IP アプリケーション サービス コンフィギュレーション ガイド Cisco IOS Release 15.1S

IP Application Services Configuration Guide Cisco IOS Release 15.1S

【注意】シスコ製品をご使用になる前に、安全上の注意（www.cisco.com/jp/go/safety_warning/）をご確認ください。

本書は、米国シスコシステムズ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動 / 変更されている場合がありますことをご了承ください。
あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。

また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

IP アプリケーション サービス コンフィギュレーション ガイド、*Cisco IOS Release 15.1S*

Cisco IOS IP アプリケーション サービス機能ロードマップ

この機能ロードマップでは、『*Cisco IOS IP アプリケーション サービス コンフィギュレーション ガイド*』に記載された Cisco IOS 機能を一覧にし、各機能の説明が記載された参照先を示します。ロードマップは、お使いのリリースで使用できる機能を参照できるように編成されています。目的の機能名を探して、「参照先」列の URL をクリックすると、その機能の説明が記載された参照先にアクセスできます。

以前使用されていた機能の多くは、コンフィギュレーション ファイルに組み込まれています。このロードマップでは、これらについては記載していない機能もあります。このロードマップ情報は、他のソフトウェア リリースやプラットフォームについてもサポートします。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。

（注） この機能ロードマップには、First Hop Redundancy Protocol（FHRP; ファーストホップ冗長プロトコル）で説明している機能は含まれていません。FHRP 機能については、『FHRP Features Roadmap』を参照してください。

機能とリリース サポート

表 1 に、次の Cisco IOS ソフトウェア リリースでサポートする IP アプリケーション サービス機能の一覧を示します。

- 「Cisco IOS Release 15.0S」
- 「Cisco IOS XE Release 15.0」
- 「Cisco IOS Release 12.2S」
- 「Cisco IOS Release 12.2SB」
- 「Cisco IOS Release 12.2SR」
- 「Cisco IOS Release 12.2SX」
- 「Cisco IOS Release 12.2T、12.3、12.3T、12.4、および 12.4T」
- 「Cisco IOS Release 12.2」
- 「Cisco IOS XE 3.1.0SG」
- 「その他の Cisco IOS リリース」

プラットフォーム サポートとソフトウェア イメージ サポートに関する情報を入手するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator を使用すると、Cisco IOS、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 1 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 1 に、各ソフトウェアの最新リリースの一覧を示します。また、対象のリリースで使用可能な機能をアルファベット順に紹介します。

表 1　サポートされる IP アプリケーション サービス機能

リリース	機能名	機能の説明	参照先
Cisco IOS Release 15.0S			
15.0(1)S	IP Precedence Accounting	IP Precedence Accounting 機能により、インターフェイス上の優先順位に基づいて IP トラフィックのアカウンティング情報が提供されます。この機能は、IP パケットを送受信したインターフェイスごとにパケット数の合計とバイト数の合計を計算し、IP 優先順位に基づいて結果をソートします。この機能はすべてのインターフェイスおよびサブインターフェイスでサポートされ、CEF、dCEF、フロー、および最適なスイッチングをサポートします。	*Configuring IP Services*
	SLB（サーバ ロード バランシング）	Cisco IOS SLB 機能は、さまざまなネットワーク デバイスおよびサービスにロード バランシングを提供する Cisco IOS ベースのソリューションです。	*Configuring Server Load Balancing*
	SLB：Access Service Network（ASN）R6 ロード バランシング	Cisco IOS SLB は、ASN ゲートウェイ セット全体にロード バランシングを提供します。ゲートウェイのクラスタは、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。	*Configuring Server Load Balancing*
	SLB：アクティブ スタンバイ	アクティブ スタンバイを使用すれば、2 つの Cisco IOS SLB が、同じ仮想 IP アドレスを負荷分散しながら、相互にバックアップとして機能することができます。	*Configuring Server Load Balancing*
	SLB：代替 IP アドレス	Cisco IOS SLB を使用すれば、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 できます。	*Configuring Server Load Balancing*
	SLB：自動サーバ障害検出	Cisco IOS SLB は、失敗した実サーバへの TCP 接続の試みを自動的に検出し、そのサーバの障害カウンタをインクリメントします。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。	*Configuring Server Load Balancing*

表 1　サポートされる IP アプリケーション サービス機能 （続き）

リリース	機能名	機能の説明	参照先
	SLB：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。タイマーがタイムアウトすると、再び、そのサーバに新しい仮想サーバ接続の資格が与えられ、Cisco 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。	*Configuring Server Load Balancing*
	SLB：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。	*Configuring Server Load Balancing*
	SLB：バインド 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。	*Configuring Server Load Balancing*
	SLB：BWG スティッキのサポート	Cisco IOS SLB は、すべてのバージョンの GTP（v0、v1、v2）に対して sticky-only をサポートします。	*Configuring Server Load Balancing*
	SLB：コンテンツ フロー モニタのサポート	Cisco 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。	*Configuring Server Load Balancing*

表 1　サポートされる IP アプリケーション サービス機能 （続き）

リリース	機能名	機能の説明	参照先
	SLB：TCP 接続コンテキストの遅延削除	IP パケットの順序異常が原因で、Cisco IOS SLB が、TCP 接続の終了（finish [FIN] または reset [RST]）後に、接続用の他のパケットが続いているのを検出する場合があります。一般的に、この問題は TCP 接続パケットがたどるパスが複数あるときに発生します。接続が終了した後に到着するパケットを適切にリダイレクトするために、Cisco IOS SLB が、指定された期間、TCP 接続情報（つまり、コンテキスト）を保持します。接続の終了後にコンテキストを保持する期間は、設定可能な遅延タイマーで制御されます。	*Configuring Server Load Balancing*
	SLB：DFP Agent Subsystem のサポート	Cisco 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る）をサポートします。そのため、Cisco 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機能することができます。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。	*Configuring Server Load Balancing*
	SLB：GTP ロード バランシングに対するデュアルスタックのサポート	IPv6 のサポートによって、Cisco IOS SLB は、GTP のすべてのバージョン（v0、v1、v2）に対して、GTP ロード バランシング用の IPv6 アドレスを管理することができます。 デュアルスタックのサポートによって、Cisco IOS SLB は、GTP ロード バランシング用のデュアルスタック実装を管理することができます。デュアルスタック実装とは、IPv4 アドレスと IPv6 アドレスの両方を使用する実装です。	*Configuring Server Load Balancing*
	SLB：Dynamic Feedback Protocol（DFP; ダイナミック フィードバック プロトコル）	Cisco 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る）をサポートします。そのため、Cisco 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機能することができます。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。	*Configuring Server Load Balancing*
	SLB：ファイアウォール ロード バランシング	Cisco IOS SLB ファイアウォール ロード バランシングを使用すれば、CPU の使用率が高くなる可能性のある特定の状態を回避できます。	*Configuring Server Load Balancing*

表 1　サポートされる IP アプリケーション サービス機能 （続き）

リリース	機能名	機能の説明	参照先
	SLB：GPRS ロード バランシング	GPRS は、European Telecommunications Standards Institute（ETSI）Global System for Mobile Communication（GSM）フェーズ 2+ 標準に基づくパケット ネットワーク インフラストラクチャです。GSM モバイル ユーザからのパケット データを Packet Data Network（PDN）に転送するために使用されます。Cisco Gateway GPRS Support Node（GGSN; ゲートウェイ GPRS サポート ノード）は、GTP を使用して Serving GPRS Support Node（SGSN）とインターフェイスします。トランスポートには UDP が使用されます。Cisco IOS SLB は、GGSN に対して、GPRS ロード バランシングを提供し、信頼性と可用性を向上させます。	*Configuring Server Load Balancing*
	SLB：GTPV2 ロード バランシング	Cisco IOS SLB は、GTP version 2（GTP v2）をサポートします。	*Configuring Server Load Balancing*
	SLB：Hot ICE 準拠	すべての Cisco IOS SLB コマンドが Hot ICE 準拠です。Hot ICE は、Cisco IOS 設定管理の運用堅牢性、スケーラビリティ、およびプログラム可能性を向上させるように設計された Cisco IOS 設定機能強化のセットです。	*Configuring Server Load Balancing*
	SLB：KeepAlive Application Protocol（KAL-AP）エージェントのサポート	KAL-AP エージェントのサポートを使用すれば、Cisco IOS SLB を通して、Global Server Load Balancing（GSLB; グローバル サーバ ロード バランシング）環境でロード バランシングを実行することができます。	*Configuring Server Load Balancing*
	SLB：最大接続数	Cisco IOS SLB を使用すれば、サーバとファイアウォールのロード バランシング用の最大接続数を設定できます。	*Configuring Server Load Balancing*
	SLB：複数ファイアウォール ファームのサポート	SLB：複数ファイアウォール ファームのサポート機能を使用すれば、ロード バランシング デバイスごとに複数のファイアウォール ファームを設定できます。	*Configuring Server Load Balancing*
	SLB：ping プローブ	Cisco IOS SLB プローブは、サーバ ファーム内の実サーバごとのステータスと、ファイアウォール ファーム内のファイアウォールごとのステータスを判断します。	*Configuring Server Load Balancing*
	SLB：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。	*Configuring Server Load Balancing*
	SLB：プローブ	Cisco IOS SLB プローブは、サーバ ファーム内の実サーバごとのステータスと、ファイアウォール ファーム内のファイアウォールごとのステータスを判断します。	*Configuring Server Load Balancing*

表 1　サポートされる IP アプリケーション サービス機能 （続き）

リリース	機能名	機能の説明	参照先
	SLB：プロトコル サポート	Cisco IOS SLB は、固定のプロトコル セットをサポートします。	*Configuring Server Load Balancing*
	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	RADIUS ロード バランシング加速データ プレーン フォワーディング（Turbo RADIUS ロード バランシングとも呼ばれる）は、CSG 環境で基本的な Policy-Based Routing（PBR; ポリシーベース ルーティング）ルート マップを使用して加入者のデータプレーン トラフィックを管理する高性能ソリューションです。	*Configuring Server Load Balancing*
	SLB：RADIUS ロード バランシング	Cisco IOS SLB は、RADIUS ロード バランシングをサポートします。	*Configuring Server Load Balancing*
	SLB：ルート ヘルス インジェクション	（**inservice** コマンドを使用して）仮想サーバをサービスに登録すると、デフォルトで、仮想サーバの IP アドレスがアドバタイズされます（ルーティング テーブルに追加されます）。Web サイトの仮想 IP アドレスに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、**advertise** コマンドを使用して、IP アドレスの可用性が Cisco IOS SLB で確認された場合にだけ、ホスト ルートをアドバタイズするように、Cisco IOS SLB を設定することができます。IP アドレスを使用できなくなると、Cisco IOS SLB が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。	*Configuring Server Load Balancing*
	SLB：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。	*Configuring Server Load Balancing*
	SLB：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 スタート機能によって、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。	*Configuring Server Load Balancing*
	SLB：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れば、Cisco IOS SLB で、ロード バランシングの決定を段階的にバックアップしたり、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」したりすることができます。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。	*Configuring Server Load Balancing*

表 1　サポートされる IP アプリケーション サービス機能 （続き）

リリース	機能名	機能の説明	参照先
	SLB：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場合は特に、ステートレス バックアップが有効です。	*Configuring Server Load Balancing*
	SLB：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。	*Configuring Server Load Balancing*
	SLB：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。オプションの **sticky** コマンドを使用すれば、Cisco IOS SLB で、同じクライアントから、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することができます。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。	*Configuring Server Load Balancing*
	SLB：サブインターフェイスのサポート	Cisco IOS SLB は、**access** コマンドに対して、サブインターフェイスのサポートを提供しています。	*Configuring Server Load Balancing*
	SLB：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 は、Cisco IOS SLB または実サーバをダウンさせるこのような攻撃を阻止します。SynGuard は、仮想サーバが処理する SYN 数を特定の間隔でモニタし、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。	*Configuring Server Load Balancing*
	SLB：TCP プローブ	Cisco IOS SLB プローブは、サーバ ファーム内の実サーバごとのステータスと、ファイアウォール ファーム内のファイアウォールごとのステータスを判断します。	*Configuring Server Load Balancing*

