vserver)# virtual 10.0.0.1 tcp www</p>	<p>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。</p> <p>(注) RADIUS ロードバランシングの場合、<b>service radius</b> キーワード オプションを指定します。</p> <p>(注) ASN R6 ロードバランシングの場合、<b>service asn r6</b> キーワード オプションを指定します。</p> <p>(注) GPRS ロードバランシングの場合：</p> <ul style="list-style-type: none"> <li>- 仮想 GGSN IP アドレスを仮想サーバとして指定し、<b>udp</b> キーワード オプションを指定します。</li> <li>- 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、すべてのポート宛で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 <b>any</b> を指定します。</li> <li>- 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 <b>any</b> を指定します。</li> <li>- 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、<b>service gtp</b> キーワード オプションを指定します。</li> <li>- 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、<b>service gtp-inspect</b> キーワード オプションを指定します。</li> </ul>

コマンド	説明
<p><b>ステップ5</b> <code>serverfarm primary-farm [backup backup-farm [sticky]] [map map-id priority priority]</code></p> <p>例： Router(config-slb-vserver)# serverfarm SF1 backup SF2 map 1 priority 1</p>	<p>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。</p> <p>(注) RADIUS ロードバランシングおよび Home Agent Director は、<b>sticky</b> キーワードをサポートしません。</p> <p>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、各サーバファームを異なる仮想サーバに関連付ける必要があります。</p> <p>特定の RADIUS 仮想サーバに複数のサーバファームを関連付けるには、複数の <b>serverfarm</b> コマンドを設定し、それぞれに固有のマップ ID と固有のプライオリティを指定します（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）。</p>
<p><b>ステップ6</b> <code>access interface [route framed-ip]</code></p> <p>例： Router(config-slb-vserver)# access Vlan20 route framed-ip</p>	<p>(任意) 入力インターフェイスを検査するには、<b>framed-IP</b> ルーティングをイネーブルにします。</p>
<p><b>ステップ7</b> <code>advertise [active]</code></p> <p>例： Router(config-slb-vserver)# advertise</p>	<p>(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。</p>
<p><b>ステップ8</b> <code>client {ip-address netmask [exclude]   gtp carrier-code [code]}</code></p> <p>例： Router(config-slb-vserver)# client 10.4.4.0 255.255.255.0</p>	<p>(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。</p> <p>(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 <b>gtp carrier-code</b> オプションだけをサポートします。</p>
<p><b>ステップ9</b> <code>delay {duration   radius framed-ip duration}</code></p> <p>例： Router(config-slb-vserver)# delay 30</p>	<p>(任意) 接続の終了後、IOS Server Load Balancing (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。</p>
<p><b>ステップ10</b> <code>gtp notification cac [reassign-count]</code></p> <p>例： Router(config-slb-vserver)# gtp notification cac 5</p>	<p>(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。</p>
<p><b>ステップ11</b> <code>hand-off radius duration</code></p> <p>例： Router(config-slb-vserver)# hand-off radius 30</p>	<p>(任意) 外部エージェントのハンドオフ時に、IOS Server Load Balancing (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。</p>

## IOS SLB の設定方法

コマンド	説明
<b>ステップ 12</b> <b>idle</b> [asn r6 request   gtp request   ipmobile request   radius {request   framed-ip}] duration  例： Router(config-slb-vserver)# idle 120	(任意) パケット アクティビティがない場合、IOS Server Load Balancing (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。  <b>(注)</b> 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。
<b>ステップ 13</b> <b>purge radius framed-ip acct on-off</b>  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 が IOS SLB RADIUS framed-ip スティック データベースのエントリを消去できるようにします。
<b>ステップ 14</b> <b>purge radius framed-ip acct stop</b> {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 が IOS SLB RADIUS framed-ip スティック データベースのエントリを消去できるようにします。
<b>ステップ 15</b> <b>radius acct local-ack key</b> [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。
<b>ステップ 16</b> <b>radius inject auth group-number</b> {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。
<b>ステップ 17</b> <b>radius inject auth timer seconds</b>  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) 関連付けのタイマーを設定します。
<b>ステップ 18</b> <b>radius inject auth vsa vendor-id</b>  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) 関連付けの VSA をバッファリングします。

コマンド	説明
<p><b>ステップ 19</b> <code>replicate casa listen-ip remote-ip port [interval] [password [encrypt] secret-string timeout]</code></p> <p>例： Router(config-slb-vserver)# replicate casa 10.10.10.11 10.10.11.12 4231</p>	<p>(任意) バックアップ スイッチに対する IOS Server Load Balancing (IOS SLB) の判定テーブルのステートフルバックアップを設定します。</p> <p><b>(注)</b> Home Agent Directorはこのコマンドをサポートしません。</p> <p><b>virtual</b> コマンドで <b>service gtp</b> キーワードを指定し、<b>sticky</b> コマンドで <b>gtp imsi</b> キーワードを指定しない場合、<b>replicate casa</b> コマンドはサポートされません (セッションは永続的ではなく、レプリケートする対象がないためです)。</p>
<p><b>ステップ 20</b> <code>replicate interval interval</code></p> <p>例： Router(config-slb-vserver)# replicate interval 20</p>	<p>(任意) IOS Server Load Balancing (IOS SLB) 仮想サーバのレプリケーション配信間隔を設定します。</p> <p><b>(注)</b> Home Agent Directorはこのコマンドをサポートしません。</p> <p><b>virtual</b> コマンドで <b>service gtp</b> キーワードを指定し、<b>sticky</b> コマンドで <b>gtp imsi</b> キーワードを指定しない場合、<b>replicate casa</b> コマンドはサポートされません (セッションは永続的ではなく、レプリケートする対象がないためです)。</p>
<p><b>ステップ 21</b> <code>replicate slave</code></p> <p>例： Router(config-slb-vserver)# replicate slave</p>	<p>(任意) IOS Server Load Balancing (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。</p> <p><b>(注)</b> Home Agent Directorはこのコマンドをサポートしません。</p> <p><b>virtual</b> コマンドで <b>service gtp</b> キーワードを指定し、<b>sticky</b> コマンドで <b>gtp imsi</b> キーワードを指定しない場合、<b>replicate casa</b> コマンドはサポートされません (セッションは永続的ではなく、レプリケートする対象がないためです)。</p> <p><b>replicate slave</b> を設定した単一の Supervisor を使用する場合、Supervisor で out-of-sync メッセージを受信することがあります。</p>
<p><b>ステップ 22</b> <code>sticky {duration [group group-id] [netmask netmask]   gtp imsi [group group-id]   radius calling-station-id   radius framed-ip [group group-id]   radius username [msid-cisco] [group group-id]}</code></p> <p>例： Router(config-slb-vserver)# sticky 60 group 10</p>	<p>(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。</p> <p><b>(注)</b> VPN サーバロードバランシングの場合、15 秒以上の <i>duration</i> を指定します。</p> <p>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。</p>

コマンド	説明
<b>ステップ 23</b> <code>synguard syn-count interval</code>  例: Router(config-slb-vserver)# synguard 50	(任意) SYN フラッド サービス拒絶攻撃を回避するために、仮想サーバが処理する TCP SYNchronize Sequence Number (SYN) を指定します。  <b>(注)</b> 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。
<b>ステップ 24</b> <code>inservice [standby group-name] [active]</code>  例: Router(config-slb-vserver)# inservice	IOS Server Load Balancing (IOS SLB) が使用する仮想サーバをイネーブルにします。

## 仮想サーバの確認

仮想サーバを確認するには、次の作業を実行します。

### 手順の概要

#### 1. show ip slb vservers

### 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

サーバファームを確認するには、次の作業を実行します。

### 手順の概要

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

### 手順の詳細

次の `show ip slb reals` コマンドで、サーバファーム PUBLIC および RESTRICTED 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
-----
10.1.1.1        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

クライアントを確認するには、次の作業を実行します。

### 手順の概要

#### 1. show ip slb 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** コマンドで、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_syms = 0, sticky = FALSE, flows attached = 0
Router#

```

## IOS SLB 接続の確認

IOS SLB 接続を確認するには、次の作業を実行します。

### 手順の概要

#### 1. show ip slb stats

### 手順の詳細

IOS SLB 機能がインストールされ、適切に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に ping を送信し、次にクライアントから仮想サーバに ping を送信します。

次の **show ip slb stats** コマンドで、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、通常の IOS スイッチング パスで IOS SLB パケットが処理されるときです (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)。特殊なスイッチングは、ハードウェア割り当てのスイッチング パスで IOS SLB パケットが処理されるときです。

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、「[IOS SLB のモニタおよびメンテナンス](#)」(P.107) 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

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 プロブが推奨されます。詳細については、「[ping プロブの設定](#)」(P.60) を参照してください。ファイアウォールで、ping プロブの転送を許可していない場合、代わりに HTTP プロブを使用します。詳細については、「[HTTP プロブの設定](#)」(P.59) 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およびファイアウォール ロード バランシングの両方を Catalyst 6500 ファミリー スイッチで実行する場合、PFC 上の TCAM の容量を超える可能性を軽減するには、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` コマンドを使用します。詳細については、「[ワイルドカード検索の設定](#)」(P.103) 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](#)」(P.104) 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](#)」(P.50) (必須)
- 「[ファイアウォール ファームの確認](#)」(P.54) (任意)
- 「[ファイアウォール接続の確認](#)」(P.55) (任意)

## ファイアウォール ファームの設定

ファイアウォール ファームを設定するには、次の作業を実行します。

### 手順の概要

#### 1. enable

2. **configure terminal**
3. **ip slb 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. **predictor hash address** [**port**]
10. **purge connection**
11. **purge sticky**
12. **replicate casa** *listen-ip remote-ip port [interval]* [**password** [[*encrypt*] *secret-string [timeout]*]]
13. **replicate interval** *interval*
14. **replicate slave**
15. **protocol tcp**
16. **delay** *duration*
17. **idle** *duration*
18. **maxconns** *maximum-number*
19. **sticky** *duration [netmask netmask]* [**source** | **destination**]
20. **protocol datagram**
21. **idle** *duration*
22. **maxconns** *maximum-number*
23. **sticky** *duration [netmask netmask]* [**source** | **destination**]
24. **inservice**

## 手順の詳細

	コマンド	目的
ステップ1	<b>enable</b>  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	<b>configure terminal</b>  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	<b>ip slb firewallfarm</b> <i>firewall-farm</i>  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 ロードバランシング (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	<b>real</b> <i>ip-address</i>  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。

## IOS SLB の設定方法

	コマンド	目的
ステップ 5	<code>probe probe</code>  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	<code>weight setting</code>  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	<code>inservice</code>  例： Router(config-slb-fw-real)# inservice	ファイアウォールおよび IOS Server Load Balancing (IOS SLB) が使用するファイアウォールをイネーブルにします。
ステップ 8	<code>access [source source-ip netmask] [destination destination-ip netmask]</code>  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 9	<code>predictor hash address [port]</code>  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	<code>purge connection</code>  例： Router(config-slb-fw)# purge connection	(任意) IOS Server Load Balancing (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。
ステップ 11	<code>purge sticky</code>  例： Router(config-slb-fw)# purge sticky	(任意) スティックタイマーが期限切れになるとき、IOS Server Load Balancing (IOS SLB) ファイアウォールロードバランシングから、スティック接続の消去要求を送信できるようにします。
ステップ 12	<code>replicate casa listen-ip remote-ip port [interval] [password [[encrypt] secret-string [timeout]]]</code>  例： Router(config-slb-fw)# replicate casa 10.10.10.11 10.10.11.12 4231	(任意) バックアップスイッチに対する IOS Server Load Balancing (IOS SLB) ファイアウォールロードバランシングの判定テーブルのステートフルバックアップを設定します。
ステップ 13	<code>replicate interval interval</code>  例： Router(config-slb-fw)# replicate interval 20	(任意) IOS Server Load Balancing (IOS SLB) 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します。  (注) Home Agent Director はこのコマンドをサポートしません。  <b>virtual</b> コマンドで <b>service gtp</b> キーワードを指定し、 <b>sticky</b> コマンドで <b>gtp imsi</b> キーワードを指定しない場合、 <b>replicate casa</b> コマンドはサポートされません (セッションは永続的ではなく、レプリケートする対象がないためです)。

コマンド	目的
<p><b>ステップ 14</b> <code>replicate slave</code></p> <p>例： Router(config-slb-fw)# replicate slave</p>	<p>(任意) IOS Server Load Balancing (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。</p> <p><b>(注)</b> Home Agent Director はこのコマンドをサポートしません。</p> <p><b>virtual</b> コマンドで <b>service gtp</b> キーワードを指定し、<b>sticky</b> コマンドで <b>gtp imsi</b> キーワードを指定しない場合、<b>replicate casa</b> コマンドはサポートされません (セッションは永続的ではなく、レプリケートする対象がないためです)。</p> <p><b>replicate slave</b> を設定した単一の Supervisor を使用する場合、Supervisor で out-of-sync メッセージを受信することがあります。</p>
<p><b>ステップ 15</b> <code>protocol tcp</code></p> <p>例： Router(config-slb-fw)# protocol tcp</p>	<p>(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。</p>
<p><b>ステップ 16</b> <code>delay duration</code></p> <p>例： Router(config-slb-fw-tcp)# delay 30</p>	<p>(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、接続の終了後、IOS Server Load Balancing (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。</p>
<p><b>ステップ 17</b> <code>idle duration</code></p> <p>例： Router(config-slb-fw-tcp)# idle 120</p>	<p>(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 アクティビティがない場合、IOS Server Load Balancing (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。</p>
<p><b>ステップ 18</b> <code>maxconns maximum-number</code></p> <p>例： Router(config-slb-fw-tcp)# maxconns 1000</p>	<p>(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。</p>
<p><b>ステップ 19</b> <code>sticky duration [netmask netmask] [source   destination]</code></p> <p>例： Router(config-slb-fw-tcp)# sticky 60</p>	<p>(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。</p> <ul style="list-style-type: none"> <li>• 同じペアの IP アドレス間に接続が存在する間 (発信元/宛先スティッキー)。</li> <li>• 最後の接続が破棄された後の <i>duration</i> で定義される期間。</li> </ul>

	コマンド	目的
ステップ 20	<code>protocol datagram</code>  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	<code>idle duration</code>  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 アクティビティがない場合、IOS Server Load Balancing (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	<code>maxconns maximum-number</code>  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	<code>sticky duration [netmask netmask] [source   destination]</code>  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。 <ul style="list-style-type: none"> <li>• 同じペアの IP アドレス間に接続が存在する間 (発信元/宛先スティッキー)。</li> <li>• 最後の接続が破棄された後の <i>duration</i> で定義される期間。</li> </ul>
ステップ 24	<code>inservice</code>  例： Router(config-slb-fw)# inservice	IOS Server Load Balancing (IOS SLB) が使用するファイアウォールファームをイネーブルにします。

## ファイアウォールファームの確認

ファイアウォールファームを確認するには、次の作業を実行します。

### 手順の概要

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

### 手順の詳細

次の `show ip slb reals` 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

```

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

ファイアウォールの接続を確認するには、次の作業を実行します。

### 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済みで、適切に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詳細情報を表示します。

```
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、通常の IOS スイッチング パスで IOS SLB パケットが処理されるときです（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）。特殊なスイッチングは、ハードウェア割り当てのスイッチング パスで IOS SLB パケットが処理されるときです。

- 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 real detail
```

```
10.1.1.3, FIRE1, state = OPERATIONAL, type = firewall
conns = 299310, dummy_conns = 0, maxconns = 4294967295
weight = 10, weight(admin) = 10, metric = 104, remainder = 2
total conns established = 1074779, hash count = 4646
server failures = 0
interface FastEthernet1/0, MAC 0010.f68f.7020
```