表 1　サポートされる IP アプリケーション サービス機能 （続き）

リリース	機能名	機能の説明	参照先
	SLB：TCP セッション再割り当て	Cisco IOS SLB は、新しい接続を開くためにクライアントから実サーバに送信された TCP SYN を追跡します。複数の連続する SYN に応答がない場合、または SYN が RST で応答される場合、TCP セッションは新しい実サーバに再割り当てされます。SYN の試行回数は、設定可能な再割り当てしきい値で制御されます。	*Configuring Server Load Balancing*
	SLB：VPN サーバ ロード バランシング	Cisco IOS SLB は VPN フローのバランスを取ることができます。	*Configuring Server Load Balancing*
	SLB：WAP ゲートウェイ ロード バランシング	Wireless Application Protocol（WAP; ワイヤレス アプリケーション プロトコル）ロード バランシング機能を使用すれば、Cisco IOS SLB を使用して、IP ベアラ ネットワーク上の WAP ゲートウェイまたはサーバのグループ内で、Wireless Session Protocol（WSP）セッションを負荷分散させることができます。	*Configuring Server Load Balancing*
	SLB：WebCache ロード バランシング	Cisco IOS SLB は、透過的 Web キャッシュのクラスタ全体で HTTP フローを負荷分散させることができます。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。	*Configuring Server Load Balancing*
	SLB：加重最小接続	Cisco IOS SLB は、加重ラウンド ロビン、加重最小接続、およびルート マップ ロード バランシング アルゴリズムを提供します。加重最小接続アルゴリズムは、サーバ ファームから選択された次の実サーバがアクティブ接続の最も少ないサーバになるように指定します。	*Configuring Server Load Balancing*
	SLB：加重ラウンド ロビン	Cisco IOS SLB は、加重ラウンド ロビン、加重最小接続、およびルート マップ ロード バランシング アルゴリズムを提供します。 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。	*Configuring Server Load Balancing*
	SLB：WSP プローブ	Cisco IOS SLB プローブは、サーバ ファーム内の実サーバごとのステータスと、ファイアウォール ファーム内のファイアウォールごとのステータスを判断します。	*Configuring Server Load Balancing*
	TCP MSS 調整	TCP MSS 調整機能では、ルータを通過する一時的なパケット（特に SYN ビットが設定された TCP セグメント）の Maximum Segment Size（MSS; 最大セグメント サイズ）を設定することができるようになります。	*Configuring TCP*

表 1　サポートされる IP アプリケーション サービス機能 （続き）

リリース	機能名	機能の説明	参照先
	受信インターフェイスでの WCCP のリダイレクション	受信インターフェイスでの WCCP のリダイレクション機能によって、特定の WCCP サービスのために入力リダイレクションのインターフェイスを設定できます。インターフェイスでこの機能をイネーブルにすると、そのインターフェイスに到達するすべてのパケットは、指定した WCCP サービスに対して比較されます。パケットが一致する場合、そのパケットはリダイレクトされます。	*Configuring WCCP*
	WCCP バージョン 1	WCCP は、シスコが開発したコンテンツルーティング テクノロジーです。IP パケットを代行受信して、パケットに指定された宛先とは別の宛先にパケットをリダイレクトします。	*Configuring WCCP*
	WCCP バージョン 2	WCCP バージョン 2 のいくつかの機能が強化され、WCCP プロトコルに機能が追加されました。	*Configuring WCCP*
Cisco IOS XE Release 15.0			
15.0(1)M	WCCP VRF のサポート	WCCP VRF のサポート機能によって、VRF の認識をサポートする既存の WCCPv2 プロトコルが強化されています。	*Configuring WCCP*
Cisco IOS Release 12.2S			
12.2(25)S	IP Precedence Accounting	IP Precedence Accounting 機能により、インターフェイス上の優先順位に基づいて IP トラフィックのアカウンティング情報が提供されます。この機能は、IP パケットを送受信したインターフェイスごとにパケット数の合計とバイト数の合計を計算し、IP 優先順位に基づいて結果をソートします。この機能はすべてのインターフェイスおよびサブインターフェイスでサポートされ、CEF、dCEF、フロー、および最適なスイッチングをサポートします。	*Configuring IP Services*
	WCCP バイパス カウンタ	WCCP バイパス カウンタ機能を使用すると、Web キャッシュによってバイパスされ、元のルータに返送され、通常どおりに転送されたパケットのカウントを表示できます。	*Configuring WCCP*
	WCCP 発信 ACL チェック	WCCP 発信 ACL チェック機能を使用すると、入力インターフェイスで WCCP によってリダイレクトされるトラフィックが、必ず発信 ACL チェックを受けるようにできます。これは、リダイレクト前に終了インターフェイスで設定できます。 この機能は WCCP バージョン 1 とバージョン 2 でサポートされています。	*Configuring WCCP*
12.2(14)S	SLB：AAA ロード バランシング	Cisco IOS SLB は、RADIUS Authentication, Authorization, and Accounting（AAA; 認証、認可、アカウンティング）サーバに RADIUS ロード バランシング機能を提供します。	*Configuring Server Load Balancing*
	SLB：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。	*Configuring Server Load Balancing*

表 1　サポートされる IP アプリケーション サービス機能 （続き）

リリース	機能名	機能の説明	参照先
	SLB：DFP Agent Subsystem のサポート	Cisco 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る）をサポートします。そのため、Cisco 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機能することができます。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。	*Configuring Server Load Balancing*
	SLB：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	Cisco IOS SLB は、GTP version 0（GTP v0）と GTP version 1（GTP v1）の両方をサポートします。GTP のサポートによって、Cisco IOS SLB は、「GTP 認識」になり、レイヤ 5 に対する知識を拡張することができます。	*Configuring Server Load Balancing*
	SLB：複数ファイアウォール ファームのサポート	複数ファイアウォール ファームのサポート機能を使用すると、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。	*Configuring Server Load Balancing*
	SLB：プローブ：DNS、Routed、および TCP プローブ	Cisco IOS SLB プローブは、サーバ ファーム内の実サーバごとのステータスと、ファイアウォール ファーム内のファイアウォールごとのステータスを判断します。	*Configuring Server Load Balancing*
	SLB：RADIUS ロード バランシング：CDMA2000	Cisco IOS SLB は、Cisco Service Selection Gateway（SSG）や Cisco Content Services Gateway（CSG））などのサービス ゲートウェイ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 バランシングを提供します。Cisco IOS SLB は、簡易 IP CDMA2000 ネットワークと Mobile IP CDMA2000 ネットワークに対して RADIUS ロード バランシングをサポートします。	*Configuring Server Load Balancing*
	SLB：RADIUS ロード バランシング：General Packet Radio Service（GPRS）ネットワーク	Cisco IOS SLB は、Cisco Service Selection Gateway（SSG）や Cisco Content Services Gateway（CSG））などのサービス ゲートウェイ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 バランシングを提供します。Cisco IOS SLB は、GPRS ネットワークに対して 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 Gateway General Packet Radio Service（GPRS）Support Node（GGSN）です。	*Configuring Server Load Balancing*
	SLB：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	Cisco IOS SLB は、Cisco Service Selection Gateway（SSG）や Cisco Content Services Gateway（CSG））などのサービス ゲートウェイ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 バランシングを提供します。Cisco IOS SLB は、複数のサービス ゲートウェイ サーバ ファーム（たとえば、SSG の 1 つのファームと CSG の別のファーム）に対して RADIUS ロード バランシングをサポートします。	*Configuring Server Load Balancing*

表 1　サポートされる IP アプリケーション サービス機能 （続き）

リリース	機能名	機能の説明	参照先
	SLB：ルート ヘルス インジェクション	（**inservice** コマンドを使用して）仮想サーバをサービスに登録すると、デフォルトで、仮想サーバの IP アドレスがアドバタイズされます（ルーティング テーブルに追加されます）。Web サイトの仮想 IP アドレスに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、**advertise** コマンドを使用して、IP アドレスの可用性が Cisco IOS SLB で確認された場合にだけ、ホスト ルートをアドバタイズするように、Cisco IOS SLB を設定することができます。IP アドレスを使用できなくなると、Cisco IOS SLB が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。	*Configuring Server Load Balancing*
	SLB：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。	*Configuring Server Load Balancing*
	SLB：VPN サーバ ロード バランシング	Cisco IOS SLB は、バーチャル プライベート ネットワーク（VPN）フローのバランスを取ることができます。	*Configuring Server Load Balancing*
Cisco IOS Release 12.2SB			
12.2(31)SB2	Clear IP Traffic CLI	Clear IP Traffic CLI 機能で、**clear ip traffic** コマンドが導入されました。これにより、ルータをリロードするのではなく、ルータ上のすべての IP トラフィック統計情報がクリアされるようになりました。安全性を高めるため、このコマンドを入力すると、ユーザに確認プロンプトが表示されます。	*Configuring IP Services*
	ICMP Unreachable Rate Limiting User Feedback	ICMP Unreachable Rate Limiting User Feedback 機能により、到達不能な宛先であるために破棄されたパケットをクリアして表示することができます。エラー メッセージをトリガーするしきい値の間隔を設定できます。メッセージ ロギングが生成されると、コンソールに表示されます。	*Configuring IP Services*
	TCP アプリケーション フラグ 拡張	TCP アプリケーション フラグ拡張機能によって、TCP アプリケーションに関する追加のフラグが表示可能になります。フラグには、ステータスやオプションという 2 種類のタイプがあります。ステータス フラグは、再送タイムアウト、アプリケーション クローズ、リスンの同期（SYNC）ハンドシェイクなど、TCP 接続のステータスを示します。追加のフラグは、バーチャル プライベート ネットワーク（VPN）のルーティングおよびフォワーディング（VRF）の識別情報が設定されているかどうか、ユーザがアイドル状態かどうか、キープアライブ タイマーが動作しているかどうかなど、オプションの状態を示します。	*Configuring TCP*

表 1　サポートされる IP アプリケーション サービス機能 （続き）

リリース	機能名	機能の説明	参照先
	TCP 明示的輻輳通知	Explicit Congestion Notification（ECN; TCP 明示的輻輳通知）機能では、中間のルータが端点のホストにネットワーク輻輳が差し迫っていることを通知できるようになります。また、Telnet、Web 閲覧、音声や映像データの転送を含む、遅延やパケット損失の影響を受けるアプリケーションに関連付けられた TCP セッションのサポートも強化されています。この機能の利点は、データ転送時の遅延やパケット損失の軽減です。	*Configuring TCP*
	TCP Show 拡張	TCP Show 拡張機能では、ホストネーム形式の代わりに IP 形式でのアドレス表示、および接続に関連するバーチャル プライベート ネットワーク（VPN）のルーティングおよびフォワーディング（VRF）テーブル表示の機能を導入します。	*Configuring TCP*
12.2(31)SB2	TCP ウィンドウ スケーリング	TCP ウィンドウ スケーリング機能は、RFC 1323 のウィンドウ スケーリング オプションのサポートを追加しました。Long Fat Network（LFN; 広帯域高遅延ネットワーク）と呼ばれる広帯域で高遅延の特性を持つネットワーク経路での TCP のパフォーマンスを改善するため、より大きなウィンドウ サイズが推奨されます。TCP ウィンドウ スケーリングの強化で、そのサポートを提供します。	*Configuring TCP*
Cisco IOS Release 12.2SR			
12.2(33)SRE	SLB：Access Service Network（ASN）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	ASN ロード バランシングは、ステートフル冗長性とスティッキ接続をサポートします。	*Configuring Server Load Balancing*
	SLB：BWG スティッキのサポート	Cisco IOS SLB は、すべてのバージョンの GTP（v0、v1、v2）に対して sticky-only をサポートします。	*Configuring Server Load Balancing*
	SLB：ファイアウォール ロード バランシング	Cisco IOS SLB ファイアウォール ロード バランシングを使用すれば、CPU の使用率が高くなる可能性のある特定の状態を回避できます。	*Configuring Server Load Balancing*
	SLB：GTPV2 ロード バランシング	Cisco IOS SLB は、GTP version 2（GTP v2）をサポートします。	*Configuring Server Load Balancing*
	SLB：Hot ICE 準拠	すべての Cisco IOS SLB コマンドが Hot ICE 準拠です。Hot ICE は、Cisco IOS 設定管理の運用堅牢性、スケーラビリティ、およびプログラム可能性を向上させるように設計された Cisco IOS 設定機能強化のセットです。	*Configuring Server Load Balancing*
	SLB：サブインターフェイスのサポート	Cisco IOS SLB は、**access** コマンドに対して、サブインターフェイスのサポートを提供しています。	*Configuring Server Load Balancing*