**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 の接続に関する詳細情報を表示します。

```
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、「[IOS SLB のモニタおよびメンテナンス](#)」(P.107) を参照してください。

## プローブの設定

プローブを設定するには、次の作業を実行します。

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.25) を参照してください。

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。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。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](#)」(P.56) (必須)
- 「[DNS プローブの設定](#)」(P.58) (必須)
- 「[HTTP プローブの設定](#)」(P.59) (必須)
- 「[ping プローブの設定](#)」(P.60) (必須)
- 「[TCP プローブの設定](#)」(P.61) (必須)
- 「[WSP プローブの設定](#)」(P.62) (必須)
- 「[プローブの関連付け](#)」(P.63) (必須)
- 「[プローブの確認](#)」(P.64) (任意)

## カスタム UDP プローブの設定

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	<b>enable</b>  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	<b>configure terminal</b>  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	<b>ip slb probe <i>probe</i> custom udp</b>  例: Router(config)# ip slb probe PROBE6 custom udp	IOS Server Load Balancing (IOS SLB) プローブの名前を設定し、カスタムユーザデータグラムプロトコル (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	<b>address [<i>ip-address</i>] [<b>routed</b>]</b>  例: Router(config-slb-probe)# address 10.1.1.1	(任意) カスタムユーザデータグラムプロトコル (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	<b>faildetect <i>number-of-probes</i></b>  例: Router(config-slb-probe)# faildetect 16	(任意) 連続して ACK が受信されないカスタムユーザデータグラムプロトコル (UDP) プローブの数を指定します。この数を超えると、実サーバの障害と見なされます。
ステップ6	<b>interval <i>seconds</i></b>  例: Router(config-slb-probe)# interval 11	(任意) カスタムユーザデータグラムプロトコル (UDP) プローブの送信タイマーを設定します。
ステップ7	<b>port <i>port</i></b>  例: Router(config-slb-probe)# port 8	カスタムユーザデータグラムプロトコル (UDP) プローブが接続するポートを設定します。
ステップ8	<b>request data {<i>start-byte</i>   <b>continue</b>} <i>hex-data-string</i></b>  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ユーザデータグラムプロトコル (UDP) 要求パケットのペイロードを定義します。

	コマンド	説明
ステップ9	<b>response</b> <i>clause-number data start-byte hex-data-string</i>  例: Router(config-slb-probe)# response 2 data 44 DD DD	カスタム ユーザ データグラム プロトコル (UDP) プローブ応答パケットに一致するデータ ストリングを定義します。
ステップ10	<b>timeout</b> <i>seconds</i>  例: Router(config-slb-probe)# timeout 20	(任意) カスタム ユーザ データグラム プロトコル (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

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	<b>enable</b>  例: Router> enable	特権 EXEC モードをイネーブルにします。 <ul style="list-style-type: none"><li>• プロンプトが表示されたら、パスワードを入力します。</li></ul>
ステップ2	<b>configure terminal</b>  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	<b>ip slb probe probe dns</b>  例: Router(config)# ip slb probe PROBE4 dns	IOS Server Load Balancing (IOS SLB) プローブの名前を設定し、ドメイン ネーム システム (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	<b>address</b> [ <i>ip-address</i> [ <b>routed</b> ]]  例: Router(config-slb-probe)# address 10.1.10.1	(任意) ドメイン ネーム システム (DNS) プローブの送信先 IP アドレスを設定します。
ステップ5	<b>faildetect</b> <i>number-of-probes</i>  例: Router(config-slb-probe)# faildetect 16	(任意) 連続して ACK が受信されないドメイン ネーム システム (DNS) 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。

	コマンド	説明
ステップ6	<b>interval</b> <i>seconds</i>  例: Router(config-slb-probe)# interval 11	(任意) ドメインネームシステム (DNS) プローブの送信タイマーを設定します。
ステップ7	<b>lookup</b> <i>ip-address</i>  例: Router(config-slb-probe)# lookup 10.1.10.1	(任意) ドメインネームシステム (DNS) サーバが、ドメインネーム解決要求に対する応答で示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

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	<b>enable</b>  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	<b>configure terminal</b>  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	<b>ip slb probe <i>probe</i> http</b>  例: Router(config)# ip slb probe PROBE2 http	IOS Server Load Balancing (IOS SLB) プローブの名前を設定し、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。

	コマンド	説明
ステップ4	<b>address</b> [ <i>ip-address</i> [ <b>routed</b> ]]  例: Router(config-slb-probe)# address 10.1.10.1	(任意) HTTP プロブの送信先 IP アドレスを設定します。
ステップ5	<b>credentials</b> { <i>username</i> [ <i>password</i> ]}  例: Router(config-slb-probe)# credentials Username1 password	(任意) HTTP プロブのヘッダー値を設定します。
ステップ6	<b>expect</b> [ <b>status</b> <i>status-code</i> ] [ <b>regex</b> <i>expression</i> ]  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	<b>header</b> <i>field-name</i> [ <i>field-value</i> ]  例: Router(config-slb-probe)# header HeaderName HeaderValue	(任意) HTTP プロブのヘッダー値を設定します。
ステップ8	<b>interval</b> <i>seconds</i>  例: Router(config-slb-probe)# interval 11	(任意) HTTP プロブの送信タイマーを設定します。
ステップ9	<b>port</b> <i>port</i>  例: Router(config-slb-probe)# port 8	(任意) HTTP プロブが接続するポートを設定します。
ステップ10	<b>request</b> [ <b>method</b> { <b>get</b>   <b>post</b>   <b>head</b>   <b>name</b> <i>name</i> }] [ <i>url path</i> ]  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。

さらに、HTTP プロ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、宛先に到達可能であることをソケット コードが確認するために必要です。結果として、HTTP プロブが適切に動作するために不可欠です。ルートには、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）またはデフォルト ルート（たとえば、**ip route 0.0.0.0 0.0.0.0** コマンドを使用して指定されます）を使用できます。

## ping プロブの設定

ping プロブを設定するには、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	<b>enable</b>  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	<b>configure terminal</b>  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	<b>ip slb probe</b> <i>probe ping</i>  例： Router(config)# ip slb probe PROBE1 ping	IOS Server Load Balancing (IOS SLB) プローブの名前を設定し、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	<b>address</b> [ <i>ip-address</i> [ <b>routed</b> ]]  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	<b>faildetect</b> <i>number-of-pings</i>  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	<b>interval</b> <i>seconds</i>  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

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	<b>enable</b>  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	<b>configure terminal</b>  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	<b>ip slb probe probe tcp</b>  例： Router(config)# ip slb probe PROBE5 tcp	IOS Server Load Balancing (IOS SLB) プローブの名前を設定し、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	<b>address [ip-address [routed]]</b>  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	<b>interval seconds</b>  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	<b>port port</b>  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

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	<b>enable</b>  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	<b>configure terminal</b>  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	<b>ip slb probe probe wsp</b>  例: Router(config)# ip slb probe PROBE3 wsp	IOS Server Load Balancing (IOS SLB) プローブの名前を設定し、Wireless Session Protocol (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	<b>address</b> [ <i>ip-address</i> [ <b>routed</b> ]]  例: Router(config-slb-probe)# address 10.1.10.1	(任意) Wireless Session Protocol (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	<b>interval</b> <i>seconds</i>  例: Router(config-slb-probe)# interval 11	(任意) Wireless Session Protocol (WSP) プローブの送信タイマーを設定します。
ステップ6	<b>url</b> [ <i>path</i> ]  例: Router(config-slb-probe)# url http://localhost/test.txt	(任意) Wireless Session Protocol (WSP) プローブの URL パスを設定します。

## プローブの関連付け

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、**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、「[サーバファームおよび実サーバの設定](#)」(P.38) および「[ファイアウォールロードバランシングの設定](#)」(P.50) 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	<b>enable</b>  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	<b>configure terminal</b>  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	<b>ip slb firewallfarm firewall-farm</b> または <b>ip slb serverfarm server-farm</b>  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	<b>probe probe</b>  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

プローブを確認するには、次の作業を実行します。

## 手順の概要

## 1. show ip slb probe

## 手順の詳細

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

DFP マネージャとして IOS SLB を設定し、IOS SLB が接続を開始する DFP エージェントを指定するには、次の作業を実行します。

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。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]]]`

### 手順の詳細

	コマンド	説明
ステップ 1	<code>enable</code>  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	<code>configure terminal</code>  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	<code>ip slb dfp [password [[encrypt] secret-string [timeout]]]</code>  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	<code>agent ip-address port [timeout [retry-count [retry-interval]]]</code>  例： Router(config-slb-dfp)# agent 10.1.1.1 2221 30 0 10	IOS Server Load Balancing (IOS SLB) が接続できる Dynamic Feedback Protocol (DFP) エージェントを指定します。

### この次の手順

IOS SLB を DFP エージェントとして設定するには、Cisco IOS リリース 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

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。
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

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。	<p>「サーバファームおよび実サーバの設定」の手順 (P.38) を参照してください。</p> <p>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。</p> <ul style="list-style-type: none"> <li>• GTP Cause Code Inspection をイネーブルにしない場合、<b>predictor</b> 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。</li> <li>• GTP Cause Code Inspection をイネーブルにする場合、加重ラウンドロビン (<b>roundrobin</b>) アルゴリズムまたは加重最小接続 (<b>leastconns</b>) アルゴリズムを指定します。</li> <li>• <b>real</b> コマンドを使用して、GGSN 機能を実行する実サーバの IP アドレス (Cisco GGSN の場合、仮想テンプレートアドレス) を指定します。</li> <li>• <b>reassign</b> コマンドを使用して、SGSN の N3-REQUESTS カウンタ値未満の <b>reassign threshold</b> を指定します。</li> </ul>

タスク	説明
<b>ステップ2</b> 仮想サーバを設定します。	<p>「<a href="#">仮想サーバの設定</a>」の手順 (P.42) を参照してください。</p> <p><b>virtual</b> 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。</p> <ul style="list-style-type: none"> <li>• 仮想 GGSN IP アドレスを仮想サーバとして指定し、<b>udp</b> キーワード オプションを指定します。</li> <li>• 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 <b>any</b> を指定します。</li> <li>• 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 <b>any</b> を指定します。</li> <li>• 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、<b>service gtp</b> キーワード オプションを指定します。</li> <li>• 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、<b>service gtp-inspect</b> キーワード オプションを指定します。</li> </ul> <p>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、<b>idle</b> コマンドを使用して <b>idle</b> 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。</p>
<b>ステップ3</b> 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。	<p>(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、『<a href="#">Cisco IOS Interface Configuration Guide</a>』の「<a href="#">Configuring Virtual Interfaces</a>」の項を参照してください。</p>
<b>ステップ4</b> 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。	<p>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、『<a href="#">Cisco IOS Mobile Wireless Configuration Guide</a>』の「<a href="#">Configuring Network Access to the GGSN</a>」の項を参照してください。</p>
<b>ステップ5</b> 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。	<p>(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。</p>
<b>ステップ6</b> GSN アイドルタイマーを設定します。	<p>(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。</p> <p>詳細については、「<a href="#">GSN アイドルタイマーの設定</a>」(P.68) を参照してください。</p>

## GSN アイドル タイマーの設定

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	<code>enable</code>  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	<code>configure terminal</code>  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	<code>ip slb timers gtp gsn duration</code>  例: Router(config)# ip slb timers gtp gsn 45	IOS Server Load Balancing (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 の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には、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には、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) を使用するよう設定します。このとき、 <b>gprs slb mode</b> 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、GGSN 5.0 for Cisco IOS リリース 12.3(2)XU 以降の『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。	「サーバファームおよび実サーバの設定」の手順 (P.38) を参照してください。  GGSN-IOS SLB メッセージングのサーバファームおよび実サーバを設定する場合、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しないように、 <b>no faildetect inband</b> コマンドを指定して、自動サーバ障害検出機能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」の手順 (P.42) を参照してください。  GGSN-IOS SLB メッセージングの仮想サーバを設定する場合、 <b>gtp notification cac</b> コマンドを指定して、IOS SLB がセッションを新しい実サーバに再割り当てできる回数を制限します。

## GPRS ロードバランシングマップの設定

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 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のマップをイネーブルにするには、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 ip-address [netmask [group]] {tcp | udp} [port | any] [service service]**
8. **serverfarm primary-farm [backup backup-farm [sticky]] [map map-id priority priority]**

## 手順の詳細

	コマンド	説明
ステップ1	<b>enable</b>  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	<b>configure terminal</b>  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	<b>ip slb map map-id gtp   radius)</b>  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	<b>apn string</b>  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	<b>exit</b>  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	<b>ip slb vserver virtual-server</b>  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	<pre>virtual ip-address [netmask [group]] {tcp   udp} [port   any] [service service]</pre> <p>例:</p> <pre>Router(config-slb-vserver)# virtual 10.10.10.10 udp 0 service gtp</pre>	<p>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。</p> <p>(注) GPRS ロードバランシングの場合:</p> <ul style="list-style-type: none"> <li>- 仮想 GGSN IP アドレスを仮想サーバとして指定し、<b>udp</b> キーワード オプションを指定します。</li> <li>- 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 <b>any</b> を指定します。</li> <li>- 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 <b>any</b> を指定します。</li> <li>- 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、<b>service gtp</b> キーワード オプションを指定します。</li> <li>- 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、<b>service gtp-inspect</b> キーワード オプションを指定します。</li> </ul>
ステップ8	<pre>serverfarm primary-farm [backup backup-farm [sticky]] [map map-id priority priority]</pre> <p>例:</p> <pre>Router(config-slb-vserver)# serverfarm farm1 backup farm2 map 1 priority 3</pre>	<p>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。</p> <p>(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。</p> <p>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、<b>serverfarm</b> コマンドを複数設定し、それぞれに固有のマップ ID と固有のプライオリティを指定します (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)。</p> <p>GTP マップを使用し、複数のサーバファームで 1 つの実サーバを設定した場合、異なる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。</p>

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

KAL-AP エージェントの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	<code>enable</code>  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	<code>configure terminal</code>  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	<code>ip slb capp udp</code>  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	<code>peer [ip-address] port port</code>  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	<code>peer [ip-address] secret [encrypt] secret-string</code>  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	<code>exit</code>  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	<code>ip slb serverfarm server-farm</code>  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	<code>kal-ap domain tag</code>  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	<code>farm-weight setting</code>  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 ステイック ルーティング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
<b>ステップ1</b> サーバファームおよび実サーバを設定します。	<p>「サーバファームおよび実サーバの設定」の手順 (P.38) を参照してください。</p> <p>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。</p> <ul style="list-style-type: none"> <li>• <b>predictor</b> 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。</li> <li>• (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、<b>faildetect numconns</b> コマンドで <b>numclients</b> キーワードに値 1 を指定します。</li> <li>• (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 スティック加入者の最大数を指定するには、<b>maxclients</b> コマンドを使用します。</li> </ul>
<b>ステップ2</b> 仮想サーバを設定します。	<p>「仮想サーバの設定」の手順 (P.42) を参照してください。</p> <p>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。</p> <ul style="list-style-type: none"> <li>• <b>virtual</b> コマンドを使用して、<b>service radius</b> キーワード オプションを指定します。</li> <li>• (任意) 入力インターフェイスを検査するために <b>framed-IP</b> ルーティングをイネーブルにするには、<b>access interface route framed-ip</b> コマンドを指定します。</li> </ul> <p><b>access interface route framed-ip</b> コマンドを設定する場合、さらに <b>service radius</b> キーワードを指定した <b>virtual</b> コマンドを設定する必要があります。</p> <ul style="list-style-type: none"> <li>• (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、<b>hand-off radius</b> コマンドを設定します。</li> <li>• (任意) IOS SLB セッションデータベースで RADIUS エントリのデューレーションを設定するには、<b>radius request</b> キーワードを指定した <b>idle</b> コマンドを設定します。</li> <li>• (任意) IOS SLB RADIUS framed-IP スティックデータベースでエントリのデューレーションを設定するには、<b>radius framed-ip</b> キーワードを指定した <b>idle</b> コマンドを設定します。</li> </ul>

タスク	説明
仮想サーバを設定します。 (続き)	<p data-bbox="635 331 1283 360">「仮想サーバの設定」の手順 (P.42) を参照してください。</p> <p data-bbox="635 376 1501 439">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。</p> <ul data-bbox="647 454 1501 577" style="list-style-type: none"> <li>• (任意) IOS SLB が、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 要求および非 RADIUS フローを同じサービス ゲートウェイに送信できるようにするには、<b>sticky</b> コマンドで <b>radius framed-ip</b> キーワードを指定します。</li> </ul> <p data-bbox="683 595 1485 658"><b>sticky radius framed-ip</b> コマンドを設定する場合、さらに <b>service radius</b> キーワードを指定した <b>virtual</b> コマンドを設定する必要があります。</p> <ul data-bbox="647 674 1501 797" style="list-style-type: none"> <li>• (任意) Accounting ON または OFF メッセージの受信時に、IOS SLB が IOS SLB RADIUS framed-ip スティッキ データベースのエントリを消去できるようにするには、<b>purge radius framed-ip acct on-off</b> 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。</li> </ul> <p data-bbox="683 815 1501 938">Accounting ON または OFF メッセージの受信時に、IOS SLB が IOS SLB RADIUS framed-ip スティッキ データベースのエントリを消去できないようにするには、<b>no purge radius framed-ip acct on-off</b> 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。</p> <ul data-bbox="647 954 1501 1077" style="list-style-type: none"> <li>• (任意) Accounting-Stop メッセージの受信時に、IOS SLB が IOS SLB RADIUS framed-ip スティッキ データベースのエントリを消去できるようにするには、<b>purge radius framed-ip acct stop</b> 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。</li> </ul> <p data-bbox="683 1095 1501 1218">Accounting-Stop メッセージの受信時に、IOS SLB が IOS SLB RADIUS framed-ip スティッキ データベースのエントリを消去できないようにするには、<b>no purge radius framed-ip acct stop</b> 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。</p>

タスク	説明
仮想サーバを設定します。 (続き)	<p>「仮想サーバの設定」の手順 (P.42) を参照してください。</p> <p>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。</p> <ul style="list-style-type: none"> <li>               (任意：CDMA2000 ネットワーク用のみ) IOS SLB が 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 ゲートウェイに送信できるようにするには、<b>sticky</b> コマンドで <b>radius calling-station-id</b> キーワードを指定します。             </li> </ul> <p>IOS SLB が 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 ゲートウェイに送信できるようにするには、<b>sticky</b> コマンドで <b>radius username</b> キーワードを指定します。</p> <p><b>sticky radius calling-station-id</b> コマンドまたは <b>sticky radius username</b> コマンドを設定する場合、さらに <b>service radius</b> キーワードを指定した <b>virtual</b> コマンドを設定し、<b>sticky radius framed-ip</b> コマンドを設定する必要があります。</p> <p>同じ仮想サーバに <b>sticky radius calling-station-id</b> コマンドと <b>sticky radius username</b> コマンドの両方を設定することはできません。</p> <ul style="list-style-type: none"> <li>               (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場合のみ) 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 が 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、<b>radius inject auth</b> コマンドを設定します。             </li> </ul> <p>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、<b>radius inject auth timer</b> コマンドを設定します。</p> <p>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、<b>radius inject auth vsa</b> コマンドを設定します。</p> <p>アカウントिंग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、<b>radius inject acct</b> コマンドを設定します。</p>
<b>ステップ 3</b> IOS SLB で、RADIUS framed-IP スティッキ ルーティングの packets を検査できるようにします。	(任意) 「RADIUS framed-IP スティッキ ルーティングの packets の検査のイネーブル化」 (P.77) を参照してください。
<b>ステップ 4</b> 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」 (P.78) を参照してください。
<b>ステップ 5</b> 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」 (P.80) を参照してください。

タスク	説明
ステップ6 使用できる MLS エントリの数を増やします。	<p>(任意) Supervisor Engine 2 を搭載した Catalyst 6500 ファミリ スイッチで <code>dispatched</code> モードを使用して IOS SLB を実行している場合、<code>no mls netflow</code> コマンドを設定するとパフォーマンスを改善できます。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。</p> <p>(注) <code>micro-flow QoS</code>、<code>reflexive ACL</code>、<code>TCP intercept</code>、<code>Web Cache Redirect</code> 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、<code>no mls netflow</code> コマンドは設定しないでください。</p> <p>MLS NetFlow の設定方法の詳細については、『<i>Catalyst 6000 Family IOS Software Configuration Guide</i>』を参照してください。</p>
ステップ7 プローブを設定します。	<p>「<a href="#">プローブの設定</a>」(P.56) を参照してください。</p> <p>サーバの動作状況を確認するには、<code>ping</code> プローブを設定します。</p>

## RADIUS framed-IP ステイッキ ルーティングの packets 検査のイネーブル化

IOS SLB で、RADIUS framed-IP ステイッキ ルーティングの packets 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 packets を検査するように設定できます。検査対象の packets の発信元 IP アドレスが、IOS SLB RADIUS framed-IP ステイッキ データベースのエントリと一致する場合、packets 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 packets 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	<b>enable</b>  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	<b>configure terminal</b>  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	<b>ip slb route {framed-ip deny   ip-address netmask framed-ip   inter-firewall}</b>  例： Router(config)# ip slb route 10.10.10.1 255.255.255.255 framed-ip	IOS Server Load Balancing (IOS SLB) で、RADIUS framed-IP ステイッキ 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、特定のファイアウォール実サーバから別のファイアウォール実サーバを介するパケットのルーティング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

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 ip-address [netmask [group]] {tcp | udp} [port | any] [service service]**
9. **serverfarm primary-farm [backup backup-farm [sticky]] [map map-id priority priority]**

## 手順の詳細

	コマンド	説明
ステップ1	<b>enable</b>  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	<b>configure terminal</b>  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	<b>ip slb map map-id radius</b>  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	<b>calling-station-id string</b>  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	<b>username string</b>  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	<b>exit</b>  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	<b>ip slb vserver virtual-server</b>  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。

<b>ステップ 8</b>	<pre>virtual ip-address [netmask [group]] {tcp   udp} [port   any] [service service]</pre> <p>例:</p> <pre>Router(config-slb-vserver)# virtual 10.0.0.1 udp 0 service radius</pre>	<p>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。</p> <p>(注) RADIUS ロードバランシングの場合、<b>service radius</b> キーワード オプションを指定します。</p>
<b>ステップ 9</b>	<pre>serverfarm primary-farm [backup backup-farm [sticky]] [map map-id priority priority]</pre> <p>例:</p> <pre>Router(config-slb-vserver)# serverfarm SF1 backup SF2 map 1 priority 1</pre>	<p>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。</p> <p>(注) RADIUS ロードバランシングは <b>sticky</b> キーワードをサポートしません。</p> <p>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、<b>serverfarm</b> コマンドを複数設定し、それぞれに固有のマップ ID と固有のプライオリティを指定します (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)。</p>

## 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

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ます) は、CSG 環境でポリシーベースルーティング (PBR) ルートマップを使用し、加入者のデータプレーントラフィックを処理する高パフォーマンスの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、アカウントिंग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 ip-address [netmask [group]] {tcp | udp} [port | any] [service service]**
8. **serverfarm primary-farm [backup backup-farm [sticky]] [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	<code>enable</code>  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	<code>configure terminal</code>  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	<code>ip slb serverfarm server-farm</code>  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	<code>predictor [roundrobin   leastconns   route-map mapname]</code>  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、 <b>route-map</b> キーワードおよび <i>mapname</i> 引数が必要です。  <b>predictor route-map</b> 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	<code>exit</code>  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	<code>ip slb vserver virtual-server</code>  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	<code>virtual ip-address [netmask [group]] {tcp   udp} [port   any] [service service]</code>  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、 <b>service radius</b> キーワード オプションを指定します。

<p><b>ステップ 8</b></p>	<pre>serverfarm primary-farm [backup backup-farm [sticky]] [map map-id priority priority]</pre> <p>例： Router(config-slb-vserver)# serverfarm AAAFARM</p>	<p>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。</p> <p>(注) RADIUS ロードバランシングは <b>sticky</b> キーワードをサポートしません。</p> <p>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、<b>serverfarm</b> コマンドを複数設定し、それぞれに固有のマップ ID と固有のプライオリティを指定します (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)。</p>
<p><b>ステップ 9</b></p>	<pre>radius acct local-ack key [encrypt] secret-string</pre> <p>例： Router(config-slb-vserver)# radius acct local-ack key SECRET_PASSWORD</p>	<p>(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。</p> <p>(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。</p> <p>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。</p>
<p><b>ステップ 10</b></p>	<pre>radius inject auth group-number {calling-station-id   username}</pre> <p>例： Router(config-slb-vserver)# radius inject auth 1 calling-station-id</p>	<p>(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。</p> <p>特定の認証仮想サーバについて、単一の <b>radius inject auth group-number calling-station-id</b> コマンド、または単一の <b>radius inject auth group-number username</b> 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。</p> <p>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。</p>

<p><b>ステップ 11</b> <code>radius inject auth timer seconds</code></p> <p>例： Router(config-slb-vserver)# radius inject auth timer 45</p>	<p>(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) 関連付けのタイマーを設定します。</p> <p>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。</p>
<p><b>ステップ 12</b> <code>radius inject auth vsa vendor-id</code></p> <p>例： Router(config-slb-vserver)# radius inject auth vsa vendor1</p>	<p>(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) 関連付けの VSA をバッファリングします。</p> <p>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。</p>

## mSEF 用 Exchange Director の設定作業リスト

mSEF 用 Exchange Director を設定するには、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」 (P.83)
- 「Exchange Director 用のファイアウォールの設定」 (P.86)

## 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 ステイックルーティングの packets 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
<b>ステップ1</b> サーバファームおよび実サーバを設定します。	<p>「サーバファームおよび実サーバの設定」の手順 (P.38) を参照してください。</p> <p>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。</p> <ul style="list-style-type: none"> <li>• (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、<b>faildetect numconns</b> コマンドで <b>numclients</b> キーワードに値 1 を指定します。</li> <li>• (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 スティック加入者の最大数を指定するには、<b>maxclients</b> コマンドを使用します。</li> </ul>
<b>ステップ2</b> 仮想サーバを設定します。	<p>「仮想サーバの設定」の手順 (P.42) を参照してください。</p> <p>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。</p> <ul style="list-style-type: none"> <li>• <b>virtual</b> コマンドを使用して、<b>service radius</b> キーワード オプションを指定します。</li> <li>• (任意) 入力インターフェイスを検査するために <b>framed-IP</b> ルーティングをイネーブルにするには、<b>access interface route framed-ip</b> コマンドを指定します。</li> </ul> <p><b>access interface route framed-ip</b> コマンドを設定する場合、さらに <b>service radius</b> キーワードを指定した <b>virtual</b> コマンドを設定する必要があります。</p> <ul style="list-style-type: none"> <li>• (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、<b>hand-off radius</b> コマンドを設定します。</li> <li>• (任意) IOS SLB セッションデータベースで RADIUS エントリのデューレーションを設定するには、<b>radius request</b> キーワードを指定した <b>idle</b> コマンドを設定します。</li> <li>• (任意) IOS SLB RADIUS framed-IP スティックデータベースでエントリのデューレーションを設定するには、<b>radius framed-ip</b> キーワードを指定した <b>idle</b> コマンドを設定します。</li> </ul>

タスク	説明
仮想サーバを設定します。 (続き)	<p>「仮想サーバの設定」の手順 (P.42) を参照してください。</p> <p>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。</p> <ul style="list-style-type: none"> <li>• (任意) IOS SLB が、IOS SLB RADIUS framed-IP スティックデータベースを作成し、特定の加入者からの RADIUS 要求および非 RADIUS フローを同じサービスゲートウェイに送信できるようにするには、<b>sticky</b> コマンドで <b>radius framed-ip</b> キーワードを指定します。</li> </ul> <p><b>sticky radius framed-ip</b> コマンドを設定する場合、さらに <b>service radius</b> キーワードを指定した <b>virtual</b> コマンドを設定する必要があります。</p> <ul style="list-style-type: none"> <li>• (任意: CDMA2000 ネットワーク用のみ) IOS SLB が IOS SLB RADIUS calling-station-ID スティック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送信できるようにするには、<b>sticky</b> コマンドで <b>radius calling-station-id</b> キーワードを指定します。</li> </ul> <p>IOS SLB が IOS SLB RADIUS username スティック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送信できるようにするには、<b>sticky</b> コマンドで <b>radius username</b> キーワードを指定します。</p> <p><b>sticky radius calling-station-id</b> コマンドまたは <b>sticky radius username</b> コマンドを設定する場合、さらに <b>service radius</b> キーワードを指定した <b>virtual</b> コマンドを設定し、<b>sticky radius framed-ip</b> コマンドを設定する必要があります。</p> <p>同じ仮想サーバに <b>sticky radius calling-station-id</b> コマンドと <b>sticky radius username</b> コマンドの両方を設定することはできません。</p>
ステップ3 IOS SLB で、RADIUS framed-IP スティックルーティングの packets を検査できるようにします。	(任意) 「RADIUS framed-IP スティックルーティングの packets の検査のイネーブル化」(P.77) 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」(P.78) 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。	<p>(任意) Supervisor Engine 2 を搭載した Catalyst 6500 ファミリスイッチで <b>dispatched</b> モードを使用して IOS SLB を実行している場合、<b>no mls netflow</b> コマンドを設定するとパフォーマンスを改善できます。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。</p> <p>(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、<b>no mls netflow</b> コマンドは設定しないでください。</p> <p>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。</p>
ステップ6 プローブを設定します。	<p>「プローブの設定」(P.56) を参照してください。</p> <p>サーバの動作状況を確認するには、<b>ping</b> プロブを設定します。</p>

## 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」(P.86) (必須)
- 「ファイアウォールファームの確認」(P.89) (任意)
- 「ファイアウォール接続の確認」(P.90) (任意)
- 「プローブの設定」(P.91) (必須)
- 「ワイルドカード検索の設定」(P.92) (任意)
- 「MLS エントリのプロトコルレベル消去の設定」(P.92) (任意)
- 「接続の消去要求動作の設定」(P.92) (任意)
- 「スティッキ接続の消去要求動作の設定」(P.92) (任意)

### ファイアウォールファームの設定

ファイアウォールファームを設定するには、次の作業を実行します。

#### 手順の概要

1. `enable`
2. `configure terminal`
3. `ip slb 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	<code>enable</code>  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	<code>configure terminal</code>  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	<code>ip slb firewallfarm firewall-farm</code>  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 ロードバランシング (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	<code>real ip-address</code>  例: Router(config-slbfw)# 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	<code>probe probe</code>  例: Router(config-slbfw-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	<code>weight setting</code>  例: Router(config-slbfw-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	<code>inservice</code>  例: Router(config-slbfw-real)# inservice	ファイアウォールおよび IOS Server Load Balancing (IOS SLB) が使用するファイアウォールをイネーブルにします。
ステップ8	<code>exit</code>  例: Router(config-slbfw-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。
ステップ9	<code>access [source source-ip netmask] [destination destination-ip netmask]   inbound inbound-interface   outbound outbound-interface]</code>  例: Router(config-slbfw)# 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
<b>ステップ 10</b> <code>predictor hash address [port]</code>  例: <code>Router(config-slb-fw)# predictor hash address</code>	(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。
<b>ステップ 11</b> <code>purge connection</code>  例: <code>Router(config-slb-fw)# purge connection</code>	(任意) IOS Server Load Balancing (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。
<b>ステップ 12</b> <code>purge sticky</code>  例: <code>Router(config-slb-fw)# purge sticky</code>	(任意) スティックイ アイドル タイマーが期限切れになるとき、IOS Server Load Balancing (IOS SLB) ファイアウォール ロード バランシングから消去要求を送信できるようにします。
<b>ステップ 13</b> <code>replicate casa listen-ip remote-ip port [interval] [password [[encrypt] secret-string [timeout]]]</code>  例: <code>Router(config-slb-fw)# replicate casa 10.10.10.11 10.10.11.12 4231</code>	(任意) バックアップ スイッチに対する IOS Server Load Balancing (IOS SLB) ファイアウォール ロード バランシングの判定テーブルのステートフル バックアップを設定します。
<b>ステップ 14</b> <code>protocol tcp</code>  例: <code>Router(config-slb-fw)# protocol tcp</code>	(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。
<b>ステップ 15</b> <code>delay duration</code>  例: <code>Router(config-slb-fw-tcp)# delay 30</code>	(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、接続の終了後、IOS Server Load Balancing (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。
<b>ステップ 16</b> <code>idle duration</code>  例: <code>Router(config-slb-fw-tcp)# idle 120</code>	(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 アクティビティがない場合、IOS Server Load Balancing (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。
<b>ステップ 17</b> <code>maxconns maximum-number</code>  例: <code>Router(config-slb-fw-tcp)# maxconns 1000</code>	(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。
<b>ステップ 18</b> <code>sticky seconds [netmask netmask] [source   destination]</code>  例: <code>Router(config-slb-fw-tcp)# sticky 60</code>	(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。 <ul style="list-style-type: none"> <li>• 同じペアの IP アドレス間に接続が存在する間 (発信元/宛先スティッキー)。</li> <li>• 最後の接続が破棄された後の <i>duration</i> で定義される期間。</li> </ul>



コマンド	目的
<b>ステップ 19</b> <code>exit</code>  例: <code>Router(config-slb-fw-tcp)# exit</code>	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。
<b>ステップ 20</b> <code>protocol datagram</code>  例: <code>Router(config-slb-fw)# protocol datagram</code>	(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。
<b>ステップ 21</b> <code>idle duration</code>  例: <code>Router(config-slb-fw-udp)# idle 120</code>	(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 アクティビティがない場合、IOS Server Load Balancing (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。
<b>ステップ 22</b> <code>maxconns maximum-number</code>  例: <code>Router(config-slb-fw-udp)# maxconns 1000</code>	(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。
<b>ステップ 23</b> <code>sticky seconds [netmask netmask] [source   destination]</code>  例: <code>Router(config-slb-fw-udp)# sticky 60</code>	(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。 <ul style="list-style-type: none"> <li>• 同じペアの IP アドレス間に接続が存在する間 (発信元/宛先スティッキー)。</li> <li>• 最後の接続が破棄された後の <i>duration</i> で定義される期間。</li> </ul>
<b>ステップ 24</b> <code>exit</code>  例: <code>Router(config-slb-fw-udp)# exit</code>	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。
<b>ステップ 25</b> <code>inservice</code>  例: <code>Router(config-slb-fw)# inservice</code>	IOS Server Load Balancing (IOS SLB) が使用するファイアウォールファームをイネーブルにします。

## ファイアウォールファームの確認

ファイアウォールファームを確認するには、次の作業を実行します。

### 手順の概要

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

## 手順の詳細

- ステップ 1** 次の **show ip slb reals** 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

ファイアウォールの接続を確認するには、次の作業を実行します。

## 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済みで、適切に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詳細情報を表示します。