表 1　サポートされる IP アプリケーション サービス機能 （続き）

リリース	機能名	機能の説明	参照先
	WCCP VRF のサポート	WCCP VRF のサポート機能によって、VRF の認識をサポートする既存の WCCPv2 プロトコルが強化されています。	*Configuring WCCP*
12.2(33) SRC1	SLB：Access Service Network（ASN）R6 ロード バランシング	Cisco IOS SLB は、ASN ゲートウェイ セット全体にロード バランシングを提供します。ゲートウェイのクラスタは、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。	*Configuring Server Load Balancing*
12.2(33)SRC	接続のレート制限	Cisco IOS SLB を使用すれば、サーバ ファーム内の 1 台の実サーバに許可する最大接続レートを指定することができます。	*Configuring Server Load Balancing*
	仮想サーバの INOP_REAL 状態	仮想サーバの INOP_REAL 状態機能により、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。	*Configuring Server Load Balancing*
	KeepAlive Application Protocol（KAL-AP）エージェントのサポート	KAL-AP エージェントのサポートを使用すれば、Cisco IOS SLB を通して、Global Server Load Balancing（GSLB; グローバル サーバ ロード バランシング）環境でロード バランシングを実行することができます。	*Configuring Server Load Balancing*
	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	RADIUS ロード バランシング加速データ プレーン フォワーディング（Turbo RADIUS ロード バランシングとも呼ばれる）は、CSG 環境で基本的な Policy-Based Routing（PBR; ポリシーベース ルーティング）ルート マップを使用して加入者のデータプレーン トラフィックを管理する高性能ソリューションです。	*Configuring Server Load Balancing*
12.2(33)SRB	GPRS ロード バランシング：GPRS ロード バランシング マップ	GPRS ロード バランシング マップによって、Cisco 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、ルーティングすることができます。	*Configuring Server Load Balancing*
	RADIUS ロード バランシング：RADIUS ロード バランシング マップ	RADIUS ロード バランシング マップによって、Cisco IOS SLB は RADIUS 発信側ステーション ID とユーザ名に基づいてユーザ トラフィックを分類し、ルーティングすることができます。RADIUS ロード バランシング マップは、Turbo RADIUS ロード バランシングおよび RADIUS ロード バランシング アカウンティングのローカル ACK と同時に使用できません。	*Configuring Server Load Balancing*

表 1　サポートされる IP アプリケーション サービス機能 （続き）

リリース	機能名	機能の説明	参照先
12.2(33)SRA	IP Precedence Accounting	IP Precedence Accounting 機能により、インターフェイス上の優先順位に基づいて IP トラフィックのアカウンティング情報が提供されます。この機能は、IP パケットを送受信したインターフェイスごとにパケット数の合計とバイト数の合計を計算し、IP 優先順位に基づいて結果をソートします。この機能はすべてのインターフェイスおよびサブインターフェイスでサポートされ、CEF、dCEF、フロー、および最適なスイッチングをサポートします。	*Configuring IP Services*
	TCP MSS 調整	TCP MSS 調整機能では、ルータを通過する一時的なパケット（特に SYN ビットが設定された TCP セグメント）の Maximum Segment Size（MSS; 最大セグメント サイズ）を設定することができるようになります。	*Configuring TCP*
	WCCP Increased Service	WCCP Increased Service 機能によって、WCCP によってサポートされるサービスの数が最大で 256 に増えます。	*Configuring WCCP*
Cisco IOS Release 12.2SX			
12.2(33) SXH1	IP Precedence Accounting	IP Precedence Accounting 機能により、インターフェイス上の優先順位に基づいて IP トラフィックのアカウンティング情報が提供されます。この機能は、IP パケットを送受信したインターフェイスごとにパケット数の合計とバイト数の合計を計算し、IP 優先順位に基づいて結果をソートします。この機能はすべてのインターフェイスおよびサブインターフェイスでサポートされ、CEF、dCEF、フロー、および最適なスイッチングをサポートします。	*Configuring IP Services*
12.2(33) SXH	TCP MSS 調整	TCP MSS 調整機能では、ルータを通過する一時的なパケット（特に SYN ビットが設定された TCP セグメント）の Maximum Segment Size（MSS; 最大セグメント サイズ）を設定することができるようになります。	*Configuring TCP*
	WCCP Increased Service	WCCP Increased Service 機能によって、WCCP によってサポートされるサービスの数が最大で 256 に増えます。	*Configuring WCCP*
12.2(18)SXF13	IP Precedence Accounting	IP Precedence Accounting 機能により、インターフェイス上の優先順位に基づいて IP トラフィックのアカウンティング情報が提供されます。この機能は、IP パケットを送受信したインターフェイスごとにパケット数の合計とバイト数の合計を計算し、IP 優先順位に基づいて結果をソートします。この機能はすべてのインターフェイスおよびサブインターフェイスでサポートされ、CEF、dCEF、フロー、および最適なスイッチングをサポートします。	*Configuring IP Services*

表 1　サポートされる IP アプリケーション サービス機能 （続き）

リリース	機能名	機能の説明	参照先
12.2(17d) SXE	SLB：GTP IMSI スティッキ データベース	Cisco IOS SLB は、特定の International Mobile Subscriber ID（IMSI）用の Gateway General Packet Radio Service（GPRS）Support Node（GGSN）を選択して、同じ IMSI から、選択された GGSN に、以降のすべての Packet Data Protocol（PDP）作成要求を転送することができます。	*Configuring Server Load Balancing*
	SLB：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 Cisco IOS SLB が必要です。たとえば、Cisco IOS SLB を通して、ファームの片側で RADIUS ロード バランシングを実行し、反対側でファイアウォール ロード バランシングを実行させることも、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させることもできます。	*Configuring Server Load Balancing*
	SLB：RADIUS ロード バランシング：RADIUS ロード バランシング IMSI スティッキ データベース	Cisco IOS SLB RADIUS International Mobile Subscriber ID（IMSI）スティッキ データベースは、各ユーザの IMSI アドレスを対応するゲートウェイにマップします。この機能を使用すれば、Cisco IOS SLB で、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することができます。	*Configuring Server Load Balancing*
12.2(17d) SXD	SLB：DFP および Home Agent Director	Home Agent Director の場合は、Cisco IOS SLB を DFP マネージャとして定義し、サーバ ファーム内の各ホーム エージェント上で DFP エージェントを定義することができます。また、DFP エージェントから、ホーム エージェントの加重を報告することができます。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。	*Configuring Server Load Balancing*
12.2(17d) SXB1	SLB：GGSN-IOS SLB メッセージング	この機能を使用すれば、特定の状態が発生したときに、GGSN から Cisco IOS SLB に通知することができます。この通知によって、Cisco IOS SLB は適切な判断を下すことができます。その結果、GPRS ロード バランシングと障害検出が改善されます。	*Configuring Server Load Balancing*

表 1　サポートされる IP アプリケーション サービス機能 （続き）

リリース	機能名	機能の説明	参照先
Cisco IOS Release 12.2T、12.3、12.3T、12.4、および 12.4T			
12.4(20)T	FHRP : **rtr** キーワードの EOT の廃止	Cisco IOS Release 12.4(20)SRB では、**track rtr** コマンドは **track ip sla** コマンドに置き換えられています。	*Configuring Enhanced Object Tracking*
	SCTP Release 4、フェーズ 2	SCTP Release 4 のフェーズ 2 で、SCTP Add-IP 機能が導入されました。SCTP Add-IP 機能では、既存の SCTP アソシエーションのエンドポイントに IP アドレスを追加または削除して、この変更をリモートの端点に伝えることができます。	*Stream Control Transmission Protocol*
	WCCP レイヤ 2 リダイレクション/フォワーディング	WCCP レイヤ 2 リダイレクション/フォワーディング機能を使用すると、直接接続している Cisco Content Engine でレイヤ 2 リダイレクトを使用できます。これは、GRE カプセル化を介するレイヤ 3 リダイレクションよりも効率的です。	*Configuring WCCP*
	WCCP L2 返送	WCCP L2 返送機能を使用すると、レイヤ 3 GRE トンネル内のルータにパケットをトンネル処理するのではなく、発信元および宛先の MAC アドレスを交換することで、コンテンツ エンジンから、レイヤ 2 で直接接続されている WCCP ルータにパケットを返送できます。	*Configuring WCCP*
	WCCP マスク割り当て	WCCP マスク割り当て機能では、キャッシュ エンジン割り当て方式として、ACNS/WAAS デバイスのサポートを導入します。	*Configuring WCCP*
12.4(15)T	SCTP Release 4	SCTP Release 4 で、SCTP ストリーム リセットと認証機能が導入されました。	*Stream Control Transmission Protocol*
12.4(11)T	SCTP Show および Clear の CLI 機能拡張	Stream Control Transmission Protocol（SCTP）Show および Clear の CLI 機能拡張で、潜在的な問題のトラブルシューティングに役立つ SCTP の追加情報にアクセスできます。また、これらの機能拡張によって、更新された SCTP **show** と **clear** コマンドは他の転送プロトコルの CLI と一致するようになりました。	*Stream Control Transmission Protocol*
	Show and Clear Commands for IOS Sockets	Show and Clear Commands for IOS Sockets 機能で、**show udp**、**show sockets**、および **clear sockets** コマンドが導入されました。これらの新しいコマンドは、Cisco IOS ソケット ライブラリのモニタリングや管理に役立ちます。	*Configuring IP Services*

表 1　　サポートされる IP アプリケーション サービス機能 （続き）

リリース	機能名	機能の説明	参照先
12.4(2)T	Clear IP Traffic CLI	Clear IP Traffic CLI 機能で、**clear ip traffic** コマンドが導入されました。これにより、ルータをリロードするのではなく、ルータ上のすべての IP トラフィック統計情報がクリアされるようになりました。安全性を高めるため、このコマンドを入力すると、ユーザに確認プロンプトが表示されます。	*Configuring IP Services*
	ICMP Unreachable Rate Limiting User Feedback	ICMP Unreachable Rate Limiting User Feedback 機能により、到達不能な宛先であるために破棄されたパケットをクリアして表示することができます。エラー メッセージをトリガーするしきい値の間隔を設定できます。メッセージ ロギングが生成されると、コンソールに表示されます。	*Configuring IP Services*
	TCP アプリケーション フラグ拡張	TCP アプリケーション フラグ拡張機能によって、TCP アプリケーションに関する追加のフラグが表示可能になります。フラグには、ステータスやオプションという 2 種類のタイプがあります。ステータス フラグは、再送タイムアウト、アプリケーション クローズ、リスンの同期（SYNC）ハンドシェイクなど、TCP 接続のステータスを示します。追加のフラグは、バーチャル プライベート ネットワーク（VPN）のルーティングおよびフォワーディング（VRF）の識別情報が設定されているかどうか、ユーザがアイドル状態かどうか、キープアライブ タイマーが動作しているかどうかなど、設定オプションの状態を示します。	*Configuring TCP*
	TCP Show 拡張	TCP Show 拡張機能では、ホストネーム形式の代わりに IP 形式でのアドレス表示、および接続に関連するバーチャル プライベート ネットワーク（VPN）のルーティングおよびフォワーディング（VRF）テーブル表示の機能を導入します。	*Configuring TCP*
12.3(14)T	WCCP Increased Service	WCCP Increased Service 機能によって、WCCP によってサポートされるサービスの数が最大で 256 に増えます。	*Configuring WCCP*