```
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、通常の IOS スイッチング パスで IOS SLB パケットが処理される時です (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)。特殊なスイッチングは、ハードウェア割り当てのスイッチング パスで IOS SLB パケットが処理される時です。

**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 real detail

10.1.1.3, FIRE1, state = OPERATIONAL, type = firewall
  conns = 299310, dummy_conns = 0, maxconns = 4294967295
  weight = 10, weight(admin) = 10, metric = 104, remainder = 2
  total conns established = 1074779, hash count = 4646
  server failures = 0
  interface FastEthernet1/0, MAC 0010.f68f.7020

```

**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の接続に関する詳細情報を表示します。

```

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、「[IOS SLB のモニタおよびメンテナンス](#)」(P.107) を参照してください。

## プローブの設定

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. 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。

- ping プロブが推奨されます。詳細については、「[ping プロブの設定](#)」(P.60) を参照してください。
- ファイアウォールで、ping プロブの転送を許可していない場合、代わりに HTTP プロブを使用します。詳細については、「[HTTP プロブの設定](#)」(P.59) 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

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. mls ip slb wildcard search rp

### 手順の詳細

PFC 上の TCAM の容量を超える可能性を減らすには、**mls ip slb wildcard search rp** コマンドを使用します。

## MLS エントリのプロトコルレベル消去の設定

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。

## 接続の消去要求動作の設定

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。

## スティッキ接続の消去要求動作の設定

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

スティッキー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、スティッキー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）。

スティッキー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
<b>ステップ1</b> サーバファームおよび実サーバを設定します。	<p>「サーバファームおよび実サーバの設定」の手順 (P.38) を参照してください。</p> <p>VPN サーバ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、<b>real</b> コマンドを使用して、VPN ターミネータとして動作する実サーバの IP アドレスを指定します。</p>
<b>ステップ2</b> 仮想サーバを設定します。	<p>「仮想サーバの設定」の手順 (P.42) を参照してください。</p> <p>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。</p> <ul style="list-style-type: none"> <li>• プロトコルを <b>udp</b>、ポートを <b>isakmp</b> に設定した <b>virtual</b> コマンドを使用して、UDP 仮想サーバを設定します。<b>isakmp</b> キーワードを使用すると、IKE (ポート 500) を介して暗号鍵を交換できます。</li> <li>• プロトコルを <b>esp</b> に設定した <b>virtual</b> コマンドを使用して、ESP 仮想サーバを設定します。</li> <li>• 15 秒以上の <i>duration</i> を指定した <b>sticky</b> 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。</li> </ul> <p>PPTP 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。</p> <ul style="list-style-type: none"> <li>• <b>tcp</b> キーワードとポート番号 <b>1723</b> を指定した <b>virtual</b> コマンドを使用して、TCP 仮想サーバを設定します。</li> <li>• <b>gre</b> キーワードを指定した <b>virtual</b> コマンドを使用して、GRE 仮想サーバを設定します。</li> <li>• 15 秒以上の <i>duration</i> を指定した <b>sticky</b> 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。</li> </ul>
<b>ステップ3</b> プローブを設定します。	<p>「プローブの設定」 (P.56) を参照してください。</p> <p>サーバの動作状況を確認するには、<b>ping</b> プローブを設定します。</p>

## ASN R6 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。	Mobile Subscriber Station (MSS) からの要求を IOS SLB で処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。	「 <a href="#">プローブの設定</a> 」(P.56) 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。	「 <a href="#">サーバファームおよび実サーバの設定</a> 」の手順 (P.38) を参照してください。 ASN R6 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、 <b>real</b> 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。
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。	「 <a href="#">仮想サーバの設定</a> 」の手順 (P.42) を参照してください。 ASN R6 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。 <ul style="list-style-type: none"> <li>• サービスを <b>asn r6</b> に設定した <b>virtual</b> コマンドを使用して、仮想サーバを設定します。</li> <li>• サービスを <b>asn r6 request</b> キーワードに設定した <b>idle</b> コマンドを使用して、ASN R6 ロードバランシングのアイドル接続タイマーを設定します。</li> </ul>

## 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. DFP を設定します。

## 手順の詳細

タスク	説明
<b>ステップ1</b> サーバファームおよび実サーバを設定します。	<p>「サーバファームおよび実サーバの設定」の手順 (P.38) を参照してください。</p> <p>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。</p> <ul style="list-style-type: none"> <li>• <b>predictor</b> 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。</li> <li>• <b>real</b> 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。</li> </ul>
<b>ステップ2</b> 仮想サーバを設定します。	<p>「仮想サーバの設定」の手順 (P.42) を参照してください。</p> <p><b>virtual</b> 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。</p> <ul style="list-style-type: none"> <li>• 仮想サーバとして Home Agent Director の IP アドレスを指定します。</li> <li>• <b>udp</b> キーワードオプションを指定します。</li> <li>• 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 <b>any</b> を指定します。</li> <li>• <b>service ipmobile</b> キーワードオプションを指定します。</li> </ul>
<b>ステップ3</b> 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。	<p>(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。</p>
<b>ステップ4</b> DFP を設定します。	<p>(任意) 「DFP の設定」 (P.65) を参照してください。</p> <p>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。</p> <ul style="list-style-type: none"> <li>• 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、<b>ip mobile home-agent dfp-max-weight</b> コマンドを使用します。</li> <li>• 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、<b>ip mobile home-agent dynamic-address</b> コマンドを使用します。</li> <li>• バインディングの最大数を設定するには、<b>ip mobile home-agent max-binding</b> コマンドを使用します。</li> </ul> <p>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。</p>



## NAT の設定

クライアント NAT 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	<code>enable</code>  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	<code>configure terminal</code>  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	<code>ip slb natpool pool start-ip end-ip [netmask netmask   prefix-length leading-1-bits] [entries init-address [max-address]]</code>  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 のクライアント アドレス プールを設定する必要はありません。
ステップ4	<code>nat {client pool   server}</code>  例: Router(config-slb-sfarm)# nat server	SLB NAT を設定し、NAT モードを指定します。

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、「[サーバファームおよび実サーバの設定](#)」(P.38) 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

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 を使用すると、一部のユーザは NAT を利用し、同じイーサネット インターフェイスの他のユーザは、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。



(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	<code>enable</code>  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	<code>configure terminal</code>  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	<code>ip slb static {drop   nat {virtual   virtual-ip [per-packet   sticky]}}</code>  例: Router(config)# ip slb static nat 10.1.10.1 per-packet	実サーバのネットワーク アドレス変換 (NAT) の動作を設定し、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) <code>virtual-ip</code> 引数を指定し、 <code>per-packet</code> オプションを指定しない場合、IOS Server Load Balancing (IOS SLB) ではサーバポートの変換を使用して、別の実サーバから開始された接続要求を区別します。
ステップ4	<code>real ip-address [port]</code>  例: Router(config-slb-static)# real 10.1.1.3	スタティック ネットワーク アドレス変換 (NAT) を使用するには、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)「 <a href="#">必須および任意の IOS SLB 機能の設定</a> 」(P.38)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)「 <a href="#">ファイアウォール ロード バランシングの設定</a> 」(P.50)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)「 <a href="#">ステートレス バックアップ設定の確認</a> 」(P.99)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

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 <b>ip slb replicate slave rate</b> 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)「 <a href="#">必須および任意の IOS SLB 機能の設定</a> 」(P.38) 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。 <ul style="list-style-type: none"> <li>• <b>replicate slave</b> コマンドを指定します。</li> <li>• (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、<b>replicate interval</b> コマンドを設定します。</li> </ul>
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)「 <a href="#">ファイアウォール ロード バランシングの設定</a> 」(P.50) 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。 <ul style="list-style-type: none"> <li>• <b>replicate slave</b> コマンドを指定します。</li> <li>• (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、<b>replicate interval</b> コマンドを設定します。</li> </ul>

## データベース エントリの設定

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 <b>enable</b>  例： Router> enable	特権 EXEC モードをイネーブルにします。 <ul style="list-style-type: none"> <li>• プロンプトが表示されたら、パスワードを入力します。</li> </ul>

## IOS SLB の設定方法

	コマンドまたはアクション	目的
ステップ2	<code>configure terminal</code>  例： Router# <code>configure terminal</code>	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	<code>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]]]</code>  例： Router(config)# <code>ip slb entries conn 128000 512000</code>	IOS Server Load Balancing (IOS SLB) データベース エントリの最初の割り当てと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 データベースのバッファの設定

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	<code>enable</code>  例： Router> <code>enable</code>	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	<code>configure terminal</code>  例： Router# <code>configure terminal</code>	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	<code>ip slb maxbuffers frag buffers</code>  例： Router(config)# <code>ip slb maxbuffers frag 300</code>	IOS Server Load Balancing (IOS SLB) フラグメント データベースのバッファの最大数を設定します。

## データベースおよびカウンタのクリア

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 gtp imsi [id imsi]`
5. `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	<pre>clear ip slb connections [firewallfarm <i>firewall-farm</i>   serverfarm <i>server-farm</i>   vserver <i>virtual-server</i>]</pre> <p>例: Router# clear ip slb connections vserver VSERVER1</p>	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、または仮想サーバについて、IOS Server Load Balancing (IOS SLB) 接続データベースをクリアします。
ステップ2	<pre>clear ip slb counters [kal-ap]</pre> <p>例: Router# clear ip slb counters</p>	IOS Server Load Balancing (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、 <b>kal-ap</b> キーワードを使用します。
ステップ3	<pre>clear ip slb sessions [firewallfarm <i>firewall-farm</i>   serverfarm <i>server-farm</i>   vserver <i>virtual-server</i>]</pre> <p>例: Router# clear ip slb sessions serverfarm FARM1</p>	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、または仮想サーバについて、IOS Server Load Balancing (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	<pre>clear ip slb sticky gtp imsi [id <i>imsi</i>]</pre> <p>例: Router# clear ip slb sticky gtp imsi</p>	IOS Server Load Balancing (IOS SLB) グローバルパケットラジオ サービス (GPRS) トンネリングプロトコル (GTP) International Mobile Subscriber ID (IMSI) スティックデータベースからのエントリをクリアします。
ステップ5	<pre>clear ip slb sticky radius {calling-station-id [id <i>string</i>]   framed-ip [<i>framed-ip</i> [<i>netmask</i>]]}</pre> <p>例: Router# clear ip slb sticky radius framed-ip</p>	IOS Server Load Balancing (IOS SLB) RADIUS スティックデータベースからのエントリをクリアします。

## ワイルドカード検索の設定

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	<b>enable</b>  例： Router> enable	特権 EXEC モードをイネーブルにします。 <ul style="list-style-type: none"><li>プロンプトが表示されたら、パスワードを入力します。</li></ul>
ステップ2	<b>configure terminal</b>  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)# <b>mls ip slb search</b> {wildcard [pfc   rp]   icmp}  例： Router(config)# mls ip slb search wildcard rp	IOS Server Load Balancing (IOS SLB) ワイルドカード検索の動作を指定します。  このコマンドがサポートされるのは Catalyst 6500 ファミリースイッチだけです。

## MLS エントリのプロトコルレベル消去の設定

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	<b>enable</b>  例： Router> enable	特権 EXEC モードをイネーブルにします。 <ul style="list-style-type: none"><li>プロンプトが表示されたら、パスワードを入力します。</li></ul>
ステップ2	<b>configure terminal</b>  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)# <b>mls ip slb purge global</b>  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。  このコマンドがサポートされるのは Catalyst 6500 ファミリースイッチだけです。



## 接続の消去および再割り当て

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 ステイッキ 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 | 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	<b>enable</b>  例： Router> enable	特権 EXEC モードをイネーブルにします。 <ul style="list-style-type: none"><li>• プロンプトが表示されたら、パスワードを入力します。</li></ul>
ステップ 2	<b>configure terminal</b>  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	<b>ip slb serverfarm <i>server-farm</i></b>  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	<b>failaction [purge   gtp purge   radius reassign]</b>  例： Router(config-slb-sfarm)# <b>failaction purge</b>	実サーバに障害が発生した場合の IOS Server Load Balancing (IOS SLB) の動作を設定します。
ステップ 5	<b>exit</b>  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。

	コマンドまたはアクション	目的
ステップ6	<code>ip slb firewallfarm <i>firewall-farm</i></code>  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	<code>failaction purge</code>  例: Router(config-slb-fw)# failaction purge	ファイアウォールに障害が発生した場合の IOS Server Load Balancing (IOS SLB) の動作を設定します。

## 自動サーバ障害検出のディセーブル化

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 ip-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	<code>enable</code>  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	<code>configure terminal</code>  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	<code>ip slb serverfarm server-farm</code>  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	<code>real ip-address [port]</code>  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。
ステップ5	<code>no faildetect inband</code>  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) <b>no faildetect inband</b> 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する場合、1 つまたは複数のプローブを設定することを強く推奨します。  <b>no faildetect inband</b> コマンドを指定する場合、 <b>faildetect numconns</b> コマンドを指定しても無視されます。

## IOS SLB のモニタおよびメンテナンス

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

## 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 で処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ている接続だけを表示します。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 Server Load Balancing (IOS SLB) の 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 Server Load Balancing (IOS SLB) のネットワーク アドレス変換 (NAT) の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 Server Load Balancing (IOS SLB) に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 Server Load Balancing (IOS SLB) に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 Server Load Balancing (IOS SLB) のレプリケーション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 Server Load Balancing (IOS SLB) に定義されている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 r6 | gtp | gtp-inspect | ipmobile | radius] [vserver virtual-server] [client ip-address netmask] [detail]`