表 1　サポートされる IP アプリケーション サービス機能 （続き）

リリース	機能名	機能の説明	参照先
12.3(7)T	TCP 輻輳回避	TCP 輻輳回避機能を使用すると、単一のウィンドウ内で複数パケットが損失しているとき、TCP 送信側に対する確認応答パケットをモニタできます。以前は、送信側は高速リカバリ モードを終了するか、3 以上の重複確認応答パケットを待ってから次の未応答パケットを再送信するか、または再送タイマーのスロー スタートを待ちました。これは、パフォーマンスの問題になることがありました。	*Configuring TCP*
	TCP 明示的輻輳通知	Explicit Congestion Notification（ECN; TCP 明示的輻輳通知）機能では、中間のルータが端点のホストにネットワーク輻輳が差し迫っていることを通知できるようになります。また、Telnet、Web 閲覧、音声や映像データの転送を含む、遅延やパケット損失の影響を受けるアプリケーションに関連付けられた TCP セッションのサポートも強化されています。この機能の利点は、データ転送時の遅延やパケット損失の軽減です。	*Configuring TCP*
	WCCP バイパス カウンタ	WCCP バイパス カウンタ機能を使用すると、Web キャッシュによってバイパスされ、元のルータに返送され、通常どおりに転送されたパケットのカウントを表示できます。	*Configuring WCCP*
	WCCP 発信 ACL チェック	WCCP 発信 ACL チェック機能を使用すると、入力インターフェイスで WCCP によってリダイレクトされるトラフィックが、必ず発信 ACL チェックを受けるようにできます。これは、リダイレクト前に終了インターフェイスで設定できます。 この機能は WCCP バージョン 1 とバージョン 2 でサポートされています。	*Configuring WCCP*
12.2(8)T	SCTP Release 2	SCTP Release 2 では、SCTP コマンドの出力が更新されています。	*Stream Control Transmission Protocol*
	TCP MSS 調整	TCP MSS 調整機能では、ルータを通過する一時的なパケット（特に SYN ビットが設定された TCP セグメント）の Maximum Segment Size（MSS; 最大セグメント サイズ）を設定することができるようになります。 この機能により導入されたコマンドが、12.2(8)T で **ip adjust-mss** から **ip tcp adjust-mss** に変更されました。	*Configuring TCP*
	TCP ウィンドウ スケーリング	TCP ウィンドウ スケーリング機能は、RFC 1323 のウィンドウ スケーリング オプションのサポートを追加しました。Long Fat Network（LFN; 広帯域高遅延ネットワーク）と呼ばれる広帯域で高遅延の特性を持つネットワーク経路での TCP のパフォーマンスを改善するため、より大きなウィンドウ サイズが推奨されます。TCP ウィンドウ スケーリングの強化で、そのサポートを提供します。	*Configuring TCP*

表 1　サポートされる IP アプリケーション サービス機能 （続き）

リリース	機能名	機能の説明	参照先
12.2(4)T	SCTP Release 1	Stream Control Transmission Protocol（SCTP; ストリーム制御通信プロトコル）は信頼性のあるデータグラム型 IP トランスポート プロトコルで、RFC 2960 で仕様が定められています。	*Stream Control Transmission Protocol*
	TCP MSS 調整	TCP MSS 調整機能では、ルータを通過する一時的なパケット（特に SYN ビットが設定された TCP セグメント）の Maximum Segment Size（MSS; 最大セグメント サイズ）を設定することができるようになります。	*Configuring TCP*
Cisco IOS Release 12.2			
12.2(21)	IP Precedence Accounting	IP Precedence Accounting 機能により、インターフェイス上の優先順位に基づいて IP トラフィックのアカウンティング情報が提供されます。この機能は、IP パケットを送受信したインターフェイスごとにパケット数の合計とバイト数の合計を計算し、IP 優先順位に基づいて結果をソートします。この機能はすべてのインターフェイスおよびサブインターフェイスでサポートされ、CEF、dCEF、フロー、および最適なスイッチングをサポートします。	*Configuring IP Services*
12.2(15)	UDP Forwarding Support for IP Redundancy Virtual Router Group	User Datagram Protocol（UDP; ユーザ データグラム プロトコル）転送は、特定の IP アドレスで受信したブロードキャスト パケットとマルチキャスト パケットを転送するために Cisco IOS ソフトウェアで使用する機能です。現在、Hot Standby Routing Protocol（HSRP; ホット スタンバイ ルーティング プロトコル）とともに Virtual Router Group（VRG; 仮想ルータ グループ）サポートが実装されているため、ルータのセットをグループ化して論理ルータとし、既知の IP アドレスに応答できます。UDP Forwarding Support for IP Redundancy Virtual Router Groups 機能を使用すると、UDP 転送で VRG を認識できるようになり、結果として VRG のアクティブ ルータのみを対象に転送できるようになります。	*Configuring UDP Forwarding Support for IP Redundancy Virtual Router Groups*

表 1　サポートされる IP アプリケーション サービス機能 （続き）

リリース	機能名	機能の説明	参照先
12.2(1)	SLB：アクティブ スタンバイ	アクティブ スタンバイを使用すれば、2 つの Cisco IOS SLB が、同じ仮想 IP アドレスを負荷分散しながら、相互にバックアップとして機能することができます。	*Configuring Server Load Balancing*
	SLB：サーバ ロード バランシングのアルゴリズム	Cisco IOS SLB は、加重ラウンド ロビン、加重最小接続、およびルート マップ ロード バランシング アルゴリズムを提供します。	*Configuring Server Load Balancing*
	SLB：代替 IP アドレス	Cisco IOS SLB を使用すれば、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 できます。	*Configuring Server Load Balancing*
	SLB：オーディオおよびビデオのロード バランシング	Cisco IOS SLB は、RealNetworks アプリケーションを実行しているサーバに対して、Real-Time Streaming Protocol（RTSP; リアルタイム トランスポート ストリーミング プロトコル）経由の RealAudio ストリームと RealVideo ストリームのバランスを取ることができます。	*Configuring Server Load Balancing*
	SLB：自動サーバ障害検出	Cisco IOS SLB は、失敗した実サーバへの TCP 接続の試みを自動的に検出し、そのサーバの障害カウンタをインクリメントします 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。	*Configuring Server Load Balancing*

表 1　サポートされる IP アプリケーション サービス機能 （続き）

リリース	機能名	機能の説明	参照先
	SLB：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。タイマーがタイムアウトすると、再び、そのサーバに新しい仮想サーバ接続の資格が与えられ、Cisco 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。	*Configuring Server Load Balancing*
	SLB：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	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。	*Configuring Server Load Balancing*
	SLB：バインド 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。	*Configuring Server Load Balancing*
	SLB：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。	*Configuring Server Load Balancing*
	SLB：クライアント NAT	ネットワークで複数のロード バランシング デバイスを使用している場合、クライアント IP アドレスを、デバイスのいずれかに関連付けられている IP アドレスで置換することで、発信フローが適切なデバイスにルーティングされます。また、クライアント NAT の場合、多数のクライアントが同じ一時ポートを使用できるため、一時クライアント ポートを変更する必要があります。複数のロード バランシング デバイスを使用しない場合でも、負荷が分散された接続のパケットがデバイス中をルーティングされないようにするには、クライアント NAT が便利です。	*Configuring Server Load Balancing*

表 1　サポートされる IP アプリケーション サービス機能 （続き）

リリース	機能名	機能の説明	参照先
	SLB：TCP 接続コンテキストの遅延削除	IP パケットの順序異常が原因で、Cisco IOS SLB が、TCP 接続の終了（finish [FIN] または reset [RST]）後に、接続用の他のパケットが続いているのを検出する場合があります。一般的に、この問題は TCP 接続パケットがたどるパスが複数あるときに発生します。接続が終了した後に到着するパケットを適切にリダイレクトするために、Cisco IOS SLB が、指定された期間、TCP 接続情報（つまり、コンテキスト）を保持します。接続の終了後にコンテキストを保持する期間は、設定可能な遅延タイマーで制御されます。	*Configuring Server Load Balancing*
	SLB：IOS SLB 用のダイナミック フィードバック プロトコル	Cisco 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る）をサポートします。そのため、Cisco 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機能することができます。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。	*Configuring Server Load Balancing*
	SLB：ファイアウォール ロード バランシング	名前が示すように、ファイアウォール ロード バランシングを使用すれば、Cisco IOS SLB でファイアウォールへのフローのバランスを取ることができます。ファイアウォール 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。	*Configuring Server Load Balancing*
	Cisco IOS SLB、12.2 の最初のリリース	Cisco IOS SLB 機能は、さまざまなネットワーク デバイスおよびサービスにロード バランシングを提供する Cisco IOS ベースのソリューションです。	*Configuring Server Load Balancing*
	SLB：最大接続数	Cisco IOS SLB を使用すれば、サーバとファイアウォールのロード バランシング用の最大接続数を設定できます。	*Configuring Server Load Balancing*
	SLB：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。	*Configuring Server Load Balancing*
	SLB：プローブ：HTTP、ping、および WSP プローブ	Cisco IOS SLB プローブは、サーバ ファーム内の実サーバごとのステータスと、ファイアウォール ファーム内のファイアウォールごとのステータスを判断します。	*Configuring Server Load Balancing*

表 1　サポートされる IP アプリケーション サービス機能 （続き）

リリース	機能名	機能の説明	参照先
	SLB：コンテンツ フロー モニタのサポート	Cisco 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。	*Configuring Server Load Balancing*
	SLB：プロトコル サポート	Cisco IOS SLB は、固定のプロトコル セットをサポートします。	*Configuring Server Load Balancing*
	SLB：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。	*Configuring Server Load Balancing*
	SLB：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 スタート機能によって、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。	*Configuring Server Load Balancing*
	SLB：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れば、Cisco IOS SLB で、ロード バランシングの決定を段階的にバックアップしたり、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」したりすることができます。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。	*Configuring Server Load Balancing*
	SLB：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場合は特に、ステートレス バックアップが有効です。	*Configuring Server Load Balancing*

表 1　サポートされる IP アプリケーション サービス機能 （続き）

リリース	機能名	機能の説明	参照先
	SLB：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。オプションの **sticky** コマンドを使用すれば、Cisco IOS SLB で、同じクライアントから、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することができます。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。	*Configuring Server Load Balancing*
	SLB：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 は、Cisco IOS SLB または実サーバをダウンさせるこのような攻撃を阻止します。SynGuard は、仮想サーバが処理する SYN 数を特定の間隔でモニタし、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。	*Configuring Server Load Balancing*
	SLB：TCP セッション再割り当て	Cisco IOS SLB は、新しい接続を開くためにクライアントから実サーバに送信された TCP SYN を追跡します。複数の連続する SYN に応答がない場合、または SYN が RST で応答される場合、TCP セッションは新しい実サーバに再割り当てされます。SYN の試行回数は、設定可能な再割り当てしきい値で制御されます。	*Configuring Server Load Balancing*
	SLB：WAP ゲートウェイ ロード バランシング	Wireless Application Protocol（WAP; ワイヤレス アプリケーション プロトコル）ロード バランシング機能を使用すれば、Cisco IOS SLB を使用して、IP ベアラ ネットワーク上の WAP ゲートウェイまたはサーバのグループ内で、Wireless Session Protocol（WSP）セッションを負荷分散させることができます。	*Configuring Server Load Balancing*
	SLB：Web キャッシュ ロード バランシング	Cisco IOS SLB は、透過的 Web キャッシュのクラスタ全体で HTTP フローを負荷分散させることができます。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。	*Configuring Server Load Balancing*

表 1　サポートされる IP アプリケーション サービス機能 （続き）

リリース	機能名	機能の説明	参照先
12.1(5)T15	IP Precedence Accounting	IP Precedence Accounting 機能により、インターフェイス上の優先順位に基づいて IP トラフィックのアカウンティング情報が提供されます。この機能は、IP パケットを送受信したインターフェイスごとにパケット数の合計とバイト数の合計を計算し、IP 優先順位に基づいて結果をソートします。この機能はすべてのインターフェイスおよびサブインターフェイスでサポートされ、CEF、dCEF、フロー、および最適なスイッチングをサポートします。	*Configuring IP Services*
Cisco IOS XE 3.1.0SG			
Cisco IOS XE 3.1.0SG	TCP MIB for RFC 4022 サポート	TCP MIB for RFC 4022 サポート機能で、RFC 4022「*Management Information Base for the Transmission Control Protocol (TCP)*」に対するサポートが導入されました。RFC 4022 は、TCP の管理容易性を向上させるための TCP MIB の増分変更です。	*Configuring TCP*
	TCP Show 拡張	TCP Show 拡張機能では、ホストネーム形式の代わりに IP 形式でのアドレス表示、および接続に関連するバーチャル プライベート ネットワーク（VPN）のルーティングおよびフォワーディング（VRF）テーブル表示の機能を導入します。	*Configuring TCP*
	UDP Forwarding Support of IP Redundancy Virtual Router Group（VRG）	User Datagram Protocol（UDP; ユーザ データグラム プロトコル）転送は、特定の IP アドレスで受信したブロードキャスト パケットとマルチキャスト パケットを転送するために Cisco IOS ソフトウェアで使用する機能です。現在、Hot Standby Routing Protocol（HSRP; ホット スタンバイ ルーティング プロトコル）とともに Virtual Router Group（VRG; 仮想ルータ グループ）サポートが実装されているため、ルータのセットをグループ化して論理ルータとし、既知の IP アドレスに応答できます。UDP Forwarding Support for IP Redundancy Virtual Router Groups 機能を使用すると、UDP 転送で VRG を認識できるようになり、結果として VRG のアクティブ ルータのみを対象に転送できるようになります。	*Configuring UDP Forwarding Support for IP Redundancy Virtual Router Groups*