IOS Server Load Balancing (IOS SLB) に処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 Addr/Port	Dest Addr/Port	Retry 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 Server Load Balancing (IOS SLB) サーバのネットワークアドレス変換 (NAT) の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 Server Load Balancing (IOS SLB) の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
```

**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 Server Load Balancing (IOS SLB) に定義されたスティッキー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 Server Load Balancing (IOS SLB) に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   OUTFSERVICE    0
TEST23           TCP   10.80.254.3:23   OUTFSERVICE    0
```

## 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ドキュメントについては、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。

- 「基本的な IOS SLB ネットワークの設定：例」(P.113)
- 「IOS SLB ネットワーク一式的設定：例」(P.115)
- 「ファイアウォールロードバランシングを使用する IOS SLB の設定：例」(P.116)
- 「プローブを使用する IOS SLB の設定：例」(P.124)
- 「IOS SLB によるレイヤ 3 スイッチングの設定：例」(P.127)
- 「NAT およびスタティック NAT を使用する IOS SLB の設定：例」(P.129)
- 「冗長性を使用する IOS SLB の設定：例」(P.133)
- 「スタティック ルートの再配布を使用する IOS SLB の設定：例」(P.148)
- 「WAP および UDP ロードバランシングを使用する IOS SLB の設定：例」(P.150)
- 「ルートヘルスインジェクションを使用する IOS SLB の設定：例」(P.151)
- 「GPRS ロードバランシングを使用する IOS SLB の設定：例」(P.155)
- 「VPN サーバロードバランシングを使用する IOS SLB の設定：例」(P.165)
- 「RADIUS ロードバランシングを使用する IOS SLB の設定：例」(P.166)
- 「Home Agent Director を使用する IOS SLB の設定：例」(P.175)
- 「スティッキー接続を使用する IOS SLB の設定：例」(P.175)



- 「GTP IMSI ステイッキ データベースを使用する IOS SLB の設定 : 例」 (P.176)
- 「透過的 Web キャッシュ ロードバランシングを使用する IOS SLB の設定 : 例」 (P.176)
- 「KAL-AP エージェントを使用する IOS SLB の設定 : 例」 (P.177)



(注)

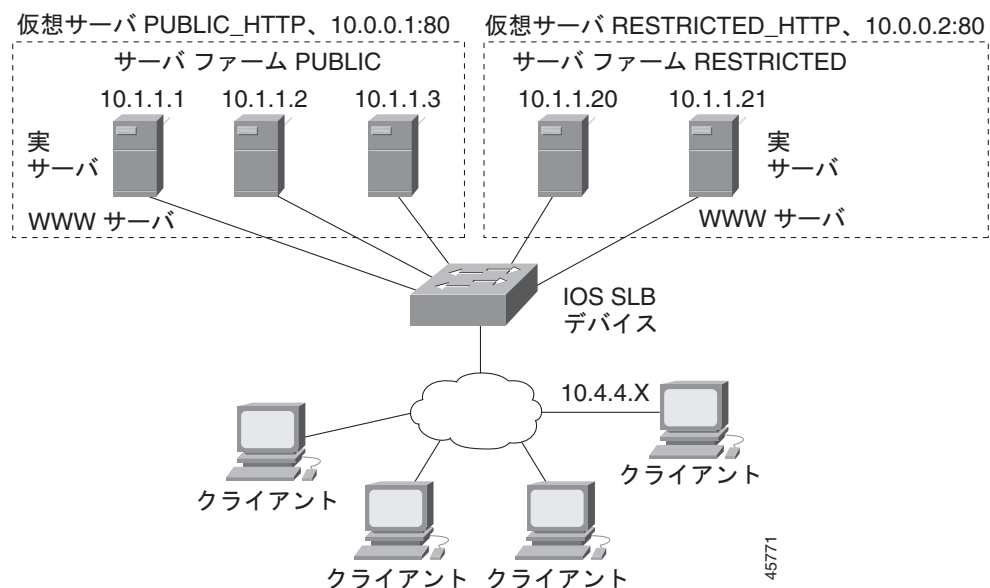
例に使用される IP アドレスおよびネットワーク アドレスは一般的なものです。実際のネットワークのアドレスで置き換えてください。

## 基本的な IOS SLB ネットワークの設定 : 例

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



45771

以下の項には、[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.114)
- 「仮想サーバの設定」(P.114)
- 「限定されたクライアントの設定」(P.115)

## 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
```

## IOS SLB ネットワークー式の設定：例

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
```

## ファイアウォール ロード バランシングを使用する IOS SLB の設定 : 例

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。

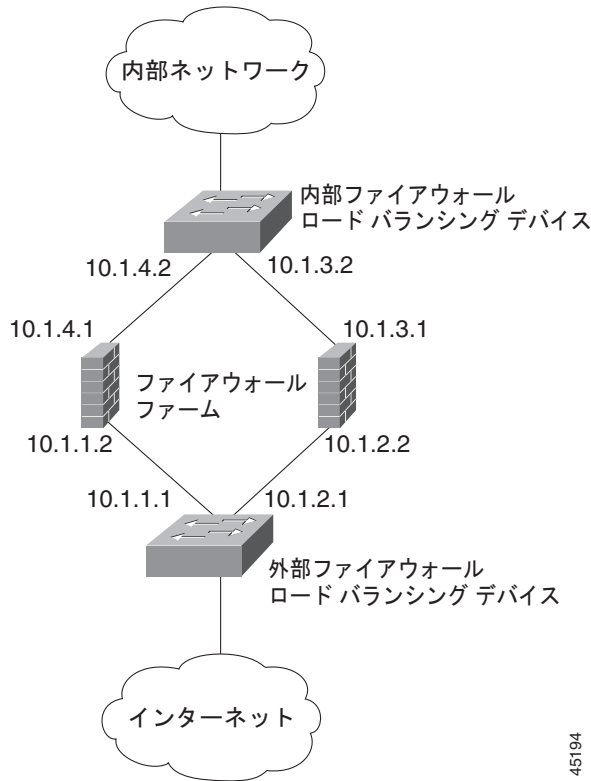
- 「基本的なファイアウォール ロード バランシングを使用する IOS SLB の設定 : 例」 (P.116)
- 「サーバロードバランシングおよびファイアウォール ロードバランシングを使用する IOS SLB の設定 : 例」 (P.118)
- 「複数のファイアウォール ファームを使用する IOS SLB の設定 : 例」 (P.120)
- 「二重ファイアウォール ロード バランシング「サンドイッチ」を使用する IOS SLB の設定 : 例」 (P.122)
- 「RADIUS ロード バランシング/ファイアウォール ロード バランシングの「サンドイッチ」を使用する IOS SLB の設定 : 例」 (P.170)

## 基本的なファイアウォール ロード バランシングを使用する IOS SLB の設定 : 例

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
- FIRE1 という 1 つのファイアウォール ファームに、両方のファイアウォールが含まれます

図 3 異なるサブネットにレイヤ 3 ファイアウォールを備えた IOS SLB



45194

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。

以下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 プロブ PROBE1、HTTP プロブ 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

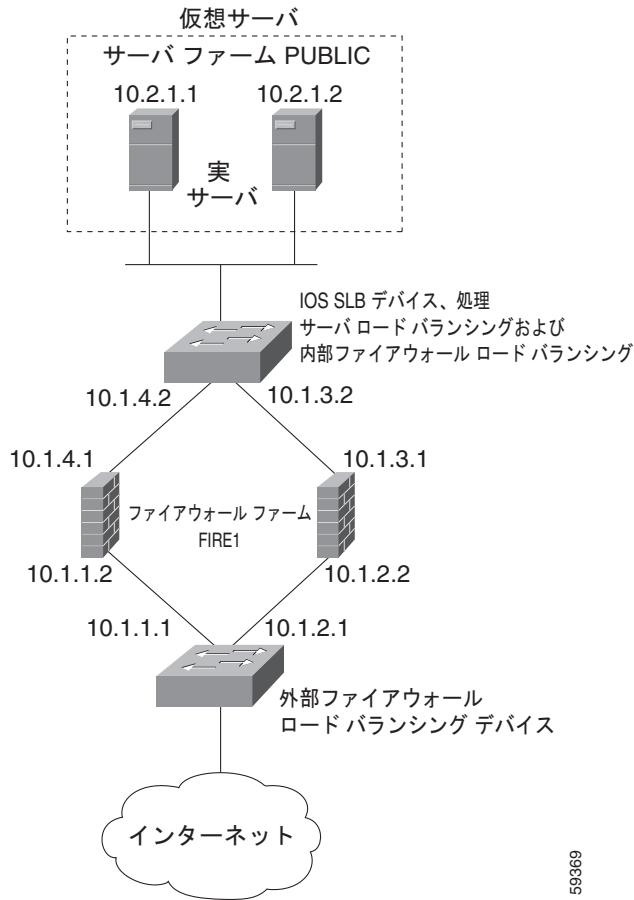
```

### 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使用する IOS SLB の設定：例

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
- PUBLIC という 1 つのサーバファームに、両方の実サーバが含まれます。
- 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
- FIRE1 という 1 つのファイアウォールファームに、両方のファイアウォールが含まれます。
- ファイアウォールのセキュア側にある内部 IOS SLB デバイスは、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します。
- 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

図 4 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使用するIOS SLB



59369

以下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)

Catalyst 6500 ファミリースイッチでは、ルートプロセッサで IOS SLB ワイルドカード検索を実行するように指定できます。この場合、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 プロンプト 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

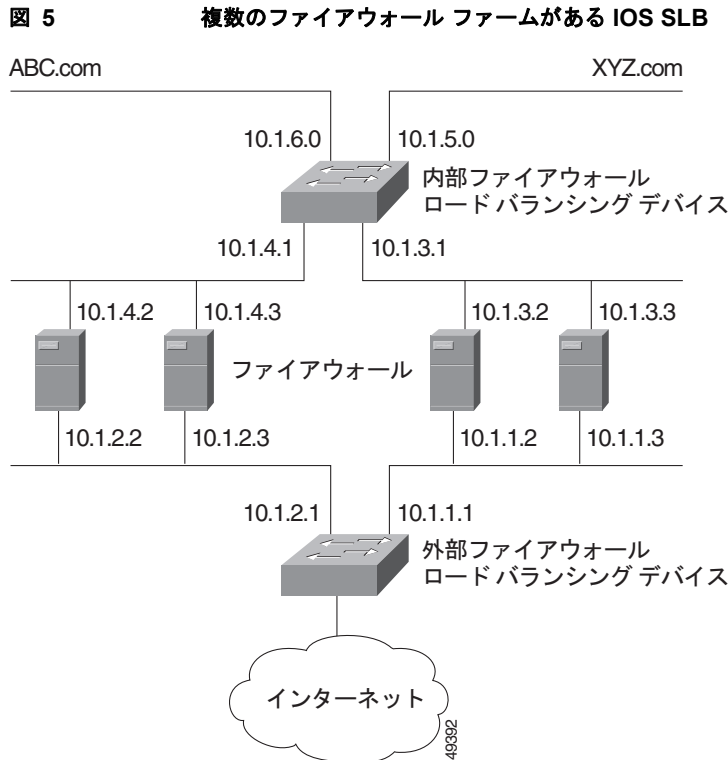
```

### 複数のファイアウォールファームを使用する IOS SLB の設定：例

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
- 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





以下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
```

## 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」を使用する IOS SLB の設定：例

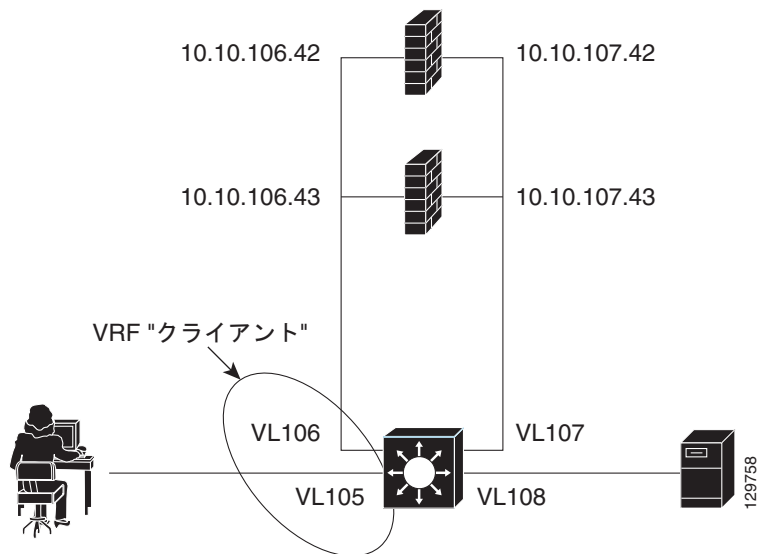
図 6 は、単一の IOS SLB デバイスでホストされる基本的な二重ファイアウォール ロードバランシング「サンドイッチ」の設定例です。Virtual Private Network (VPN) Routing and Forwarding (VRF) とアクセスインターフェイス設定を含みます。VL105、VL106、VL107、および VL108 は VLAN です。



(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」を使用する 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

```

## プローブを使用する IOS SLB の設定 : 例

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。

- 「[ping プローブおよび HTTP プローブを使用する IOS SLB の設定 : 例](#)」 (P.124)
- 「[ルーテッドプローブを使用する IOS SLB の設定 : 例](#)」 (P.126)

## ping プローブおよび HTTP プローブを使用する IOS SLB の設定 : 例

図 7 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。ping プローブおよび HTTP プローブを使用して、サーバロードバランシングを使用するアプリケーションを監視する処理を中心に説明します。

図 7 ping プロブおよび HTTP プロブ トポロジの例

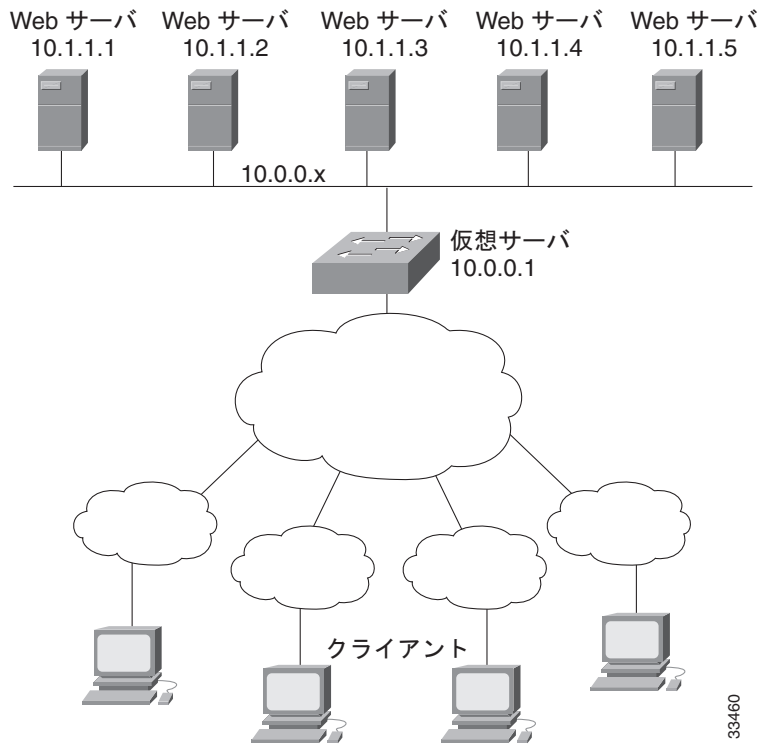


図 7 のトポロジは、単一の仮想サーバにサービスを提供する混在型サーバファームです。次に、このトポロジの設定文を示します。トポロジには、PROBE1 という ping プロブと PROBE2 という HTTP プロブがあります。

```
! 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
```

```

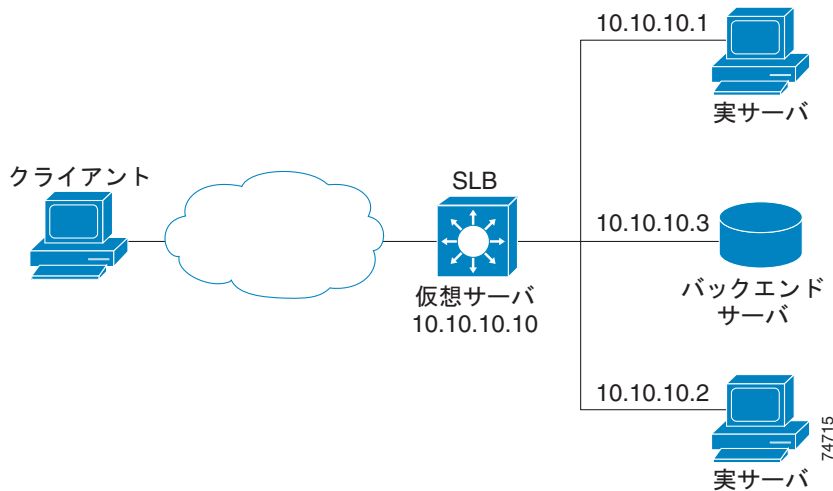
inservice
real 10.1.1.5
inservice
! Configure ping probe on the server farm
probe PROBE1
! Configure HTTP probe on the server farm
probe PROBE2
end

```

## ルーテッド プローブを使用する IOS SLB の設定 : 例

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を見なすことを希望しています。実サーバを介してヘルスチェックを送信せずにこの設定を達成するには、ルーテッド ping プローブの BACKEND をバックエンドサーバの IP アドレスに定義します。

図 8 ルーテッド ping プローブを使用する 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

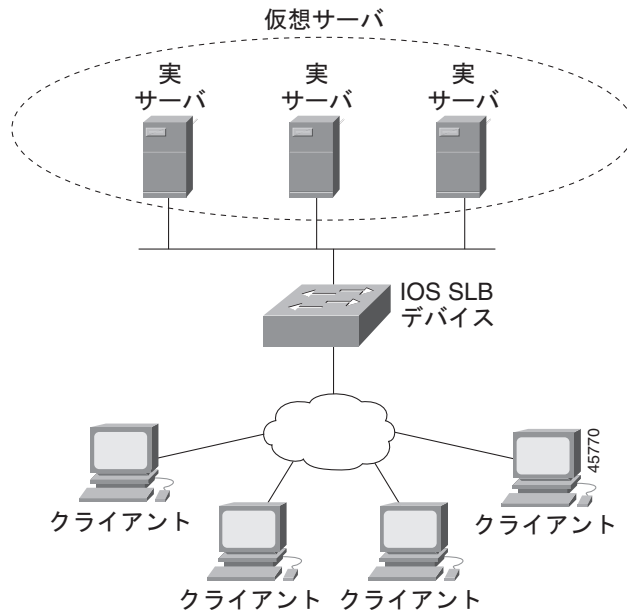
ip slb vserver ACME_VSERVER
virtual 10.10.10.10 tcp 80
serverfarm ACME_SFARM
inservice

```

## IOS SLB による レイヤ 3 スイッチングの設定 : 例

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
```

## NAT およびスタティック NAT を使用する IOS SLB の設定 : 例

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。

- 「[NAT を使用する IOS SLB の設定 : 例](#)」 (P.129)
- 「[スタティック NAT を使用する IOS SLB の設定 : 例](#)」 (P.132)
- 「[GPRS ロードバランシングおよび NAT を使用する IOS SLB の設定 : 例](#)」 (P.160)
- 「[GPRS ロードバランシング、NAT、および GTP Cause Code Inspection を使用する IOS SLB の設定 : Example](#)」 (P.163)

## NAT を使用する IOS SLB の設定 : 例

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。

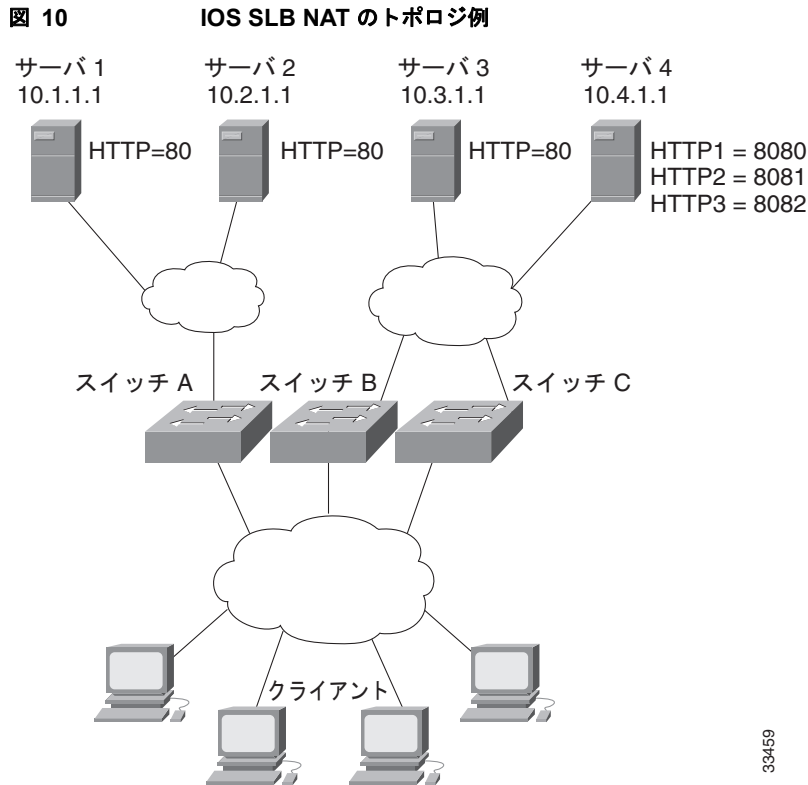


図 10 のトポロジには 4 つの Web サーバがあり、次のように設定されています。

- 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
! Handle 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
! Handle 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
! Handle HTTP (port 80) requests
virtual 128.4.0.1 tcp www
serverfarm FARM2
idle 120
delay 5
inservice

```

## スタティック NAT を使用する IOS SLB の設定 : 例

次の例では、次のアイテムの設定文を示します。

- DNS プロブの 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