表 1　サポートされる IP アプリケーション サービス機能 （続き）

リリース	機能名	機能の説明	参照先
その他の Cisco IOS リリース			
12.2(18)ZU2	TCP MSS 調整	TCP MSS 調整機能では、ルータを通過する一時的なパケット（特に SYN ビットが設定された TCP セグメント）の Maximum Segment Size（MSS; 最大セグメント サイズ）を設定することができるようになります。	*Configuring TCP*
12.2(14)ZA5	SLB : Exchange Director 機能	Cisco IOS SLB は、Cisco 7600 シリーズ ルータ用の mobile Service Exchange Framework（mSEF）に対して Exchange Director をサポートします。	*Configuring Server Load Balancing*
	SLB：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。	*Configuring Server Load Balancing*
	SLB：冗長ルート プロセッサのステートフル バックアップ	RPR+ を併用した場合、Cisco IOS SLB は、Cisco 7600 シリーズ ルータの mSEF に対して、冗長ルート プロセッサのステートフル バックアップをサポートします。この機能を使用すれば、Cisco IOS SLB と同じシャーシに Cisco Multiprocessor WAN Application Module（MWAN）を配置しながら、ロード バランシング割り当てのハイ アベイラビリティを維持することができます。	*Configuring Server Load Balancing*
12.2(14)ZA4	SLB：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	Cisco IOS SLB は、失敗した実サーバへの TCP 接続の試みを自動的に検出し、そのサーバの障害カウンタをインクリメントします。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。	*Configuring Server Load Balancing*

表 1　サポートされる IP アプリケーション サービス機能 （続き）

リリース	機能名	機能の説明	参照先
12.2(14)ZA2	SLB：GPRS ロード バランシング：GTP v0 および GTP v1 のサポート	Cisco IOS SLB は、GTP version 0（GTP v0）と GTP version 1（GTP v1）の両方をサポートします。GTP のサポートによって、Cisco IOS SLB は、「GTP 認識」になり、レイヤ 5 に対する知識を拡張することができます。	*Configuring Server Load Balancing*
	SLB：GTP Cause Code Inspection を備えた 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れば、Cisco IOS SLB で、GGSN サーバ ファームとの間で送受信するすべての PDP コンテキスト シグナリング フローをモニタすることができます。この機能を使用すれば、Cisco IOS SLB を通して、GTP 障害の原因コードをモニタし、Cisco GGSN と非 Cisco GGSN の両方で発生したシステム レベルの問題を検出することができます。	*Configuring Server Load Balancing*
	SLB：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。	*Configuring Server Load Balancing*
	SLB：プローブ：カスタム UDP プローブ	Cisco IOS SLB プローブは、サーバ ファーム内の実サーバごとのステータスと、ファイアウォール ファーム内のファイアウォールごとのステータスを判断します。	*Configuring Server Load Balancing*
12.1(27b)E1	IP Precedence Accounting	IP Precedence Accounting 機能により、インターフェイス上の優先順位に基づいて IP トラフィックのアカウンティング情報が提供されます。この機能は、IP パケットを送受信したインターフェイスごとにパケット数の合計とバイト数の合計を計算し、IP 優先順位に基づいて結果をソートします。この機能はすべてのインターフェイスおよびサブインターフェイスでサポートされ、CEF、dCEF、フロー、および最適なスイッチングをサポートします。	*Configuring IP Services*
12.1(3)T	受信インターフェイスでの WCCP のリダイレクション	受信インターフェイスでの WCCP のリダイレクション機能によって、特定の WCCP サービスのために入力リダイレクションのインターフェイスを設定できます。インターフェイスでこの機能をイネーブルにすると、そのインターフェイスに到達するすべてのパケットは、指定した WCCP サービスに対して比較されます。パケットが一致する場合、そのパケットはリダイレクトされます。	*Configuring WCCP*
12.0(3)T	WCCP バージョン 2	WCCP バージョン 2 のいくつかの機能が強化され、WCCP プロトコルに機能が追加されました。	*Configuring WCCP*

表 1　サポートされる IP アプリケーション サービス機能 （続き）

リリース	機能名	機能の説明	参照先
10.0	スパニング ツリーを使用したパケットのフラッディング	スパニング ツリー転送テーブルを使用した UDP ブロードキャスト パケットの高速転送を行うことができるようにします。	*Configuring IPv4 Broadcast Packet Handling*
	IP 誘導ブロードキャスト	誘導ブロードキャストの物理ブロードキャストへの変換をイネーブルにします。	*Configuring IPv4 Broadcast Packet Handling*
	IP ブロードキャスト アドレスの指定	インターフェイスの IP ブロードキャスト アドレスを指定します。	*Configuring IPv4 Broadcast Packet Handling*
	UDP ブロードキャスト パケット転送	UDP ブロードキャスト パケットの転送をイネーブルにします。	*Configuring IPv4 Broadcast Packet Handling*

サーバ ロード バランシングの設定

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

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

IOS SLB 機能の使用方法

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

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

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

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

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

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

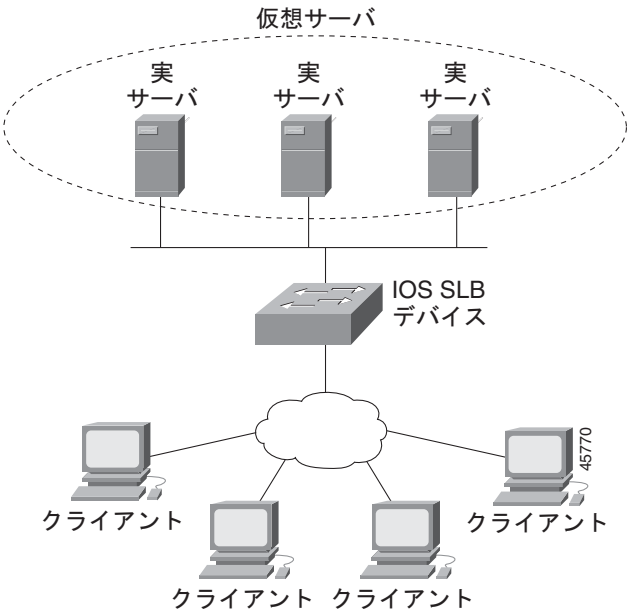
- モバイル、Public Wireless LAN（PWLAN; パブリック ワイヤレス LAN）、およびサービス プロバイダー ネットワーク用のその他のコンポーネント：
  - Wireless Application Protocol（WAP; ワイヤレス アプリケーション プロトコル）ゲートウェイ
  - プロトコル最適化ゲートウェイ
  - 他社製 GGSN および Home Agent
  - 他の RADIUS 対応フロー ゲートウェイ。これらのゲートウェイは、ゲートウェイを介してユーザに送信されるルートの RADIUS 認可要求およびアカウンティング要求を受信するプロキシまたは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

また、Exchange Director には次の機能もあります。

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

図 1 に、単純な IOS SLB ネットワークを示します。

図 1　　Cisco IOS SLB の論理構成図



機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。この章に記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「IOS SLB の機能情報」（P.194）を参照してください。

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

この章の構成

Cisco IOS SLB に関する制約事項

一般的な制約事項

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

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

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

スタティック NAT に関する制約事項

- クライアント NAT サーバ ファームと併用できません。つまり、実サーバでサーバ NAT に仮想 IP アドレスが使用されており、サーバ ファームがそれと同じ仮想 IP アドレスに関連付けられている場合は、クライアント NAT を使用するようにサーバ ファームを設定することができません。
- 各実サーバは 1 つの仮想サーバにのみ関連付ける必要があります。これは、IOS SLB が接続を適切に作成するためです。
- 0 ポートの仮想サーバが必要です。

- 仮想サービス FTP はサポートされません。
- パケット単位サーバ ロード バランシングを使用したスタティック NAT では、フラグメント化されたパケットが負荷分散されません。

バックアップ サーバ ファームに関する制約事項

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

ファイアウォール ロード バランシングに関する制約事項

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

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

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

- Client-Assigned ロード バランシング
- スロー スタート
- 加重最小接続ロード バランシング アルゴリズム

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

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

GTP v2 に関する制約事項

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

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

VPN サーバ ロード バランシングに関する制約事項

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

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

- ルート マップ アルゴリズムが必要です。
- 最適な結果を得るには、冗長 CSG が必要です。
- 加入者のアドレスの範囲による負荷分散のスタティック プロビジョニングが必要です。
- 簡易な IP Access Control List（ACL; アクセス コントロール リスト）だけがサポートされます。

- VSA 関連付けが使用されている場合は、IOS SLB が、関連付け情報をアクティブな RADIUS ロード バランシング デバイスにだけ保存し、バックアップ RADIUS ロード バランシング デバイスには保存しません。バックアップ RADIUS ロード バランシング デバイスは、アクティブな RADIUS ロード バランシング デバイスから VSA 関連付け情報を受信しません。
- すべての Accounting-Request メッセージおよび Access-Accept メッセージには、RADIUS 割り当ての Framed-ip-address アトリビュートを含める必要があります。また、各加入者フローの発信元 IP アドレスは、Access-Accept メッセージの Framed-ip-address アトリビュートの値と一致する必要があります。
- RADIUS アカウンティングを RADIUS クライアント（一般的に Network Access Server（NAS））でイネーブルにする必要があります。
- SLB サーバ ファーム コンフィギュレーション モードで **predictor route-map** コマンドを指定する場合、SLB サーバ ファーム コンフィギュレーション モードまたは実サーバ コンフィギュレーション モードで他のコマンドは使用できません。

VSA 関連付けに関する制約事項

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

GPRS 用の RADIUS ロード バランシングに関する制約事項

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

CDMA2000 用の RADIUS ロード バランシングに関する制約事項

- 加重ラウンド ロビン アルゴリズムが必要です。
- フラグメント化された RADIUS パケットはサポートされません。
- モバイル ネットワークのすべての加入者には、モバイル ワイヤレス ネットワーク内でルーティング可能な、固有の IP アドレスを割り当てる必要があります（つまり、重複する IP アドレスがない状態）。
- User-Name アトリビュートは 1 人の加入者、または、多くても極少数の加入者に対応付ける必要があります。そうしなかった場合は、予想外に大きな負荷が 1 つの SSG にかかる可能性があります。

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

Home Agent Director に関する制約事項

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

HTTP プローブに関する制約事項

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

UDP プローブに関する制約事項

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

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

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

ASN Release 6 ロード バランシングに関する制約事項

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

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

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

Cisco IOS SLB に関する情報

IOS SLB を設定するには、次の概念を理解する必要があります。

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

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

IOS SLB の利点

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

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

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

さらに、スケーラビリティ、可用性、およびメンテナンス容易性を向上します。

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

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

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

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

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

Cisco IOS SLB 機能

Cisco IOS SLB には次のようなサブ機能が含まれています。

ルーティング機能

IOS SLB には次のルーティング機能があります。

サーバ ロード バランシングのアルゴリズム

IOS SLB には次のロード バランシング アルゴリズムがあります。

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

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

加重ラウンド ロビン アルゴリズム

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

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

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

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

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

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

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

加重最小接続アルゴリズム

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

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

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

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

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

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

ルート マップ アルゴリズム

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

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

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

バインディング ID のサポート

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

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

Client-Assigned ロード バランシング

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

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

接続のレート制限

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

コンテンツ フロー モニタのサポート

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

TCP 接続コンテキストの遅延削除

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

ファイアウォール ロード バランシング

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

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

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

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

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

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

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

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

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

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

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

GTP IMSI スティッキ データベース

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

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

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

Home Agent Director

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

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

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

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

インターフェイス認識

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

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

最大接続

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

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

複数ファイアウォール ファームのサポート

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

ネットワーク アドレス変換

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

ここでは、次の内容について説明します。

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

セッション リダイレクション

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

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

dispatched モード

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

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

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

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

directed モード

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

IOS SLB は次の種類の NAT をサポートします。

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

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

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

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

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

サーバ NAT

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

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

クライアント NAT

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

スタティック NAT

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

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

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

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

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

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

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

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

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

ステップ 1 パケットは実サーバと一致しますか。

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

ステップ 2 パケットは既存の接続と一致しますか。

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

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

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

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

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

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

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

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

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

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

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

サーバ ポート変換

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

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

ポートバインド サーバ

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

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

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

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

ルート ヘルス インジェクション

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

スティッキ接続

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

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

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

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

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

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

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

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

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

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

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

TCP セッションの再割り当て

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

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

透過的 Web キャッシュ ロード バランシング

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

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

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

セキュリティ機能

IOS SLB には次のセキュリティ機能があります。

- 「代替 IP アドレス」（P.23）
- 「サーバ ファームおよびファイアウォール ファームに対する攻撃の回避」（P.23）
- 「スロー スタート」（P.23）
- 「SynGuard」（P.24）