```

## 冗長性を使用する IOS SLB の設定 : 例

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。

- 「ステートレス バックアップを使用する IOS SLB の設定 : 例」 (P.133)
- 「ステートフル バックアップを使用する IOS SLB の設定 : 例」 (P.142)
- 「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する IOS SLB の設定 : 例」 (P.144)
- 「アクティブ スタンバイを使用する IOS SLB の設定 : 例」 (P.145)

## ステートレス バックアップを使用する IOS SLB の設定 : 例

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 デバイスに レイヤ 2 スwitチングおよび VLAN トランキングの機能がある場合 (Catalyst 6500 ファミリー スwitチなど)、デバイスをその実サーバに直接接続できます。また、実サーバからの発信フローを処理しながら、IOS SLB のスタンバイとして動作できます。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wit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wit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wit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wit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 グループを動機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。

- 「ダイナミック ルーティングおよびトランキングの設定 : 例」 (P.133)
- 「ダイナミック ルーティングあり、トランキングなしの設定 : 例」 (P.135)
- 「スタティック ルーティングおよびトランキングの設定 : 例」 (P.137)
- 「スタティック ルーティングあり、トランキングなしの設定 : 例」 (P.139)



(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、「ステートフル バックアップを使用する IOS SLB の設定 : 例」 (P.142) を参照してください。

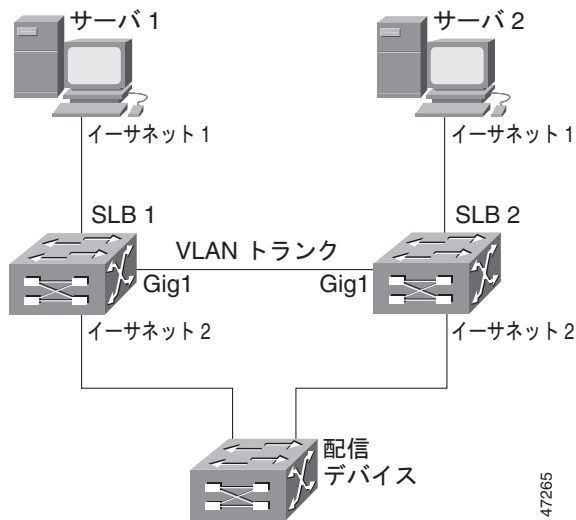
## ダイナミック ルーティングおよびトランキングの設定 : 例

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、10.10.2.1 または 10.10.3.1 (IOS SLB がアクティブな方によって変わります) を介して 10.10.14.1 に送信されるルートを認識します。

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



47265

### 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

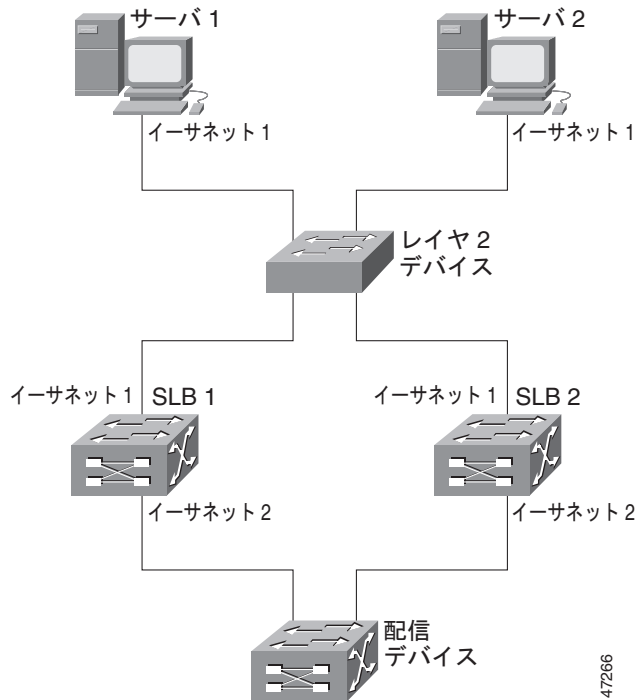
```
ip slb serverfarm SF1
  real 10.10.1.3
  reassign 2
  faildetect numconns 4
  retry 20
  inservice
  real 10.10.1.4
  reassign 2
  faildetect numconns 4
  retry 20
  inservice
ip slb vserver VS1
  virtual 10.10.14.1 tcp www
  serverfarm SF1
  idle 120
  delay 5
  inservice standby SERVER
!
interface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

### ダイナミックルーティングあり、トランキングなしの設定：例

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、10.10.2.2 または 10.10.3.2 (IOS SLB がアクティブな方によって変わります) を介して 10.10.14.1 に送信されるルートを認識します。

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



47266

## 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

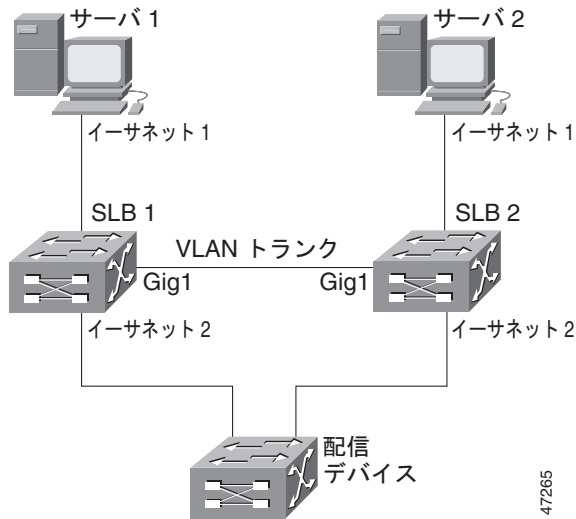
```
ip slb serverfarm SF1
  real 10.10.1.3
    reassign 2
    faildetect numconns 4
    retry 20
    inservice
  real 10.10.1.4
    reassign 2
    faildetect numconns 4
    retry 20
    inservice
ip slb vserver VS1
  virtual 10.10.14.1 tcp www
  serverfarm SF1
  idle 120
  delay 5
  inservice standby 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
```

### スタティック ルーティングおよびトランキングの設定 : 例

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



47265

## 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
```

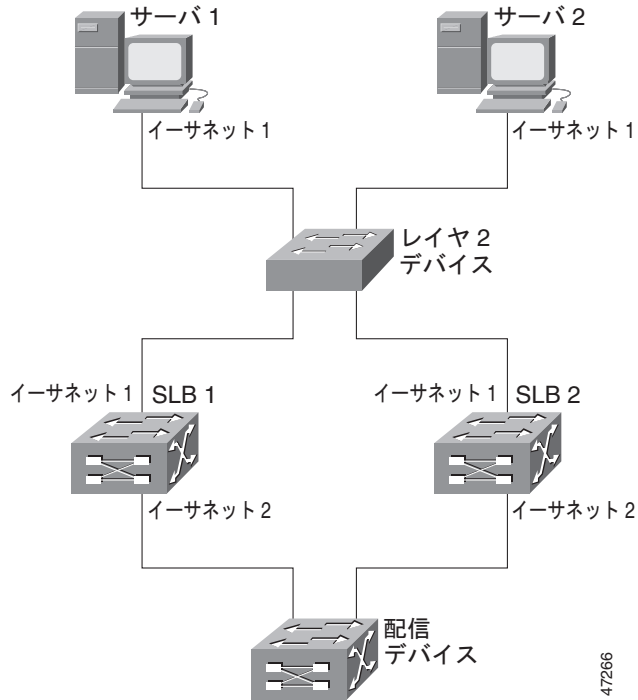
## スタティックルーティングあり、トランキングなしの設定：例

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、トランッキングなしのステートレス バックアップ



47266

### 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
```

## ステートフルバックアップを使用する IOS SLB の設定 : 例

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 はステートフルバックアップ設定の例です。クライアント側およびサーバ側の両方で HSRP を使用して、フェールオーバーを処理します。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。

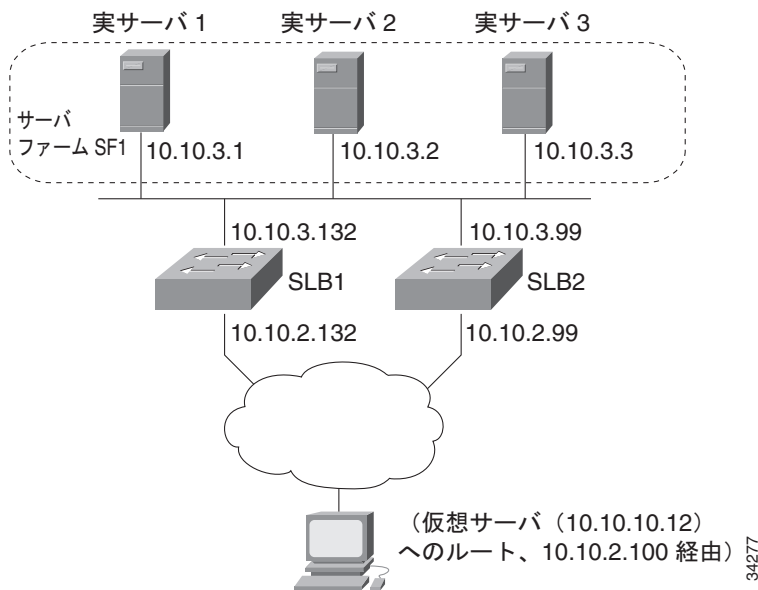
ループバックインターフェイスは、これらのメッセージ交換のために、両方のデバイスで設定されています。また、各 IOS SLB には、他のスイッチループバックアドレス宛ての二重ルートを割り当てる必要があります。この設定では、インターフェイスで障害が発生しても、レプリケーションメッセージを送信できます。



(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



34277

### 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

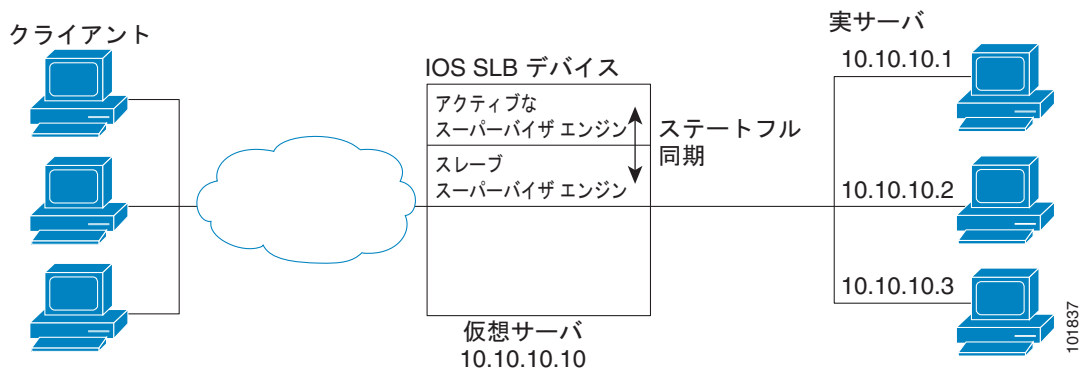
```
ip slb serverfarm SF1
  nat server
  real 10.10.3.1
  inservice
  real 10.10.3.2
  inservice
  real 10.10.3.3
  inservice
!
ip slb vserver VS1
  virtual 10.10.10.12 tcp telnet
  serverfarm SF1
  replicate casa 10.10.99.99 10.10.99.132 1024 password PASS
  inservice standby virt
!
interface loopback 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
```

## 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する IOS SLB の設定 : 例

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 同期情報が設定済みの RPR+ を介して、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 プロセッサを使用する 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
```



## アクティブスタンバイを使用する IOS SLB の設定 : 例

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。いずれかのデバイスに障害が発生すると、もう一方は通常の HSRP フェールオーバーと IOS SLB ステートレス冗長機能を介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

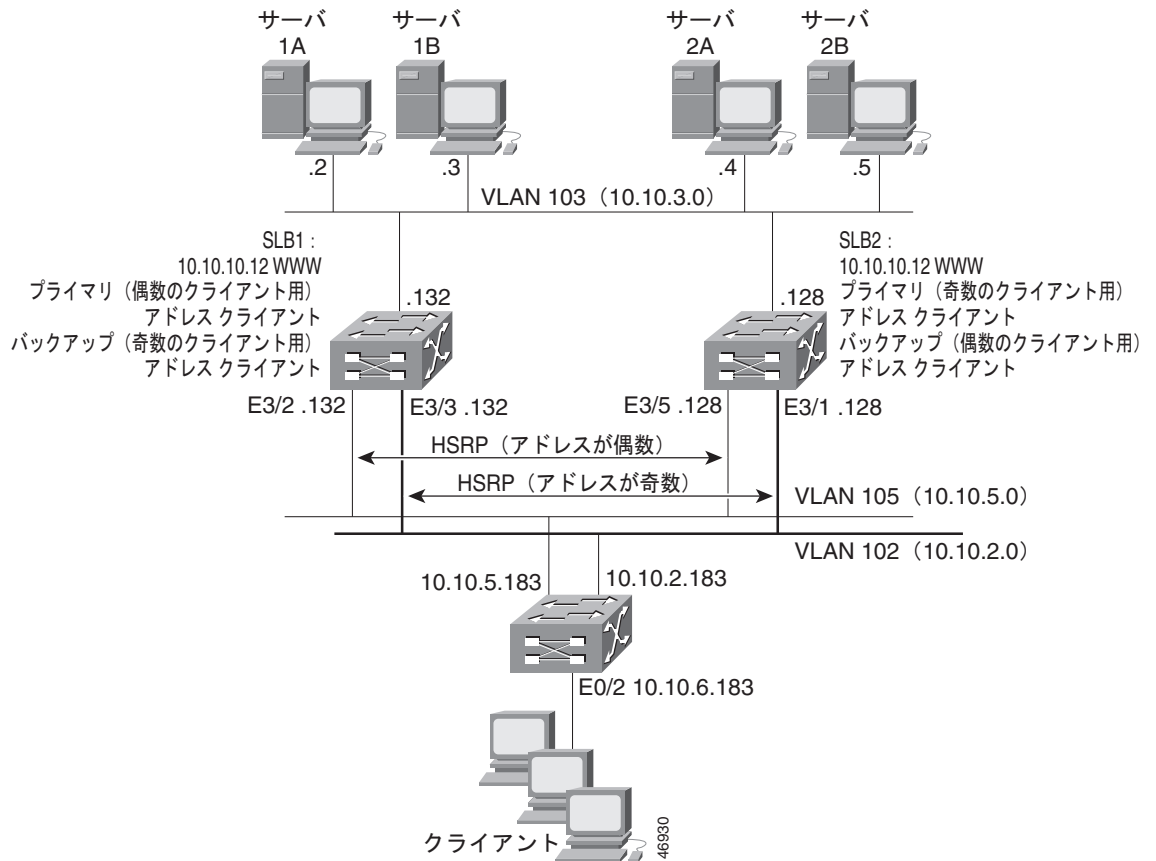


図 17 のネットワーク設定例には、次の特徴があります。

- 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。
- 単一の仮想 IP アドレス (Web の場合は 10.10.10.12) は、2 つの IOS SLB デバイス全体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 アドレスが偶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

```

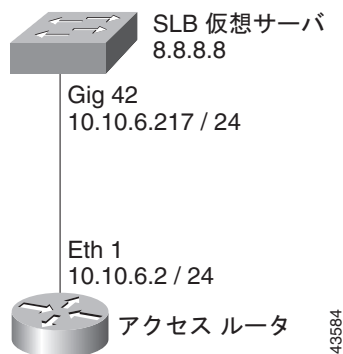
interface Ethernet0/0
 ip address 10.10.5.183 255.255.255.0
 no ip directed-broadcast
 no ip route-cache
 no ip mroute-cache
!
interface Ethernet0/1
 ip address 10.10.2.183 255.255.255.0
 no ip directed-broadcast
 no ip route-cache
 no ip mroute-cache
!
interface Ethernet0/2
 ip address 10.10.6.183 255.255.255.0
 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

```

## スタティック ルートの再配布を使用する IOS SLB の設定 : 例

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 の再配布



## 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。

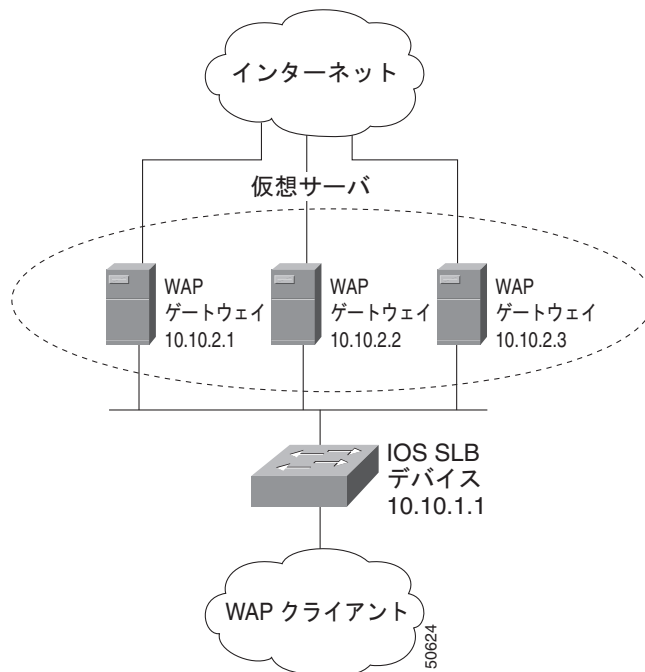
```
router eigrp 666
 network 10.0.0.0
 network 8.0.0.0
```

## WAP および UDP ロードバランシングを使用する IOS SLB の設定：例

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する 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。

## UDP ポート 9201 の WAP フローのロードバランシング

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
```

## UDP ポート 9203 の WAP フローのロードバランシング

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
```

## ルートヘルスインジェクションを使用する IOS SLB の設定 : 例

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。

- 「1 つずつ Web サーバがある 2 つの分散サイトの設定 : 例」 (P.151)
- 「2 つずつ Web サーバがある 2 つの分散サイトの設定 : 例」 (P.152)
- 「それぞれ 1 つの Web サーバと 1 つのバックアップ IOS SLB スイッチがある 2 つの分散サイトの設定 : 例」 (P.154)

### 1 つずつ Web サーバがある 2 つの分散サイトの設定 : 例

[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

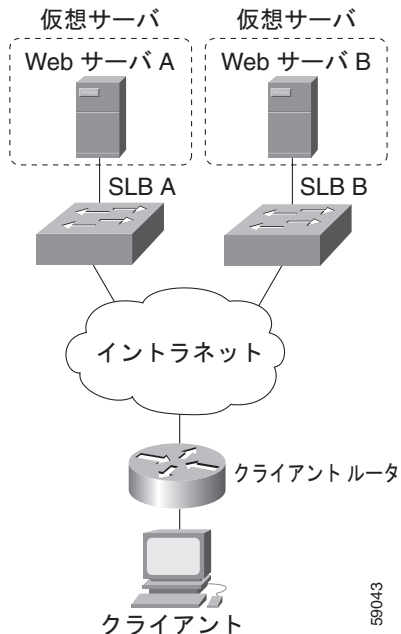


図 20 の両方の Web サーバが動作している場合、クライアントルータは、両方の IOS SLB デバイスからホストルートを受信します。

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。

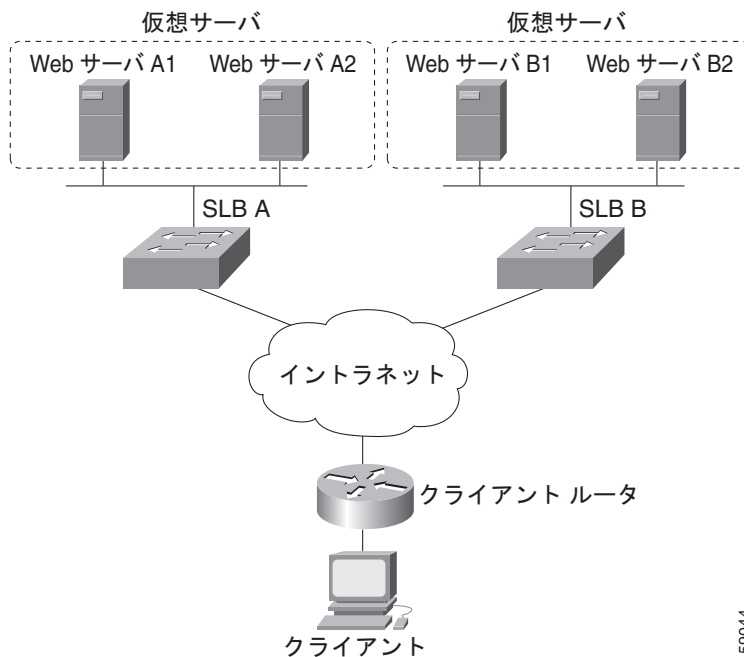
## 2 つずつ Web サーバがある 2 つの分散サイトの設定 : 例

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



59044

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。

## それぞれ 1 つの Web サーバと 1 つのバックアップ IOS SLB スイッチがある 2 つの分散サイトの設定：例

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 サーバだけを含まる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 それぞれ 1 つの Web サーバと 1 つのバックアップ IOS SLB スイッチがある 2 つの分散サイト