代替 IP アドレス

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

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

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

サーバ ファームおよびファイアウォール ファームに対する攻撃の回避

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

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

スロー スタート

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

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

SynGuard

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

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

サーバ障害の検出機能および回復機能

IOS SLB には、次のサーバ障害検出機能と回復機能があります。

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

自動サーバ障害検出

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

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

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

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

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

自動アンフェイル

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

バックアップ サーバ ファーム

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

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

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

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

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

Cisco IOS SLB 用の DFP

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

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

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

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

詳細については、次のセクションを参照してください。

- 「DFP および GPRS ロード バランシング」（P.26）

- 「DFP および Home Agent Director」（P.26）

DFP および GPRS ロード バランシング

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

（既存の PDP コンテキスト数）/（最大 PDP コンテキスト数）

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

（既存の PDP コンテキスト）/10000 = 低い GGSN 加重

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

DFP および Home Agent Director

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

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

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

GGSN-IOS SLB メッセージング

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

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

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

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

仮想サーバの INOP_REAL 状態

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

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

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

プローブ

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

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

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

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

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

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

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

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

サーバ ロード バランシングのプローブ

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

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

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

ファイアウォール ロード バランシングのプローブ

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

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

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

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

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

プロトコル サポート機能

IOS SLB には次のプロトコル サポート機能があります。

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

プロトコル サポート

IOS SLB は次のプロトコルをサポートします。

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

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

AAA ロード バランシング

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

また、次の RADIUS ロード バランシング機能があります。

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

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

オーディオおよびビデオのロード バランシング

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

VPN サーバ ロード バランシング

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

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

冗長機能

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

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

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

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

ステートレス バックアップ

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

ステートフル バックアップ

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

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

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

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

アクティブ スタンバイ

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

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

Exchange Director 機能

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

ASN ロード バランシング

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

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

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

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

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

GPRS ロード バランシング

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

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

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

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

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

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

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

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

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

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

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

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

表 1　PDP 作成応答原因コードと対応する IOS SLB アクション

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

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

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

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

GTP ロード バランシングに対するデュアルスタック サポート

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

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

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

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

Home Agent Director

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

Home Agent Director には次の特徴があります。

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

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

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

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

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

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

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

相対的 KAL-AP 負荷値

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

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

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

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

絶対的 KAL-AP 負荷値

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

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

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

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

たとえば、次の設定のサイトがあるとします。

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

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

このサイトの KAL-AP 負荷値は次のようになります。

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

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

RADIUS ロード バランシング

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

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

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

また、次の RADIUS ロード バランシング機能があります。

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

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

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

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

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

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

RADIUS ロード バランシング加速データ プレーン フォワーディング

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

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

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

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

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

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

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

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

Turbo RADIUS ロード バランシング

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

WAP ロード バランシング

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

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

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

冗長ルート プロセッサのステートフル バックアップ

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

フローの永続性

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

IOS SLB 機能の設定方法

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

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

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

IOS SLB を設定するには、次の項の作業を実行します。

必須と任意の IOS SLB 機能の設定方法

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

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

サーバ ファームと実サーバの設定方法

サーバ ファームと実サーバを設定するには、この必須作業を実行します。

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

手順の概要

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

手順の詳細

	コマンド	説明
ステップ 1	**enable** 例： Router> **enable**	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： Router# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip slb serverfarm** *server-farm* 例： Router(config)# **ip slb serverfarm PUBLIC**	サーバ ファームの定義を IOS SLB 設定に追加し、サーバ ファーム コンフィギュレーション モードを開始します。
ステップ 4	**access** *interface* 例： Router(config-slb-sfarm)# **access GigabitEthernet 0/1.1**	（任意）サーバ ファームのアクセス インターフェイスまたはサブインターフェイスを設定します。
ステップ 5	**bindid** [*bind-id*] 例： Router(config-slb-sfarm)# **bindid 309**	（任意）Dynamic Feedback Protocol（DFP）に使用されるサーバ ファームのバインド ID を指定します。 **（注）** GPRS ロード バランシングおよび Home Agent Director は、このコマンドをサポートしません。
ステップ 6	**nat** {**client** *pool* | **server**} 例： Router(config-slb-sfarm)# **nat server**	（任意）サーバ ファームで、ネットワーク アドレス変換（NAT）クライアントの変換モードまたは NAT サーバ アドレス変換モードを設定します。 同じ仮想サーバに関連付けられたすべての IPv4 または IPv6 サーバ ファームは、同じ NAT 設定にする必要があります。

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

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

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

仮想サーバの設定方法

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

手順の概要

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

   または

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

手順の詳細

	コマンド	説明
ステップ 1	**enable** 例： Router> **enable**	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： Router# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip slb vserver** *virtual-server* 例： Router(config)# **ip slb vserver PUBLIC_HTTP**	仮想サーバを指定し、仮想サーバ コンフィギュレーション モードを開始します。
ステップ 4	**virtual** *ipv4-address* [*ipv4-netmask* [**group**]] {**esp** | **gre** | *protocol*} または **virtual** *ipv4-address* [*ipv4-netmask* [**group**]] [**ipv6** *ipv6-address* [**prefix** *ipv6-prefix*]] {**tcp** | **udp**} [*port* | **any**] [**service** *service*] 例： Router(config-slb-vserver)# **virtual 10.0.0.1 tcp www**	仮想サーバの IP アドレス、接続の種類、およびオプションの TCP またはユーザ データグラム プロトコル（UDP）のポート番号を指定し、Internet Key Exchange（IKE; インターネット キー エクスチェンジ）または Wireless Session Protocol（WSP）の設定、およびサービスのカップリングを指定します。 **（注）** RADIUS ロード バランシングの場合、**service radius** キーワード オプションを指定します。 **（注）** ASN ロード バランシングの場合、**service asn** キーワード オプションを指定します。 **（注）** GPRS ロード バランシングの場合： – 仮想 GGSN IP アドレスを仮想サーバとして指定し、**udp** キーワード オプションを指定します。 – GTP v1 および GTP v2 セッションの負荷を分散するには、GGSN および SGSN が ETSI 標準に準拠している場合、ポート番号 2123 を指定します。また、全ポート仮想サーバ（つまり、すべてのポート宛てのフローを受け入れる仮想サーバ）を設定するには、ポート番号 0 または **any** を指定します。 – GTP v0 セッションの負荷を分散するには、GGSN および SGSN が ETSI 標準に準拠している場合、ポート番号 3386 を指定します。また、全ポート仮想サーバを設定するには、ポート番号 0 または **any** を指定します。 – GTP Cause Code Inspection *なし*の GPRS ロード バランシングをイネーブルにするには、**service gtp** キーワード オプションを指定します。 – GTP Cause Code Inspection *あり*の GPRS ロード バランシングをイネーブルにするには、**service gtp-inspect** キーワード オプションを指定します。 – GTP ロード バランシングに対するデュアルスタック サポートの場合は、仮想サーバの IPv4 アドレス、IPv6 アドレス、およびオプションの IPv6 プレフィクスを指定します。

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

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

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

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

仮想サーバの確認方法

仮想サーバを確認するには、次の任意作業を実行します。

手順の概要

1. **show ip slb vservers**

手順の詳細

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

```
Router# show ip slb vservers

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

サーバ ファームの確認方法

サーバ ファームを確認するには、次の任意作業を実行します。

手順の概要

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

手順の詳細

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

```
Router# show ip slb real

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

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

```
Router# show ip slb serverfarm

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

クライアントの確認方法

クライアントを確認するには、次の任意作業を実行します。

手順の概要

1. **show ip slb conns**

手順の詳細

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

```
Router# show ip slb conns

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

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

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

IOS SLB 接続の確認方法

IOS SLB 接続を確認するには、次の任意作業を実行します。

手順の概要

1. **show ip slb stats**

手順の詳細

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

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

```
Router# show ip slb stats

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

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

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

ファイアウォール ロード バランシングの設定方法

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

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

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

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

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

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

ファイアウォール ファームの設定方法

ファイアウォール ファームを設定するには、次の必須作業を実行します。

手順の概要

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

手順の詳細

	コマンド	目的
ステップ 1	**enable** 例： Router> **enable**	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： Router# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip slb firewallfarm** *firewall-farm* 例： Router(config)# **ip slb firewallfarm FIRE1**	ファイアウォール ファームの定義を IOS SLB 設定に追加し、ファイアウォール ファーム コンフィギュレーション モードを開始します。
ステップ 4	**real** *ip-address* 例： Router(config-slb-fw)# **real 10.1.1.1**	ファイアウォール ファームのメンバとして、ファイアウォールを IP アドレスで指定し、実サーバ コンフィギュレーション モードを開始します。
ステップ 5	**probe** *probe* 例： Router(config-slb-fw-real)# **probe FireProbe**	プローブをファイアウォールに関連付けます。
ステップ 6	**weight** *setting* 例： Router(config-slb-fw-real)# **weight 24**	（任意）ファイアウォールの作業負荷容量を指定します。ファイアウォール ファーム内の他のファイアウォールと相対的な値です。
ステップ 7	**inservice** 例： Router(config-slb-fw-real)# **inservice**	ファイアウォールをファイアウォール ファームと IOS SLB で使用できるようにします。
ステップ 8	**access** [**source** *source-ip netmask* | **destination** *destination-ip netmask* | **inbound** {*inbound-interface* | **datagram connection**} | **outbound** *outbound-interface*] 例： Router(config-slb-fw)# **access destination 10.1.6.0 255.255.255.0**	（任意）特定のフローをファイアウォール ファームにルーティングします。

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

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

ファイアウォール ファームの確認方法

ファイウォール ファームを確認するには、次の任意作業を実行します。

手順の概要

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

手順の詳細

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

```
Router# show ip slb real

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

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

```
Router# show ip slb firewallfarm

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

ファイアウォール接続の確認方法

ファイアウォール接続を確認するには、次の任意作業を実行します。

手順の概要

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

手順の詳細

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

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

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

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

```
Router# show ip slb stats

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

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

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

```
Router# show ip slb reals detail

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

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

```
Router# show ip slb conns

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

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

プローブの設定方法

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

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

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

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

カスタム UDP プローブの設定方法

カスタム UDP プローブを設定するには、次の作業を実行します。

手順の概要

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

手順の詳細

	コマンド	説明
ステップ 1	**enable** 例： Router> **enable**	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： Router# **configure terminal**	グローバル コンフィギュレーション モードを開始します。

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

DNS プローブの設定方法

DNS プローブを設定するには、次の作業を実行します。

手順の概要

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

手順の詳細

	コマンド	説明
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip slb probe** *probe* **dns** 例： `Router(config)# ip slb probe PROBE4 dns`	IOS SLB プローブ名を設定し、DNS プローブ コンフィギュレーション モードを開始します。
ステップ 4	**address** [*ip-address* [**routed**]] 例： `Router(config-slb-probe)# address 10.1.10.1`	（任意）DNS プローブを送信する IP アドレスを設定します。
ステップ 5	**faildetect** *number-of-probes* 例： `Router(config-slb-probe)# faildetect 16`	（任意）実サーバまたはファイアウォールの障害の原因となる連続無応答 DNS プローブの数を指定します。
ステップ 6	**interval** *seconds* 例： `Router(config-slb-probe)# interval 11`	（任意）DNS プローブ送信タイマーを設定します。
ステップ 7	**lookup** *ip-address* 例： `Router(config-slb-probe)# lookup 10.1.10.1`	（任意）DNS サーバがドメイン ネーム解決要求に対する応答で返す必要がある実サーバの IP アドレスを設定します。