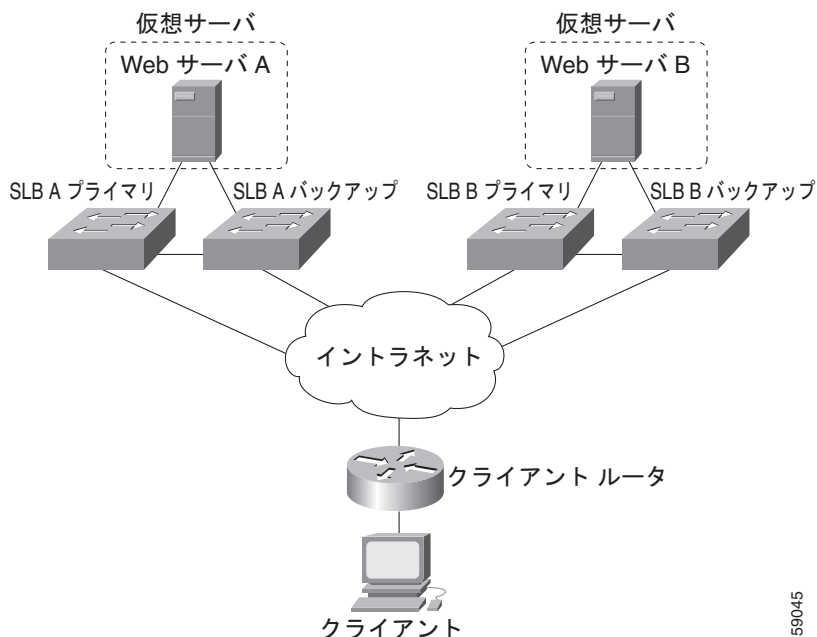


図 22 の両方の Web サーバが動作している場合、クライアントルータは、SLB A Primary および SLB B Primary の両方からホストルートを受信します。

SLB A Primary に障害が発生すると、SLB A Backup 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 Backup にも障害が発生すると、SLB A Primary および SLB A Backup 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 Primary (SLB B Primary が使用できない場合は、SLB B Backup) に対するルートの使用を開始します。

SLB A Primary または SLB A Backup 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 Primary または SLB A Backup の使用を開始します。

## GPRS ロードバランシングを使用する IOS SLB の設定：例

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。

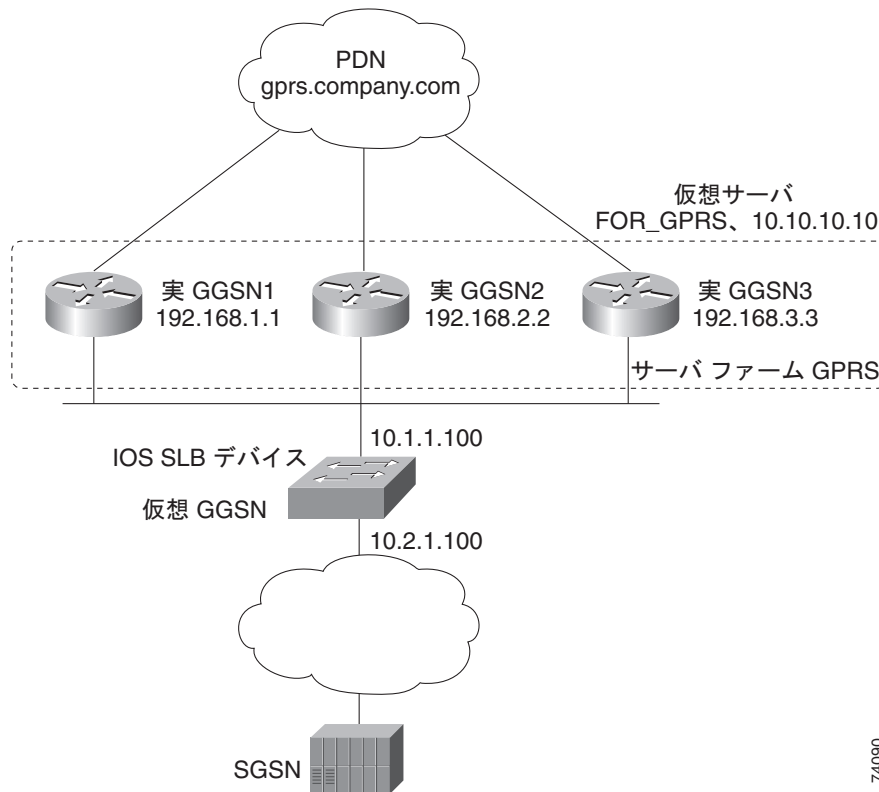
- 「GTP Cause Code Inspection なしで GPRS ロードバランシングを使用する IOS SLB の設定：例」 (P.155)
- 「GPRS ロードバランシングおよび NAT を使用する IOS SLB の設定：例」 (P.160)
- 「GPRS ロードバランシング、NAT、および GTP Cause Code Inspection を使用する IOS SLB の設定：Example」 (P.163)
- 「GPRS ロードバランシング マップを使用する IOS SLB の設定：例」 (P.164)
- 「GPRS ネットワークに RADIUS ロードバランシングを使用する IOS SLB の設定：例」 (P.166)

## GTP Cause Code Inspection なしで GPRS ロードバランシングを使用する IOS SLB の設定：例

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、複数の実 GGSN が単一の仮想 GGSN のように「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する IOS SLB



74090

次に、図 23 の設定の設定文を示します。

- 「IOS SLB の設定文」 (P.156)
- 「GGSN1 の設定文」 (P.157)
- 「GGSN2 の設定文」 (P.158)
- 「GGSN3 の設定文」 (P.159)

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-Templat1
  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
```

## GPRS ロードバランシングおよび NAT を使用する IOS SLB の設定 : 例

次の例では、図 23 のネットワークを含め、「GTP Cause Code Inspection なしで GPRS ロードバランシングを使用する IOS SLB の設定 : 例」(P.155) 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.160)
- 「GGSN1 の設定文」(P.161)
- 「GGSN2 の設定文」(P.161)
- 「GGSN3 の設定文」(P.162)

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
```

## GPRS ロードバランシング、NAT、および GTP Cause Code Inspection を使用する IOS SLB の設定 : Example

次の例では、[図 23](#) のネットワークを含め、「[GPRS ロードバランシングおよび NAT を使用する IOS SLB の設定 : 例](#)」(P.160) 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.163)
- 「[GGSN1 の設定文](#)」(P.161) (GTP Cause Code Inspection に変更はありません)
- 「[GGSN2 の設定文](#)」(P.161) (GTP Cause Code Inspection に変更はありません)
- 「[GGSN3 の設定文](#)」(P.162) (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

```

## GPRS ロードバランシングマップを使用する IOS SLB の設定 : 例

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

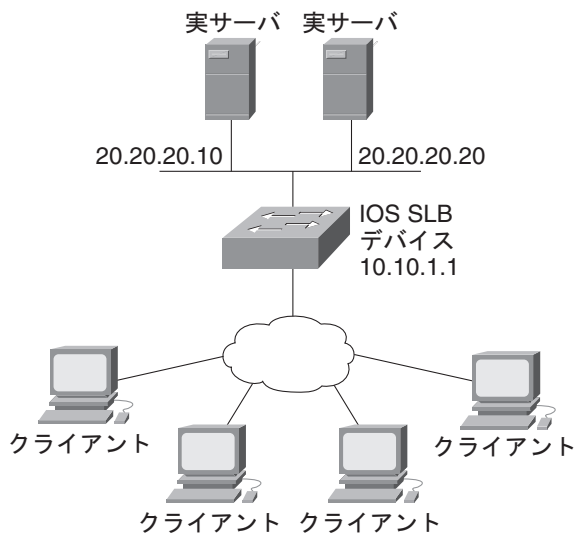
```

## VPN サーバロードバランシングを使用する IOS SLB の設定 : 例

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。
- 暗号鍵の交換は、IKE を介して発生します (ISAKMP、ポート 500)。

図 24 VPN サーバロードバランシングを使用する 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
```

## RADIUS ロード バランシングを使用する IOS SLB の設定 : 例

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。

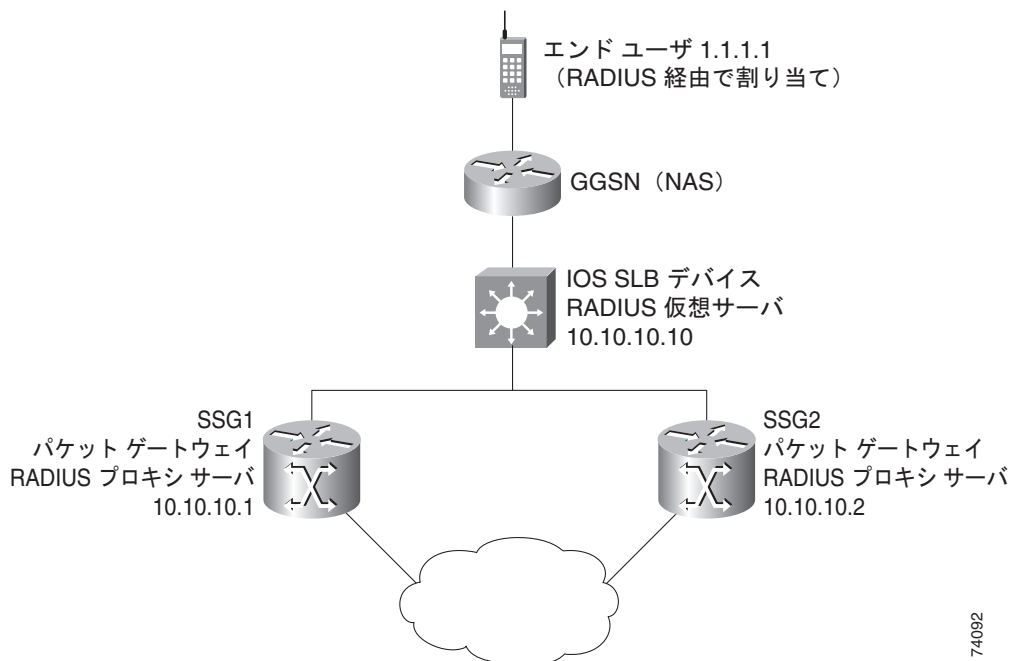
- 「[GPRS ネットワークに RADIUS ロード バランシングを使用する IOS SLB の設定 : 例](#)」 (P.166)
- 「[簡易 IP CDMA2000 ネットワークに RADIUS ロード バランシングを使用する IOS SLB の設定 : 例](#)」 (P.168)
- 「[Mobile IP CDMA2000 ネットワークに RADIUS ロード バランシングを使用する IOS SLB の設定 : 例](#)」 (P.169)
- 「[複数のサービス ゲートウェイ ファームに RADIUS ロード バランシングを使用する IOS SLB の設定 : 例](#)」 (P.170)
- 「[RADIUS ロード バランシング/ファイアウォール ロード バランシングの「サンドイッチ」を使用する IOS SLB の設定 : 例](#)」 (P.170)
- 「[RADIUS ロード バランシング マップを使用する IOS SLB の設定 : 例](#)」 (P.172)
- 「[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する IOS SLB の設定 : 例](#)」 (P.173)

## GPRS ネットワークに RADIUS ロード バランシングを使用する IOS SLB の設定 : 例

[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 ネットワークに RADIUS ロード バランシングを使用する IOS SLB



74092

次に、図 25 の設定の IOS SLB 設定文を示します。

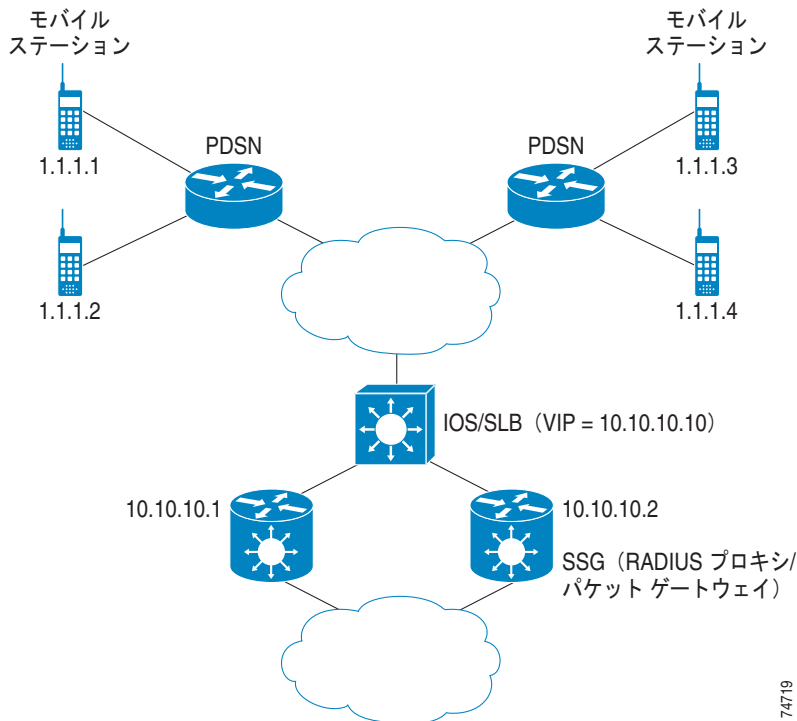
```
ip slb route 1.1.0.0 255.255.0.0 framed-ip
!
ip slb serverfarm SSGFARM
  nat server
  real 10.10.10.1
    inservice
  real 10.10.10.2
    inservice
!
ip slb vserver RADIUS_ACCT
  virtual 10.10.10.10 udp 1813 service radius
  serverfarm SSGFARM
  idle radius request 20
  idle radius framed-ip 7200
  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
```

## 簡易 IP CDMA2000 ネットワークに RADIUS ロードバランシングを使用する IOS SLB の設定：例

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 ネットワークに RADIUS ロードバランシングを使用する IOS SLB



74719

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
```

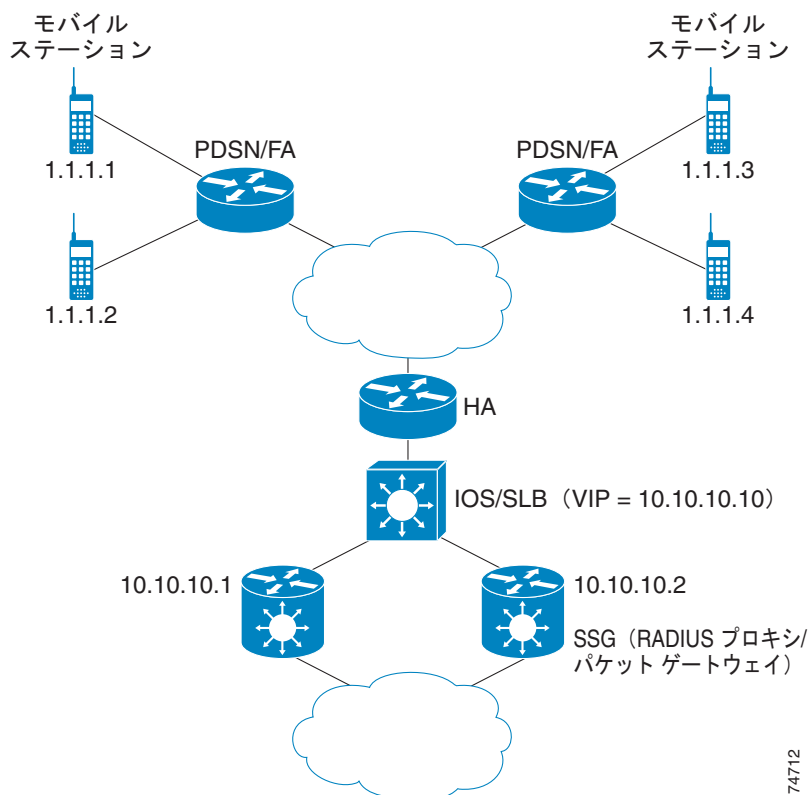


## Mobile IP CDMA2000 ネットワークに RADIUS ロードバランシングを使用する IOS SLB の設定 : 例

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 ネットワークに RADIUS ロードバランシングを使用する 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

```

## 複数のサービス ゲートウェイ ファームに RADIUS ロード バランシングを使用する IOS SLB の設定 : 例

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

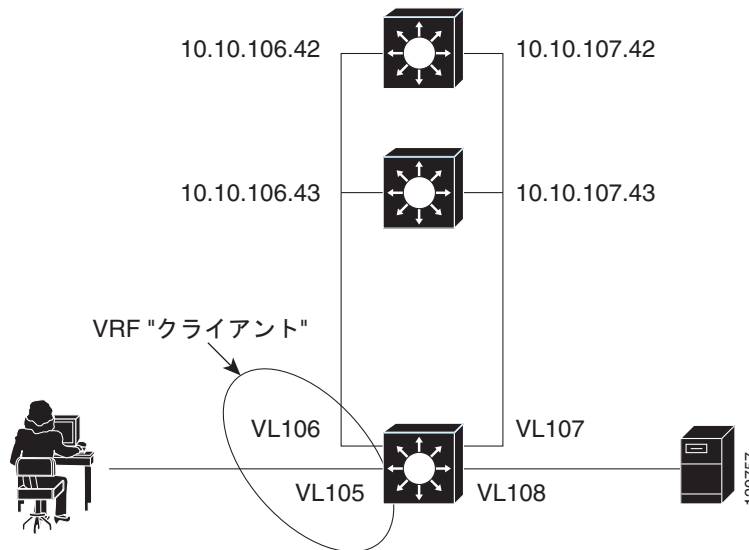
```

## RADIUS ロード バランシング/ファイアウォール ロード バランシングの「サンドイッチ」を使用する IOS SLB の設定 : 例

図 28 に、単一の 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 バランシングの「サンドイッチ」設定を示します。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。
- 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、スティッキー接続されます。
- 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の「サンドイッチ」を使用する 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

```

## RADIUS ロードバランシング マップを使用する IOS SLB の設定 : 例

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

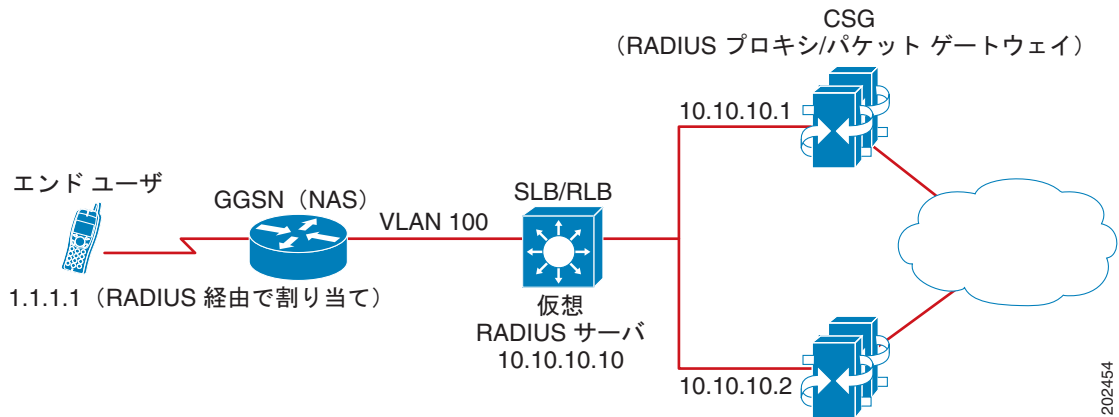
!
interface vlan 100
  ip policy route-map rlb-pbr
!
access-list 1 permit 0.0.0.1 255.255.255.254
access-list 2 permit 0.0.0.0 255.255.255.254
!
route-map rlb-pbr permit 10
  match ip address 1
  set ip next-hop 10.10.10.1
!
route-map rlb-pbr permit 20
  match ip address 2
  set ip next-hop 10.10.10.2
```

## 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する IOS SLB の設定 : 例

この IOS SLB 設定には、次の特徴があります。

- Network Access Server (NAS) デバイスを処理する IP アドレス 10.10.10.10 の仮想 RADIUS サーバがあります。
- 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する 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

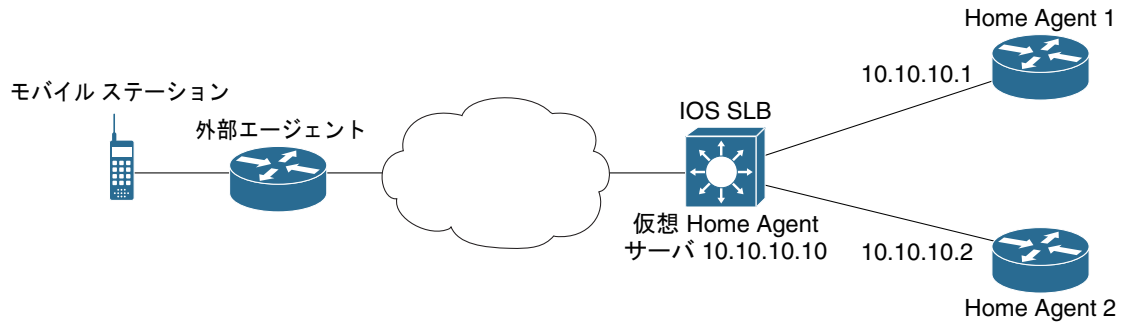
```

202454

## Home Agent Director を使用する IOS SLB の設定 : 例

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 を使用する 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
```