HTTP プローブの設定方法

HTTP プローブを設定するには、次の作業を実行します。

手順の概要

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

手順の詳細

	コマンド	説明
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip slb probe** *probe* **http** 例： `Router(config)# ip slb probe PROBE2 http`	IOS SLB プローブ名を設定し、HTTP プローブ コンフィギュレーション モードを開始します。
ステップ 4	**address** [*ip-address* [**routed**]] 例： `Router(config-slb-probe)# address 10.1.10.1`	（任意）HTTP プローブの送信先 IP アドレスを設定します。
ステップ 5	**credentials** {*username* [*password*]} 例： `Router(config-slb-probe)# credentials Username1 password`	（任意）HTTP プローブのヘッダー値を設定します。

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

ping プローブの設定方法

ping プローブを設定するには、次の作業を実行します。

手順の概要

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

手順の詳細

	コマンド	説明
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip slb probe** *probe* **ping** 例： `Router(config)# ip slb probe PROBE1 ping`	IOS SLB プローブ名を設定し、ping プローブ コンフィギュレーション モードを開始します。
ステップ 4	**address** [*ip-address* [**routed**]] 例： `Router(config-slb-probe)# address 10.1.10.1`	（任意）ping プローブの送信先 IP アドレスを設定します。
ステップ 5	**faildetect** *number-of-pings* 例： `Router(config-slb-probe)# faildetect 16`	（任意）連続して ACK が受信されない ping プローブの数を指定します。この数を超えると、実サーバまたはファイアウォールの障害と見なされます。
ステップ 6	**interval** *seconds* 例： `Router(config-slb-probe)# interval 11`	（任意）ping プローブの送信タイマーを設定します。

TCP プローブの設定方法

TCP プローブを設定するには、次の作業を実行します。

手順の概要

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

手順の詳細

	コマンド	説明
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip slb probe** *probe* **tcp** 例： `Router(config)# ip slb probe PROBE5 tcp`	IOS SLB プローブ名を設定し、TCP プローブ コンフィギュレーション モードを開始します。
ステップ 4	**address** [*ip-address* [**routed**]] 例： `Router(config-slb-probe)# address 10.1.10.1`	（任意）TCP プローブの送信先 IP アドレスを設定します。
ステップ 5	**interval** *seconds* 例： `Router(config-slb-probe)# interval 5`	（任意）TCP プローブの送信タイマーを設定します。
ステップ 6	**port** *port* 例： `Router(config-slb-probe)# port 8`	TCP プローブが接続するポートを設定します。

WSP プローブの設定方法

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

手順の概要

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

手順の詳細

	コマンド	説明
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip slb probe** *probe* **wsp** 例： `Router(config)# ip slb probe PROBE3 wsp`	IOS SLB プローブ名を設定し、WSP プローブ コンフィギュレーション モードを開始します。
ステップ 4	**address** [*ip-address* [**routed**]] 例： `Router(config-slb-probe)# address 10.1.10.1`	（任意）WSP プローブの送信先 IP アドレスを設定します。
ステップ 5	**interval** *seconds* 例： `Router(config-slb-probe)# interval 11`	（任意）WSP プローブ送信タイマーを設定します。
ステップ 6	**url** [*path*] 例： `Router(config-slb-probe)# url http://localhost/test.txt`	（任意）WSP プローブ URL パスを設定します。

プローブの関連付け方法

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

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

（注） WSP プローブをファイアウォールに関連付けることはできません。

手順の概要

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

   または

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

手順の詳細

	コマンド	説明
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip slb firewallfarm** *firewall-farm* または **ip slb serverfarm** *server-farm* 例： `Router(config)# ip slb serverfarm PUBLIC` または `Router(config)# ip slb firewallfarm FIRE1`	ファイアウォール ファームを指定し、ファイアウォール ファーム コンフィギュレーション モードを開始します。 または サーバ ファームを指定し、SLB サーバ ファーム コンフィギュレーション モードを開始します。
ステップ 4	**probe** *probe* 例： `Router(config-slb-sfarm)# probe PROBE1` または `Router(config-slb-fw-real)# probe FireProbe`	プローブをファイアウォール ファームまたはサーバ ファームに関連付けます。

プローブの確認方法

プローブを確認するには、次の任意作業を実行します。

概要手順

1. **show ip slb probe**

詳細手順

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

```
Router# show ip slb probe

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

DFP の設定方法

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

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

手順の概要

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

手順の詳細

	コマンド	説明
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip slb dfp** [**password** [[*encrypt*] *secret-string* [*timeout*]] 例： `Router(config)# ip slb dfp password Password1 360`	Dynamic Feedback Protocol（DFP）を設定し、オプションのパスワードを指定し、DFP コンフィギュレーション モードを開始します。
ステップ 4	**agent** *ip-address port* [*timeout* [*retry-count* [*retry-interval*]]] 例： `Router(config-slb-dfp)# agent 10.1.1.1 2221 30 0 10`	IOS SLB が接続可能な DFP エージェントを特定します。
ステップ 5	IOS SLB を DFP エージェントとして設定します。	IOS SLB を DFP エージェントとして設定するには、Cisco IOS Release 12.2(18)SXB の *DFP Agent Subsystem* 機能のマニュアルを参照してください。

GPRS ロード バランシングの設定作業リスト

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

手順の概要

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

手順の詳細

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

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

GSN アイドル タイマーの設定方法

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

手順の概要

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

手順の詳細

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

GGSN-IOS SLB メッセージング作業リスト

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

手順の概要

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

手順の詳細

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

GPRS ロード バランシング マップの設定方法

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

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

手順の概要

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

手順の詳細

	コマンド	説明
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip slb map** *map-id* **gtp** | **radius**} 例： `Router(config)# ip slb map 1 radius`	IOS SLB GTP マップを設定し、SLB GTP マップ コンフィギュレーション モードを開始します。
ステップ 4	**apn** *string* 例： `Router(config-slb-map-gtp) # apn abc`	グローバル パケット ラジオ サービス（GPRS）ロード バランシングのアクセス ポイント ネーム（APN）とマッチングする ASCII 正規表現ストリングを設定します。

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

KAL-AP エージェント サポートの設定方法

KAL-AP エージェント サポートを設定するには、次の作業を実行します。

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

手順の概要

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

手順の詳細

	コマンド	説明
ステップ 1	**enable** 例： Router> **enable**	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： Router# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip slb capp udp** 例： Router(config)# ip slb capp udp	KAL-AP エージェントをイネーブルにし、SLB Content Application Peering Protocol（CAPP）コンフィギュレーション モードを開始します。
ステップ 4	**peer** [*ip-address*] **port** *port* 例： Router(config-slb-capp)# peer port 6000	（任意）KAL-AP エージェントが接続するポートを指定します。
ステップ 5	**peer** [*ip-address*] **secret** [*encrypt*] *secret-string* 例： Router(config-slb-capp)# peer secret SECRET_STRING	（任意）KAL-AP エージェントのために Message Digest Algorithm Version 5（MD5）認証をイネーブルにします。
ステップ 6	**exit** 例： Router(config-slb-map-gtp)# exit	SLB CAPP コンフィギュレーション モードを終了します。
ステップ 7	**ip slb serverfarm** *server-farm* 例： Router(config)# ip slb serverfarm PUBLIC	サーバ ファームを指定し、SLB サーバ ファーム コンフィギュレーション モードを開始します。
ステップ 8	**kal-ap domain** *tag* 例： Router(config-slb-sfarm)# kal-ap domain chicago-com	（任意）KAL-AP エージェントが仮想サーバの負荷をレポートするとき、ドメイン タグを確認できるようにします。
ステップ 9	**farm-weight** *setting* 例： Router(config-slb-sfarm)# farm-weight 16	（任意）サーバ ファームの負荷値を算出するときに、KAL-AP エージェントが使用する加重を指定します。

RADIUS ロード バランシングの設定作業リスト

RADIUS ロード バランシングを設定するには、次の作業を実行します。

手順の概要

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

手順の詳細

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

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

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

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

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

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

手順の概要

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

手順の詳細

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

RADIUS ロード バランシング マップの設定方法

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

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

手順の概要

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

手順の詳細

	コマンド	説明
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip slb map** *map-id* **radius** 例： `Router(config)# ip slb map 1 radius`	IOS SLB RADIUS マップを設定し、SLB RADIUS マップ コンフィギュレーション モードを開始します。
ステップ 4	**calling-station-id** *string* 例： `Router(config-slb-radius-map) # calling-station-id .919*`	RADIUS ロード バランシングの発信ステーション ID アトリビュートとマッチングする ASCII 正規表現ストリングを設定します。
ステップ 5	**username** *string* 例： `Router(config-slb-map-radius) # )# username ...?525*`	RADIUS ロード バランシングのユーザ名アトリビュートとマッチングする ASCII 正規表現ストリングを設定します。
ステップ 6	**exit** 例： `Router(config-slb-map-gtp) # exit`	SLB RADIUS マップ コンフィギュレーション モードを終了します。
ステップ 7	**ip slb vserver** *virtual-server* 例： `Router(config)# ip slb vserver GGSN_SERVER`	仮想サーバを指定し、仮想サーバ コンフィギュレーション モードを開始します。
ステップ 8	**virtual** *ipv4-address* [*ipv4-netmask* [**group**]] [**ipv6** *ipv6-address* [**prefix** *ipv6-prefix*]] {**tcp** | **udp**} [*port* | **any**] [**service** *service*] 例： `Router(config-slb-vserver) # virtual 10.0.0.1 udp 0 service radius`	仮想サーバの IP アドレス、接続の種類、およびオプションの TCP またはユーザ データグラム プロトコル（UDP）のポート番号を指定し、Internet Key Exchange（IKE; インターネット キー エクスチェンジ）または Wireless Session Protocol（WSP）の設定、およびサービスのカップリングを指定します。 **（注）** RADIUS ロード バランシングの場合、**service radius** キーワード オプションを指定します。
ステップ 9	**serverfarm** *primary-farm* [**backup** *backup-farm* [**sticky**]] [**ipv6-primary** *ipv6-primary-farm* [**ipv6-backup** *ipv6-backup-farm*]] [**map** *map-id* **priority** *priority*] 例： `Router(config-slb-vserver) # serverfarm SF1 backup SF2 map 1 priority 1`	RADIUS マップをサーバ ファームに関連付けます。実サーバ ファームを仮想サーバに関連付け、オプションで、バックアップ サーバ ファームを設定し、バックアップ サーバ ファームでスティッキ接続を使用することを指定します。 **（注）** RADIUS ロード バランシングは **sticky** キーワードをサポートしません。 複数のサーバ ファームを特定の仮想サーバに関連付けるには、**複数の serverfarm** コマンドのそれぞれを一意のマップ ID とプライオリティで設定します（つまり、各マップ ID および各マップ プライオリティは、仮想サーバに関連付けられているすべてのサーバ ファームで固有にする必要があります）。

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

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

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

前提条件

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

手順の概要

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

手順の詳細

	コマンド	説明
ステップ 1	**enable** 例： Router> **enable**	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： Router# **configure terminal**	グローバル コンフィギュレーション モードを開始します。

ステップ 3	**ip slb serverfarm** *server-farm* 例： `Router(config)# ip slb serverfarm PUBLIC`	サーバ ファームを指定し、SLB サーバ ファーム コンフィギュレーション モードを開始します。
ステップ 4	**predictor** [**roundrobin** | **leastconns** | **route-map** *mapname*] 例： `Router(config-slb-sfarm)# predictor route-map map1`	（任意）実サーバを選択する方法を決定するために使用するアルゴリズムを指定します。 Turbo RADIUS ロード バランシングには、**route-map** キーワードおよび *mapname* 引数が必要です。 **predictor route-map** コマンドを指定する場合、SLB サーバ ファーム コンフィギュレーション モードまたは実サーバ コンフィギュレーション モードで他のコマンドは使用できません。
ステップ 5	**exit** 例： `Router(config-slb-sfarm)# exit`	SLB サーバ ファーム コンフィギュレーション モードを終了します。
ステップ 6	**ip slb vserver** *virtual-server* 例： `Router(config)# ip slb vserver RADIUS_AUTH`	仮想サーバを指定し、仮想サーバ コンフィギュレーション モードを開始します。
ステップ 7	**virtual** *ipv4-address* [*ipv4-netmask* [**group**]] [**ipv6** *ipv6-address* [**prefix** *ipv6-prefix*]] {**tcp** | **udp**} [*port* | **any**] [**service** *service*] 例： `Router(config-slb-vserver)# virtual 10.10.10.10 udp 1813 service radius`	仮想サーバの IP アドレス、接続の種類、およびオプションの TCP またはユーザ データグラム プロトコル（UDP）のポート番号を指定し、Internet Key Exchange（IKE; インターネット キー エクスチェンジ）または Wireless Session Protocol（WSP）の設定、およびサービスのカップリングを指定し、SLB 仮想サーバ コンフィギュレーション モードを開始します。 **（注）** RADIUS ロード バランシングの場合、**service radius** キーワード オプションを指定します。
ステップ 8	**serverfarm** *primary-farm* [**backup** *backup-farm* [**sticky**]] [**ipv6-primary** *ipv6-primary-farm* [**ipv6-backup** *ipv6-backup-farm*]] [**map** *map-id* **priority** *priority*] 例： `Router(config-slb-vserver)# serverfarm AAAFARM`	RADIUS マップをサーバ ファームに関連付けます。実サーバ ファームを仮想サーバに関連付け、オプションで、バックアップ サーバ ファームを設定し、バックアップ サーバ ファームでスティッキ接続を使用することを指定します。 **（注）** RADIUS ロード バランシングは **sticky** キーワードをサポートしません。 複数のサーバ ファームを特定の仮想サーバに関連付けるには、**複数の serverfarm** コマンドのそれぞれを一意のマップ ID とプライオリティで設定します（つまり、各マップ ID および各マップ プライオリティは、仮想サーバに関連付けられているすべてのサーバ ファームで固有にする必要があります）。

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

mSEF 用 Exchange Director の設定作業リスト

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

ここでは、次の内容について説明します。

Exchange Director 用の RADIUS の設定

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

手順の概要

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

手順の詳細

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

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

Exchange Director 用のファイアウォールの設定

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

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

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

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

ファイアウォール ファームの設定方法

ファイアウォール ファームを設定するには、次の必須作業を実行します。

手順の概要

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

手順の詳細

	コマンド	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip slb firewallfarm** *firewall-farm* 例： `Router(config)# ip slb firewallfarm FIRE1`	ファイアウォール ファームの定義を IOS SLB 設定に追加し、ファイアウォール ファーム コンフィギュレーション モードを開始します。
ステップ 4	**real** *ip-address* 例： `Router(config-slb-fw)# real 10.1.1.1`	ファイアウォール ファームのメンバとして、ファイアウォールを IP アドレスで指定し、実サーバ コンフィギュレーション モードを開始します。
ステップ 5	**probe** *probe* 例： `Router(config-slb-fw-real) # probe FireProbe`	プローブをファイアウォールに関連付けます。
ステップ 6	**weight** *setting* 例： `Router(config-slb-fw-real) # weight 16`	（任意）ファイアウォールの作業負荷容量を指定します。ファイアウォール ファーム内の他のファイアウォールと相対的な値です。
ステップ 7	**inservice** 例： `Router(config-slb-fw-real) # inservice`	ファイアウォールをファイアウォール ファームと IOS SLB で使用できるようにします。
ステップ 8	**exit** 例： `Router(config-slb-fw-real) # exit`	実サーバ コンフィギュレーション モードを終了します。

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

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

ファイアウォール ファームの確認方法

ファイウォール ファームを確認するには、次の任意作業を実行します。

手順の概要

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

手順の詳細

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