## スティッキ接続を使用する IOS SLB の設定 : 例

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。

## GTP IMSI スティック データベースを使用する IOS SLB の設定 : 例

次の設定例で、IOS SLB GTP IMSI スティック 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
```

## 透過的 Web キャッシュ ロードバランシングを使用する IOS SLB の設定 : 例

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。

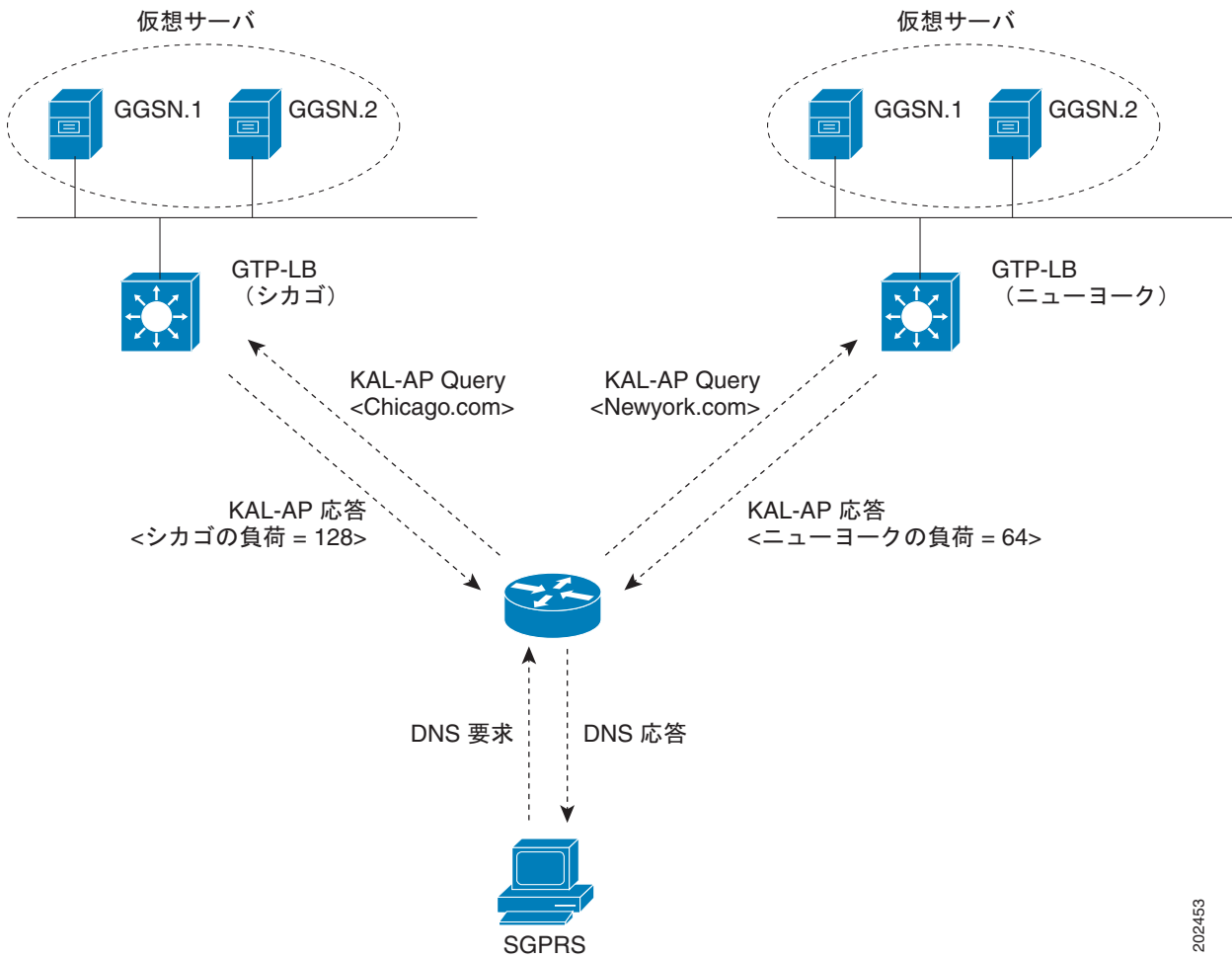
```
ip slb serverfarm WEBCACHE-FARM
  real 80.80.7.188
    inservice
  real 80.80.7.189
    inservice
ip slb vserver WEBCACHE
  virtual 0.0.0.0 0.0.0.0 tcp www
  serverfarm WEBCACHE-FARM
  client 80.80.7.0 255.255.255.0 exclude
  inservice
```



## KAL-AP エージェントを使用する IOS SLB の設定 : 例

次の設定例では、ドメイン名システム (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する 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
```

202453

```

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
```

## 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。

- [「トラブルシューティング」 \(P.180\)](#)
- [「サポートされているプラットフォーム」 \(P.182\)](#)
- [「関連資料」 \(P.182\)](#)
- [「規格」 \(P.182\)](#)
- [「MIB」 \(P.183\)](#)
- [「RFC」 \(P.183\)](#)
- [「シスコのテクニカル サポート」 \(P.184\)](#)

## 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。 <b>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 packets を入出力できません。</b>
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。	<b>numclients</b> 、 <b>numconns</b> 、および <b>delay</b> の各キーワードの値を調整します。クライアント数のごく少数の場合（たとえば、テスト環境）、 <b>numclients</b> 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、 <b>IOS SLB</b> 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、 <b>show ip slb reals detail</b> 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 スティック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。 <ol style="list-style-type: none"><li>1. スティック接続を設定します。</li><li>2. クライアント接続を開始します。</li><li>3. <b>show ip slb reals detail</b> および <b>show ip slb conns</b> コマンドを入力します。</li><li>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。</li><li>5. <b>show ip slb sticky</b> コマンドを入力して、IOS SLB に格納されているスティックの関係を表示します。</li><li>6. 接続を終了します。</li><li>7. 実サーバの接続カウントが減ることを確認します。</li><li>8. スティック タイムアウト値の間待つてから、接続を再開します。</li><li>9. もう一度 <b>show ip slb conns</b> コマンドを入力します。</li><li>10. 実サーバの接続カウントをもう一度調べて、スティック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。</li></ol>

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。	<p>次の手順を使用します。</p> <ol style="list-style-type: none"> <li>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 <b>FAILED</b> と表示されないように、<b>faildetect numconns (実サーバ)</b> コマンドで <b>numclients</b> キーワードを調整します。</li> <li>2. <b>show ip slb reals detail</b> 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。</li> <li>3. 実サーバのステータスと接続カウントを確認します。 <ul style="list-style-type: none"> <li>- 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、<b>FAILED</b>、<b>TESTING</b>、または <b>READY_TO_TEST</b> のステータスを示します。</li> <li>- 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 (<b>SYN</b> または <b>ACK</b> を受信していない) 接続は、<b>reassign</b> しきい値に達した後、最初に受信した <b>SYN</b> 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。</li> <li>- 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、低速で開始されず (詳細については、「<b>スロースタート</b>」(P.22) 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「<b>ダミー接続</b>」を示します。ダミー接続は、スロースタート期間に、<b>IOS SLB</b> 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。</li> </ul> </li> </ol>
<b>no inservice</b> 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。	<p><b>inservice</b> コマンドの <b>no</b> 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。</p> <p>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、<b>clear ip slb connections</b> コマンドを使用します。</p>
同じ Catalyst 6500 ファミリスイッチに <b>IOS SLB</b> と入力 <b>ACL</b> の両方を設定すると、「 <b>TCAM Capacity Exceeded</b> 」メッセージが表示されます。なぜですか。	<p>同じ Catalyst 6500 ファミリスイッチに <b>IOS SLB</b> と、入力 <b>ACL</b> またはファイアウォールロードバランシングを設定すると、ポリシーフィーチャカード (PFC) の <b>TCAM</b> の容量を超過する可能性があります。この問題を修正するには、<b>mls ip slb search wildcard rp</b> コマンドを使用して、<b>IOS SLB</b> が使用する <b>TCAM</b> 容量を減らします。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やや増加する可能性があります。</p>
<b>IOS SLB VRF</b> をサポートする <b>IOS</b> リリースおよびプラットフォームはどれですか。	<p><b>IOS SLB</b> の <b>Virtual Private Network (VPN) Routing and Forwarding (VRF)</b> は、Cisco 7600 シリーズルータ用の <b>MSFC3 (SUP720-MSFC3)</b> を搭載した <b>Supervisor Engine 720</b> 上の <b>IOS</b> リリース <b>12.2(18)SXE</b> 以降でサポートされます。</p>

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。	<b>replicate slave</b> を設定して単一のスーパーバイザを使用している場合、スーパーバイザで out-of-sync メッセージを受信することがあります。
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。

## 関連資料

内容	参照先
Cisco IOS コマンド	『 <a href="#">Cisco IOS Master Commands List, All Releases</a> 』
Cisco IOS 設定の基礎	『 <a href="#">Cisco IOS Configuration Fundamentals Configuration Guide</a> 』
Cisco IOS IP 設定情報	『 <a href="#">Cisco IOS IP Addressing Configuration Guide</a> 』 『 <a href="#">Cisco IOS IP Addressing Command Reference</a> 』 『 <a href="#">Cisco IOS IP Application Services Configuration Guide</a> 』 『 <a href="#">Cisco IOS IP Application Services Command Reference</a> 』
Cisco IOS モバイルワイヤレス設定情報	『 <a href="#">Cisco IOS IP Mobility Configuration Guide</a> 』 『 <a href="#">Cisco IOS IP Mobility Command Reference</a> 』
DFP 設定情報	『 <a href="#">Dynamic Feedback Protocol Support in Distributed Director</a> 』
CFM 設定情報	『 <a href="#">Using Content Flow Monitor</a> 』

## 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	<ul style="list-style-type: none"> <li>MSFC2A を搭載した Supervisor Engine 32 (SUP32-MSFC2A)</li> <li>MSFC3 を搭載した Supervisor Engine 720 (SUP720-MSFC3)</li> <li>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)</li> </ul>

## 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 <i>read-create</i> と定義されていますが、 <b>SNMP SET</b> 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、新しい値が <b>SNMP</b> で反映されます。	選択したプラットフォーム、Cisco IOS リリース、および機能セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

## RFC

RFC	タイトル
RFC 1631	「 <i>The IP Network Address Translator (NAT)</i> 」

## シスコのテクニカル サポート

説明	リンク
<p>Cisco Support Web サイトには、豊富なオンライン リソースが提供されており、それらに含まれる資料やツールを利用して、トラブルシューティングやシスコ製品およびテクノロジーに関する技術上の問題の解決に役立てることができます。</p> <p>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。</p> <ul style="list-style-type: none"> <li>• テクニカル サポートを受ける</li> <li>• ソフトウェアをダウンロードする</li> <li>• 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</li> <li>• ツールおよびリソースへアクセスする</li> <li>• Product Alert の受信登録</li> <li>• Field Notice の受信登録</li> <li>• Bug Toolkit を使用した既知の問題の検索</li> <li>• 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</li> <li>• トレーニング リソースへアクセスする</li> <li>• 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</li> </ul> <p>Japan テクニカル サポート Web サイトでは、Technical Support Web サイト (<a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a>) の、利用頻度の高いドキュメントを日本語で提供しています。Japan テクニカル サポート Web サイトには、次の URL からアクセスしてください。 <a href="http://www.cisco.com/jp/go/tac">http://www.cisco.com/jp/go/tac</a></p>	<p><a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a></p>

## 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 リリース 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。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、Cisco IOS、Cisco Catalyst OS、Cisco IOS XE ソフトウェア イメージがサポートする特定のソフトウェア リリース、機能セット、またはプラットフォームを確認できます。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 には、一連の Cisco IOS ソフトウェア リリースのうち、特定の機能が初めて導入された Cisco IOS ソフトウェア リリースだけが記載されています。特に明記していないかぎり、その機能は、一連の Cisco IOS ソフトウェア リリースの以降のリリースでもサポートされます。

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)	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。
アクティブスタンバイ	12.2(1)	<p>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。</p> <p>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。</p> <ul style="list-style-type: none"> <li>「アクティブスタンバイ」(P.29)</li> <li>「ステートレスバックアップの設定作業リスト」(P.98)</li> <li>「アクティブスタンバイを使用する IOS SLB の設定 : 例」(P.145)</li> </ul>
サーバロードバランシングのアルゴリズム	12.2(1)	<p>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。</p> <ul style="list-style-type: none"> <li>「加重ラウンドロビン」(P.11)</li> <li>「加重最小接続」(P.12)</li> <li>「ルートマップ」(P.13)</li> </ul> <p>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。</p> <ul style="list-style-type: none"> <li>「サーバロードバランシングのアルゴリズム」(P.11)</li> <li>「サーバファームおよび実サーバの設定」(P.38)</li> </ul>
代替 IP アドレス	12.2(1)	<p>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。</p> <p>この機能に関する詳細については、次の項を参照してください。</p> <ul style="list-style-type: none"> <li>「代替 IP アドレス」(P.21)</li> </ul>
オーディオおよびビデオのロードバランシング	12.2(1)	<p>IOS SLB は、RealNetworks アプリケーションを実行するサーバについて、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) を介する RealAudio および RealVideo ストリームの負荷を分散できます。</p> <p>この機能に関する詳細については、次の項を参照してください。</p> <ul style="list-style-type: none"> <li>「オーディオおよびビデオのロードバランシング」(P.28)</li> </ul>
自動サーバ障害検出	12.2(1)	<p>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。</p> <p>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。</p> <ul style="list-style-type: none"> <li>「自動サーバ障害検出」(P.23)</li> <li>「自動サーバ障害検出のディセーブル化」(P.106)</li> </ul>

表 2 IOS SLB の機能情報 (続き)

機能名	リリース	機能情報
自動アンフェイル	12.2(1)	<p>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。</p> <p>この機能に関する詳細については、次の項を参照してください。</p> <ul style="list-style-type: none"> <li>「<a href="#">自動アンフェイル</a>」(P.23)</li> </ul>
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)	<p>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。</p> <p>この機能に関する詳細については、次の項を参照してください。</p> <ul style="list-style-type: none"> <li>「<a href="#">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</a>」(P.22)</li> </ul>
バインディング ID のサポート	12.2(1)	<p>バインド ID を使用すると、単一の物理サーバを複数の仮想サーバにバインドし、それぞれについて異なる加重をレポートできます。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。</p> <p>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。</p> <ul style="list-style-type: none"> <li>「<a href="#">バインディング ID のサポート</a>」(P.13)</li> <li>「<a href="#">IOS SLB 用 Dynamic Feedback Protocol</a>」(P.24)</li> <li>「<a href="#">サーバファームおよび実サーバの設定</a>」(P.38)</li> </ul>
Client-Assigned ロードバランシング	12.2(1)	<p>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。</p> <p>この機能に関する詳細については、次の項を参照してください。</p> <ul style="list-style-type: none"> <li>「<a href="#">Client-Assigned ロードバランシング</a>」(P.13)</li> </ul>

表 2 IOS SLB の機能情報 (続き)

機能名	リリース	機能情報
クライアント NAT	12.2(1)	<p>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的ポートを使用できるため、一時的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 packets 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。</p> <p>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。</p> <ul style="list-style-type: none"> <li>「クライアント NAT」(P.18)</li> <li>「NAT の設定」(P.97)</li> <li>「NAT およびスタティック NAT を使用する IOS SLB の設定：例」(P.129)</li> </ul>
コンテンツフローモニタのサポート	12.2(1)	<p>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 ベースステータスマonitoring アプリケーションです。CFM 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。</p> <p>この機能に関する詳細については、次の項を参照してください。</p> <ul style="list-style-type: none"> <li>「コンテンツフローモニタのサポート」(P.13)</li> </ul>
TCP 接続コンテキストの遅延削除	12.2(1)	<p>IP パケットは順序どおりに到達しないため、IOS SLB の視点では、TCP 接続の終了 (finish [FIN] または reset [RST]) 後に、接続の他のパケットが到達することがあります。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達するパケットを適切にリダイレクトするために、IOS SLB は、特定の期間、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。</p> <p>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。</p> <ul style="list-style-type: none"> <li>「TCP 接続コンテキストの遅延削除」(P.14)</li> <li>「サーバファームおよび実サーバの設定」(P.38)</li> </ul>

表 2 IOS SLB の機能情報 (続き)

機能名	リリース	機能情報
IOS SLB 用 Dynamic Feedback Protocol	12.2(1)	<p>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。</p> <p>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。</p> <ul style="list-style-type: none"> <li>「IOS SLB 用 Dynamic Feedback Protocol」 (P.24)</li> <li>「DFP の設定」 (P.65)</li> <li>「GPRS ロード バランシングを使用する IOS SLB の設定 : 例」 (P.155)</li> <li>「KAL-AP エージェントを使用する IOS SLB の設定 : 例」 (P.177)</li> </ul>
ファイアウォール ロード バランシング	12.2(1)	<p>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。</p> <p>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。</p> <ul style="list-style-type: none"> <li>「ファイアウォール ロード バランシング」 (P.14)</li> <li>「ファイアウォール ロード バランシングの設定」 (P.50)</li> <li>「ファイアウォール ロード バランシングを使用する IOS SLB の設定 : 例」 (P.116)</li> </ul>
最大接続	12.2(1)	<p>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。</p> <ul style="list-style-type: none"> <li>「最大接続」 (P.16)</li> <li>「サーバ ファームおよび実サーバの設定」 (P.38)</li> <li>「ファイアウォール ファームの設定」 (P.50)</li> <li>「IOS SLB ネットワーク方式の設定 : 例」 (P.115)</li> </ul>
ポートバインド サーバ	12.2(1)	<p>仮想サーバを定義する場合、その仮想サーバで処理する TCP または UDP の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。</p> <p>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。</p> <ul style="list-style-type: none"> <li>「ポートバインド サーバ」 (P.19)</li> <li>「仮想サーバの設定」 (P.42)</li> </ul>

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 : HTTP プローブ、ping プローブ、および WSP プローブ	12.2(1)	<p>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。</p> <p>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。</p> <ul style="list-style-type: none"> <li>「プローブ」(P.25)</li> <li>「プローブの設定」(P.56)</li> <li>「プローブを使用する IOS SLB の設定 : 例」(P.124)</li> </ul>
プロトコル サポート	12.2(1)	<p>IOS SLB がサポートするプロトコルセットは固定です。</p> <p>この機能に関する詳細については、次の項を参照してください。</p> <ul style="list-style-type: none"> <li>「プロトコル サポート」(P.27)</li> </ul>
サーバ NAT	12.2(1)	<p>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。</p> <p>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。</p> <ul style="list-style-type: none"> <li>「サーバ NAT」(P.17)</li> <li>「NAT の設定」(P.97)</li> <li>「NAT およびスタティック NAT を使用する IOS SLB の設定 : 例」(P.129)</li> </ul>
スロー スタート	12.2(1)	<p>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。</p> <p>この機能に関する詳細については、次の項を参照してください。</p> <ul style="list-style-type: none"> <li>「スロー スタート」(P.22)</li> </ul>
ステートフル バックアップ	12.2(1)	<p>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。</p> <p>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。</p> <ul style="list-style-type: none"> <li>「ステートフルバックアップ」(P.29)</li> <li>「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.100)</li> <li>「ステートフルバックアップを使用する IOS SLB の設定 : 例」(P.142)</li> <li>「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する IOS SLB の設定 : 例」(P.144)</li> </ul>

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)	<p>ステートレス バックアップは、シングル レイヤ 3 スイッチの可用性に依存することなく、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で、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。</p> <p>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。</p> <ul style="list-style-type: none"> <li>「ステートレス バックアップ」 (P.29)</li> <li>「ステートレス バックアップの設定作業リスト」 (P.98)</li> <li>「ステートレス バックアップを使用する IOS SLB の設定 : 例」 (P.133)</li> </ul>
スティッキ接続	12.2(1)	<p>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 <b>sticky</b> 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。</p> <p>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。</p> <ul style="list-style-type: none"> <li>「スティッキ接続」 (P.20)</li> <li>「サーバファームおよび実サーバの設定」 (P.38)</li> <li>「仮想サーバの設定」 (P.42)</li> <li>「ファイアウォールファームの設定」 (P.50)</li> <li>「スティッキ接続を使用する IOS SLB の設定 : 例」 (P.175)</li> </ul>
サポートされているプラットフォーム	12.2(1)	<p>IOS SLB for 12.2(1) は、次のプラットフォームだけをサポートに含めました。</p> <ul style="list-style-type: none"> <li>Cisco 7200 シリーズ ルータ</li> </ul>

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)	<p>SynGuard は、仮想サーバが処理する TCP start-of-connection パケットのレート (SYNchronize Sequence Number (SYN)) を制限することで、SYN フラッド サービス拒絶攻撃と呼ばれる種類のネットワークの問題を回避します。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、仮想サーバが処理する SYN 数を特定の間隔で監視し、設定した SYN しきい値を超える数の SYN を許可しません。しきい値に達すると、新しい SYN はドロップされます。</p> <p>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。</p> <ul style="list-style-type: none"> <li>「SynGuard」(P.22)</li> <li>「仮想サーバの設定」(P.42)</li> <li>「IOS SLB ネットワーク方式の設定：例」(P.115)</li> </ul>
TCP セッションの再割り当て	12.2(1)	<p>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。</p> <p>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。</p> <ul style="list-style-type: none"> <li>「TCP セッションの再割り当て」(P.21)</li> <li>「サーバファームおよび実サーバの設定」(P.38)</li> <li>「GPRS ロードバランシングの設定作業リスト」(P.66)</li> </ul>
透過的 Web キャッシュロードバランシング	12.2(1)	<p>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。</p> <p>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。</p> <ul style="list-style-type: none"> <li>「透過的 Web キャッシュロードバランシング」(P.21)</li> <li>「仮想サーバの設定」(P.42)</li> <li>「透過的 Web キャッシュロードバランシングを使用する IOS SLB の設定：例」(P.176)</li> </ul>

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)	<p>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。</p> <p>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。</p> <ul style="list-style-type: none"> <li>「WAP ロード バランシング」 (P.36)</li> <li>「仮想サーバの設定」 (P.42)</li> <li>「WSP プローブの設定」 (P.62)</li> <li>「WAP および UDP ロード バランシングを使用する IOS SLB の設定：例」 (P.150)</li> </ul>
AAA ロード バランシング	12.2(14)S	<p>IOS SLB には、RADIUS の認証、認可、アカウントिंग (AAA) サーバ用の RADIUS ロード バランシング機能があります。</p> <p>この機能に関する詳細については、次の項を参照してください。</p> <ul style="list-style-type: none"> <li>「AAA ロード バランシング」 (P.28)</li> </ul>
バックアップ サーバファーム	12.2(14)S	<p>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。</p> <p>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。</p> <ul style="list-style-type: none"> <li>「バックアップ サーバファーム」 (P.23)</li> <li>「仮想サーバの設定」 (P.42)</li> </ul>
DFP Agent Subsystem のサポート	12.2(14)S	<p>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。</p> <p>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。</p> <ul style="list-style-type: none"> <li>「DFP Agent Subsystem のサポート」 (P.24)</li> <li>「DFP の設定」 (P.65)</li> <li>「GTP Cause Code Inspection なしで GPRS ロード バランシングを使用する IOS SLB の設定：例」 (P.155)</li> <li>「GPRS ロード バランシングおよび NAT を使用する IOS SLB の設定：例」 (P.160)</li> <li>「KAL-AP エージェントを使用する IOS SLB の設定：例」 (P.177)</li> </ul>



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 : GPRS トンネリング プロトコル (GTP) v0 のサポート	12.2(14)S	<p>IOS SLB は GTP バージョン 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 対応」になるため、IOS SLB の認識をレイヤ 5 まで拡張できます。</p> <p>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。</p> <ul style="list-style-type: none"> <li>「GPRS ロード バランシング」 (P.30)</li> <li>「仮想サーバの設定」 (P.42)</li> <li>「GPRS ロード バランシングの設定作業リスト」 (P.66)</li> <li>「GPRS ロード バランシングを使用する IOS SLB の設定 : 例」 (P.155)</li> </ul>
複数ファイアウォールファームのサポート	12.2(14)S	<p>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。</p> <p>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。</p> <ul style="list-style-type: none"> <li>「複数ファイアウォールファームのサポート」 (P.16)</li> <li>「ファイアウォールロードバランシングの設定」 (P.50)</li> <li>「複数のファイアウォールファームを使用する IOS SLB の設定 : 例」 (P.120)</li> </ul>
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	<p>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。</p> <p>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。</p> <ul style="list-style-type: none"> <li>「プローブ」 (P.25)</li> <li>「プローブの設定」 (P.56)</li> <li>「プローブを使用する IOS SLB の設定 : 例」 (P.124)</li> </ul>

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	<p>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。</p> <ul style="list-style-type: none"> <li>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。</li> <li>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。</li> </ul> <p>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。</p> <ul style="list-style-type: none"> <li>「RADIUS ロードバランシング」 (P.34)</li> <li>「RADIUS ロードバランシングの設定作業リスト」 (P.73)</li> <li>「簡易 IP CDMA2000 ネットワークに RADIUS ロードバランシングを使用する IOS SLB の設定 : 例」 (P.168)</li> <li>「Mobile IP CDMA2000 ネットワークに RADIUS ロードバランシングを使用する IOS SLB の設定 : 例」 (P.169)</li> </ul>
RADIUS ロードバランシング : グローバルパケットラジオサービス (GPRS) ネットワーク	12.2(14)S	<p>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。</p> <p>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。</p> <ul style="list-style-type: none"> <li>「RADIUS ロードバランシング」 (P.34)</li> <li>「RADIUS ロードバランシングの設定作業リスト」 (P.73)</li> <li>「GPRS ネットワークに RADIUS ロードバランシングを使用する IOS SLB の設定 : 例」 (P.166)</li> </ul>

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 : 複数のサービス ゲートウェイ サーバ ファーム	12.2(14)S	<p>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)。</p> <p>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。</p> <ul style="list-style-type: none"> <li>「RADIUS ロード バランシング」 (P.34)</li> <li>「RADIUS ロード バランシングの設定作業リスト」 (P.73)</li> <li>「複数のサービス ゲートウェイ ファームに RADIUS ロード バランシングを使用する IOS SLB の設定 : 例」 (P.170)</li> </ul>
ルート ヘルス インジェクション	12.2(14)S	<p>(<b>inservice</b> 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 アドレスは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、<b>advertise</b> 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。</p> <p>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。</p> <ul style="list-style-type: none"> <li>「ルート ヘルス インジェクション」 (P.20)</li> <li>「仮想サーバの設定」 (P.42)</li> <li>「ルート ヘルス インジェクションを使用する IOS SLB の設定 : 例」 (P.151)</li> </ul>
スタティック NAT	12.2(14)S	<p>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。</p> <p>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。</p> <ul style="list-style-type: none"> <li>「スタティック NAT」 (P.18)</li> <li>「NAT の設定」 (P.97)</li> <li>「スタティック NAT を使用する IOS SLB の設定 : 例」 (P.132)</li> </ul>
VPN サーバ ロード バランシング	12.2(14)S	<p>IOS SLB は、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できます。</p> <p>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。</p> <ul style="list-style-type: none"> <li>「VPN サーバ ロード バランシング」 (P.28)</li> <li>「VPN サーバ ロード バランシングの設定作業リスト」 (P.93)</li> <li>「VPN サーバ ロード バランシングを使用する IOS SLB の設定 : 例」 (P.165)</li> </ul>

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 および GTP v1 をサポートします。	12.2(14)ZA2	<p>IOS SLB は、GTP バージョン 0 (GTP v0) および GTP バージョン 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 対応」になるため、IOS SLB の認識をレイヤ 5 まで拡張できます。</p> <p>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。</p> <ul style="list-style-type: none"> <li>「GPRS ロードバランシング」 (P.30)</li> <li>「仮想サーバの設定」 (P.42)</li> <li>「GPRS ロードバランシングの設定作業リスト」 (P.66)</li> <li>「GPRS ロードバランシングを使用する IOS SLB の設定 : 例」 (P.155)</li> </ul>
GTP Cause Code Inspection ありの GPRS ロードバランシング	12.2(14)ZA2	<p>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 フローを監視できます。それによって、GTP 障害の原因コードを監視し、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。</p> <p>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。</p> <ul style="list-style-type: none"> <li>「GTP Cause Code Inspection ありの GPRS ロードバランシング」 (P.31)</li> <li>「GPRS ロードバランシングの設定作業リスト」 (P.66)</li> <li>「GPRS ロードバランシング、NAT、および GTP Cause Code Inspection を使用する IOS SLB の設定 : Example」 (P.163)</li> </ul>
Home Agent Director	12.2(14)ZA2	<p>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。</p> <p>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。</p> <ul style="list-style-type: none"> <li>「Home Agent Director」 (P.32)</li> <li>「Home Agent Director の設定作業リスト」 (P.95)</li> <li>「Home Agent Director を使用する IOS SLB の設定 : 例」 (P.175)</li> </ul>
プローブ : カスタム UDP プローブ	12.2(14)ZA2	<p>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。</p> <p>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。</p> <ul style="list-style-type: none"> <li>「プローブ」 (P.25)</li> <li>「プローブの設定」 (P.56)</li> <li>「プローブを使用する IOS SLB の設定 : 例」 (P.124)</li> </ul>

表 2 IOS SLB の機能情報 (続き)

機能名	リリース	機能情報
サポートされているプラットフォーム	12.2(14)ZA2	<p>IOS SLB for 12.2(14)ZA2 は、次のプラットフォームだけをサポートに含めました。</p> <ul style="list-style-type: none"> <li>• Cisco 7100 シリーズ ルータ</li> <li>• Cisco 7200 シリーズ ルータ</li> <li>• Cisco Catalyst 6500 ファミリ スイッチ用の MSFC2 搭載の Supervisor Engine 1</li> <li>• Cisco Catalyst 6500 ファミリ スイッチ用の MSFC2 搭載の Supervisor Engine 2 (SUP2-MSFC2)</li> <li>• Cisco 7600 シリーズ ルータ用の MSFC2 搭載の Supervisor Engine 1</li> <li>• Cisco 7600 シリーズ ルータ用の MSFC2 搭載の Supervisor Engine 2 (SUP2-MSFC2)</li> </ul>
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	<p>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。</p> <p>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。</p> <ul style="list-style-type: none"> <li>• 「<a href="#">自動サーバ障害検出</a>」 (P.23)</li> <li>• 「<a href="#">自動サーバ障害検出のディセーブル化</a>」 (P.106)</li> </ul>
Exchange Director 機能	12.2(14)ZA5	<p>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。</p> <p>この機能に関する詳細については、次の項を参照してください。</p> <ul style="list-style-type: none"> <li>• 「<a href="#">Exchange Director 機能</a>」 (P.29)</li> </ul>
フローの永続性	12.2(14)ZA5	<p>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。</p> <p>この機能に関する詳細については、次の項を参照してください。</p> <ul style="list-style-type: none"> <li>• 「<a href="#">フローの永続性</a>」 (P.37)</li> </ul>

表 2 IOS SLB の機能情報 (続き)

機能名	リリース	機能情報
冗長ルートプロセッサのステートフルバックアップ	12.2(14)ZA5	<p>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高可用性を維持できます。</p> <p>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。</p> <ul style="list-style-type: none"> <li>「冗長ルートプロセッサのステートフルバックアップ」(P.37)</li> <li>「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.100)</li> <li>「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する IOS SLB の設定 : 例」(P.144)</li> </ul>
—	12.2(14)ZA6	このリリースでは、小さな修正と文章の明確化を組み込みました。
サポートされているプラットフォーム	12.2(17d)SXB	<p>IOS SLB for 12.2(17d)SXB は、次のプラットフォームだけをサポートに含めました。</p> <ul style="list-style-type: none"> <li>Cisco Catalyst 6500 ファミリ スイッチ用の MSFC2 搭載の Supervisor Engine 2 (SUP2-MSFC2)</li> <li>Cisco 7600 シリーズ ルータ用の MSFC2 搭載の Supervisor Engine 2 (SUP2-MSFC2)</li> </ul>
GGSN-IOS SLB メッセージング	12.2(17d)SXB1	<p>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。</p> <p>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。</p> <ul style="list-style-type: none"> <li>「GGSN-IOS SLB メッセージング」(P.25)</li> <li>「GGSN-IOS SLB のメッセージング作業リスト」(P.68)</li> </ul>

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	<p>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 エージェントでは、CPU 使用率、プロセッサメモリ、および各ホームエージェントで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が算出されます。</p> <p>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。</p> <ul style="list-style-type: none"> <li>「IOS SLB 用 Dynamic Feedback Protocol」 (P.24)</li> <li>「DFP および Home Agent Director」 (P.25)</li> <li>「Home Agent Director」 (P.32)</li> <li>「DFP の設定」 (P.65)</li> <li>「Home Agent Director の設定作業リスト」 (P.95)</li> <li>「GPRS ロードバランシングを使用する IOS SLB の設定：例」 (P.155)</li> <li>「Home Agent Director を使用する IOS SLB の設定：例」 (P.175)</li> <li>「KAL-AP エージェントを使用する IOS SLB の設定：例」 (P.177)</li> </ul>
サポートされているプラットフォーム	12.2(17d)SXD	<p>IOS SLB for 12.2(17d)SXD は、次のプラットフォームだけをサポートに含めました。</p> <ul style="list-style-type: none"> <li>Cisco Catalyst 6500 ファミリ スイッチ用の MSFC2 搭載の Supervisor Engine 2 (SUP2-MSFC2)</li> <li>Cisco Catalyst 6500 ファミリ スイッチ用の MSFC3 搭載の Supervisor Engine 720 (SUP720-MSFC3)</li> <li>Cisco 7600 シリーズ ルータ用の MSFC2 搭載の Supervisor Engine 2 (SUP2-MSFC2)</li> <li>Cisco 7600 シリーズ ルータ用の MSFC3 搭載の Supervisor Engine 720 (SUP720-MSFC3)</li> </ul>
GTP IMSI スティックデータベース	12.2(17d)SXE	<p>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。</p> <p>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。</p> <ul style="list-style-type: none"> <li>「GTP IMSI スティックデータベース」 (P.15)</li> <li>「GTP IMSI スティックデータベースを使用する IOS SLB の設定：例」 (P.176)</li> </ul>

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	<p>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。</p> <p>このような「サンドイッチ」環境で、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対してパケットをマッピングする場合、IOS SLB では入力インターフェイスを考慮に入れる必要があります。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)。</p> <p>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。</p> <ul style="list-style-type: none"> <li>• 「<a href="#">インターフェイス認識</a>」 (P.16)</li> <li>• 「<a href="#">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」を使用する IOS SLB の設定 : 例</a>」 (P.122)</li> <li>• 「<a href="#">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の「サンドイッチ」を使用する IOS SLB の設定 : 例</a>」 (P.170)</li> </ul>
RADIUS ロードバランシング : RADIUS ロードバランシング IMSI ステイッキデータベース	12.2(17d)SXE	<p>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。</p> <p>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。</p> <ul style="list-style-type: none"> <li>• 「<a href="#">RADIUS ロードバランシング</a>」 (P.34)</li> <li>• 「<a href="#">RADIUS ロードバランシングの設定作業リスト</a>」 (P.73)</li> </ul>
—	12.2(18)SXF	このリリースでは、小さな修正と文章の明確化を組み込みました。
サポートされているプラットフォーム	12.2(17d)SXF5	<p>IOS SLB for 12.2(17d)SXF5 は、次のプラットフォームだけをサポートに含めました。</p> <ul style="list-style-type: none"> <li>• Cisco Catalyst 6500 ファミリ スイッチ用の MSFC2 搭載の Supervisor Engine 2 (SUP2-MSFC2)</li> <li>• Cisco Catalyst 6500 ファミリ スイッチ用の MSFC2A 搭載の Supervisor Engine 32 (SUP32-MSFC2A)</li> <li>• Cisco Catalyst 6500 ファミリ スイッチ用の MSFC3 搭載の Supervisor Engine 720 (SUP720-MSFC3)</li> <li>• Cisco 7600 シリーズ ルータ用の MSFC2 搭載の Supervisor Engine 2 (SUP2-MSFC2)</li> <li>• Cisco 7600 シリーズ ルータ用の MSFC2A 搭載の Supervisor Engine 32 (SUP32-MSFC2A)</li> <li>• Cisco 7600 シリーズ ルータ用の MSFC3 搭載の Supervisor Engine 720 (SUP720-MSFC3)</li> </ul>
—	12.2(18)SXF7	このリリースでは、小さな修正と文章の明確化を組み込みました。



表 2 IOS SLB の機能情報 (続き)

機能名	リリース	機能情報
サポートされているプラットフォーム	12.2(33)SRB	<p>IOS SLB for 12.2(33)SRB は、次のプラットフォームだけをサポートに含めました。</p> <ul style="list-style-type: none"> <li>• Cisco 7600 シリーズ ルータ用の MSFC2A 搭載の Supervisor Engine 32 (SUP32-MSFC2A)</li> <li>• Cisco 7600 シリーズ ルータ用の MSFC3 搭載の Supervisor Engine 720 (SUP720-MSFC3)</li> </ul>
GPRS ロードバランシング : GPRS ロードバランシング マップ	12.2(33)SRB	<p>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。</p> <p>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。</p> <ul style="list-style-type: none"> <li>• 「GPRS ロードバランシング」 (P.30)</li> <li>• 「GPRS ロードバランシング マップの設定」 (P.69)</li> <li>• 「GPRS ロードバランシング マップを使用する IOS SLB の設定 : 例」 (P.164)</li> </ul>
RADIUS ロードバランシング : RADIUS ロードバランシング マップ	12.2(33)SRB	<p>RADIUS ロードバランシング マップによって、IOS SLB は RADIUS 発信ステーション 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。</p> <p>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。</p> <ul style="list-style-type: none"> <li>• 「RADIUS ロードバランシング」 (P.34)</li> <li>• 「RADIUS ロードバランシング マップの設定」 (P.78)</li> <li>• 「RADIUS ロードバランシング マップを使用する IOS SLB の設定 : 例」 (P.172)</li> </ul>
サポートされているプラットフォーム	12.2(33)SRC	<p>IOS SLB for 12.2(33)SRC は、次のプラットフォームだけをサポートに含めました。</p> <ul style="list-style-type: none"> <li>• Cisco 7600 シリーズ ルータ用の MSFC2A 搭載の Supervisor Engine 32 (SUP32-MSFC2A)</li> <li>• Cisco 7600 シリーズ ルータ用の MSFC3 搭載の Supervisor Engine 720 (SUP720-MSFC3)</li> <li>• 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)</li> </ul>
接続のレート制限	12.2(33)SRC	<p>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。</p> <p>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。</p> <ul style="list-style-type: none"> <li>• 「接続のレート制限」 (P.13)</li> <li>• 「サーバファームおよび実サーバの設定」 (P.38)</li> </ul>

表 2 IOS SLB の機能情報 (続き)

機能名	リリース	機能情報
仮想サーバの INOP_REAL 状態	12.2(33)SRC	<p>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。</p> <ul style="list-style-type: none"> <li>仮想サーバを INOP_REAL 状態に設定します。</li> <li>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。</li> <li>仮想サーバは ICMP 要求に対する応答を停止します。</li> </ul> <p>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。</p> <ul style="list-style-type: none"> <li>「仮想サーバの INOP_REAL 状態」(P.25)</li> <li>「仮想サーバの設定」(P.42)</li> </ul>
KeepAlive Application Protocol (KAL-AP) エージェントのサポート	12.2(33)SRC	<p>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。</p> <p>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。</p> <ul style="list-style-type: none"> <li>「KeepAlive Application Protocol (KAL-AP) エージェントのサポート」(P.32)</li> <li>「KeepAlive Application Protocol (KAL-AP) エージェントのサポートの設定」(P.72)</li> <li>「KAL-AP エージェントを使用する IOS SLB の設定 : 例」(P.177)</li> </ul>
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	<p>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) は、CSG 環境でポリシーベースルーティング (PBR) ルートマップを使用し、加入者のデータプレーントラフィックを処理する高パフォーマンスの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、ペイロードが検査され、framed-IP アトリビュートが抽出され、ルートマップがその IP アドレスに適用され、加入者を処理する CSG が決定されます。</p> <p>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。</p> <ul style="list-style-type: none"> <li>「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.35)</li> <li>「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」(P.80)</li> <li>「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する IOS SLB の設定 : 例」(P.173)</li> </ul>

表 2 IOS SLB の機能情報 (続き)

機能名	リリース	機能情報
Access Service Network (ASN) R6 ロードバランシング	12.2(33)SRC1	<p>IOS SLB には、ASN ゲートウェイ セット全体のロードバランシング機能があります。ゲートウェイのクラスタは、ベースステーションから単一の ASN ゲートウェイのように見えます。</p> <p>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。</p> <ul style="list-style-type: none"> <li>「IOS SLB に関する制約事項」 (P.3)</li> <li>「ASN R6 ロードバランシング」 (P.30)</li> <li>「ASN R6 ロードバランシングの設定作業リスト」 (P.95)</li> </ul> <p>この機能によって、次のコマンドが変更されました。</p> <p><b>debug ip slb、idle (仮想サーバ)、show ip slb sessions、show ip slb stats、show ip slb vservers、virtual</b></p>
Access Service Network (ASN) R6 ロードバランシング ステートフルおよびスティッキのサポート	12.2(33)SRE	<p>Access Service Network (ASN) R6 ロードバランシングは、ステートフル冗長性およびスティッキ接続をサポートします。</p>
ファイアウォール ロードバランシングのパフォーマンス改善	12.2(33)SRE	<p>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。</p> <p>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。</p> <ul style="list-style-type: none"> <li>「ファイアウォール ロードバランシングの設定」 (P.50)</li> <li>「MLS エントリのプロトコルレベル消去の設定」 (P.92)</li> <li>「接続の消去要求動作の設定」 (P.92)</li> <li>「スティッキ接続の消去要求動作の設定」 (P.92)</li> </ul> <p>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。</p> <p><b>purge connection、purge sticky</b></p> <p>この機能により次のコマンドが変更されました。</p> <p><b>access (ファイアウォール ファーム)</b></p>
GPRS ロードバランシング : GPRS トンネリング プロトコル (GTP) v2 のサポート	12.2(33)SRE	<p>IOS SLB は GTP バージョン 2 (GTP v2) をサポートします。</p>
Sub-Interface のサポート	12.2(33)SRE	<p>IOS SLB は、<b>access</b> 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。</p> <p>この機能によって、次のコマンドが変更されました。</p> <p><b>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)</b></p>

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLYNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0910R)

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアル内の例、コマンド出力、ネットワーク トポロジ図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際のアドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

© 2009 Cisco Systems, Inc.  
All rights reserved.

Copyright © 2009–2010, シスコシステムズ合同会社 .  
All rights reserved.