```
Router# show ip slb real

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

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

```
Router# show ip slb firewallfarm

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

ファイアウォール接続の確認方法

ファイアウォール接続を確認するには、次の任意作業を実行します。

手順の概要

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

手順の詳細

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

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

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

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

```
Router# show ip slb stats

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

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

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

```
Router# show ip slb reals detail

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

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

```
Router# show ip slb conns

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

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

プローブの設定方法

プローブを設定するには、次の必須作業を実行します。

手順の概要

1. ファイアウォール ファームの各実サーバにプローブを設定します。

手順の詳細

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

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

ワイルドカード検索の設定方法

ワイルドカード検索を設定するには、次の任意作業を実行します。

手順の概要

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

手順の詳細

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

MLS エントリのプロトコルレベル消去の設定方法

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

手順の概要

1. **mls ip slb purge global**

手順の詳細

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

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

接続消去要求動作の設定方法

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

手順の概要

1. **purge connection**

手順の詳細

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

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

スティッキ接続消去要求動作の設定方法

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

手順の概要

1. **purge sticky**

手順の詳細

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

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

VPN サーバ ロード バランシングの設定作業リスト

VPN サーバ ロード バランシングを設定するには、次の作業を実行します。

手順の概要

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

手順の詳細

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

ASN ロード バランシングの設定作業リスト

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

手順の概要

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

手順の詳細

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

Home Agent Director の設定作業リスト

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

手順の概要

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

手順の詳細

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

NAT の設定方法

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

手順の概要

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

手順の詳細

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

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

スタティック NAT の設定方法

スタティック NAT を設定するには、次の作業を実行します。

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

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

手順の概要

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

手順の詳細

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

ステートレス バックアップの設定作業リスト

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

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

手順の概要

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

手順の詳細

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

ステートレス バックアップ設定の確認方法

ステートレス バックアップ設定を確認するには、次の作業を実行します。

手順の概要

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

手順の詳細

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

```
Router# show ip slb vservers

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

Router# show ip slb vservers detail

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

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

```
Router# show ip slb firewallfarm

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

Router# show ip slb firewallfarm details

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

冗長ルート プロセッサのステートフル バックアップの設定作業リスト

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

手順の概要

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

手順の詳細

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

データベース エントリの設定方法

データベース エントリを設定するには、次の作業を実行します。

手順の概要

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

手順の詳細

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

フラグメント データベース用のバッファの設定方法

フラグメント データベースのバッファを設定するには、次の作業を実行します。

手順の概要

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

手順の詳細

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

データベースとカウンタのクリア方法

データベースおよびカウンタをクリアするには、次の作業を実行します。

手順の概要

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

手順の詳細

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

ワイルドカード検索の設定方法

ワイルドカード検索を設定するには、次の作業を実行します。

手順の概要

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

手順の詳細

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

MLS エントリのプロトコルレベル消去の設定方法

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

手順の概要

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

手順の詳細

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

接続の消去方法と再割り当て方法

接続を消去し、再割り当てするには、次の作業を実行します。

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

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

手順の概要

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

7. **failaction purge**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip slb serverfarm** *server-farm* 例： `Router(config)# ip slb serverfarm PUBLIC`	サーバ ファーム コンフィギュレーション モードを開始します。
ステップ 4	**failaction** [**purge** | **asn purge** | **gtp purge** | **radius reassign**] 例： `Router(config-slb-sfarm)# failaction purge`	実サーバで障害が発生した場合の IOS SLB 動作を設定します。
ステップ 5	**exit** 例： `Router(config-slb-sfarm)# exit`	サーバ ファーム コンフィギュレーション モードを終了します。
ステップ 6	**ip slb firewallfarm** *firewall-farm* 例： `Router(config)# ip slb firewallfarm fire1`	ファイアウォール ファーム コンフィギュレーション モードを開始します。
ステップ 7	**failaction purge** 例： `Router(config-slb-fw)# failaction purge`	ファイアウォールで障害が発生した場合の IOS SLB 動作を設定します。

自動サーバ障害検出のディセーブル方法

自動サーバ障害検出をディセーブルにするには、次の作業を実行します。

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

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip slb serverfarm** *server-farm* 例： `Router(config)# ip slb serverfarm PUBLIC`	サーバ ファーム コンフィギュレーション モードを開始します。
ステップ 4	**real** *ipv4-address* [**ipv6** *ipv6-address*] [*port*] 例： `Router(config-slb-sfarm)# real 10.1.1.1`	サーバ ファームのメンバとして実サーバを指定し、実サーバ コンフィギュレーション モードを開始します。 **（注）** GTP ロード バランシングに対するデュアルスタック サポートの場合は、実サーバの IPv4 アドレスと IPv6 アドレスを指定します。
ステップ 5	**no faildetect inband** 例： `Router(config-slb-real)# no faildetect inband`	自動サーバ障害検出をディセーブルにします。 **（注）** **no faildetect inband** コマンドを使用して自動サーバ障害検出をディセーブルにした場合は、1 つ以上のプローブを設定することを推奨します。 **no faildetect inband** コマンドを指定した場合は、指定された **faildetect numconns** コマンドが無視されます。

Cisco IOS SLB 機能のモニタ方法と保守方法

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

手順の概要

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

手順の詳細

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

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

```
Router# show ip slb conns

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

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

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

```
Router# show ip slb dfp

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

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

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

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

```
Router# show ip slb firewallfarm

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

ステップ 4　show ip slb fragments

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

```
Router# show ip slb fragments

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

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

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

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

ステップ 6　show ip slb map [*map-id*]

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

```
Router# show ip slb map

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

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

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

```
Router# show ip slb natpool

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

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

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

```
Router# show ip slb probe

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

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

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

```
Router# show ip slb reals

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

ステップ 10 **show ip slb replicate**

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

```
Router# show ip slb replicate

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

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

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

```
Router# show ip slb serverfarms

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

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

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

```
Router# show ip slb sessions radius

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

ステップ 13　show ip slb static

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

```
Router# show ip slb static

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

ステップ 14　show ip slb stats

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

```
Router# show ip slb stats

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

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

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

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

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

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

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

```
Router# show ip slb vservers

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

ステップ 17 **show ip slb wildcard**

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

```
Router# show ip slb wildcard

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

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

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

IOS SLB の設定例

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

ここでは、次の設定例について説明します。

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

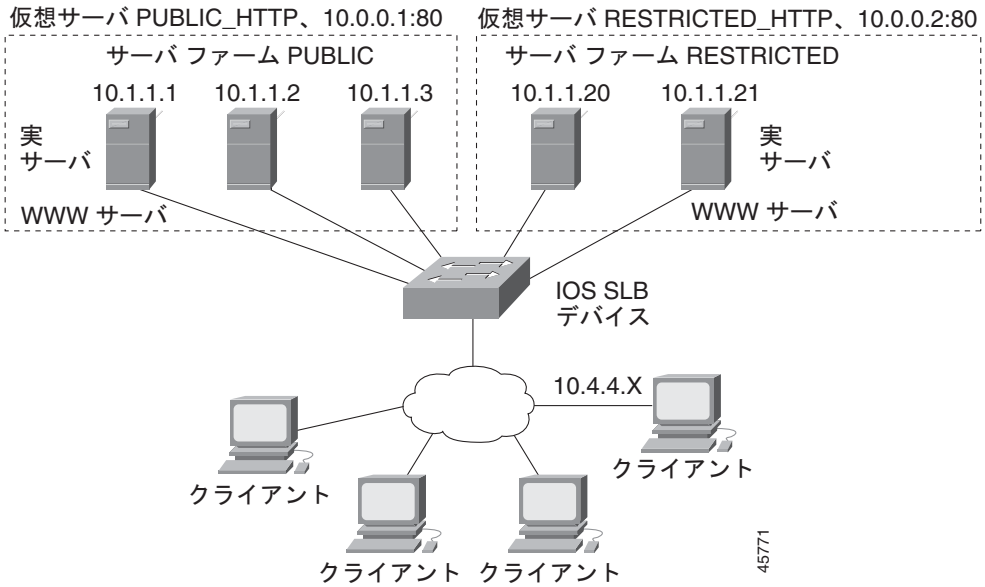
（注） 例に使用される IP アドレスおよびネットワーク アドレスは一般的なものです。実際のネットワークのアドレスで置き換えてください。

例：基本的な IOS SLB ネットワークの設定方法

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

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

図 2　IOS SLB ネットワークの例



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

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

サーバ ファームの設定

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

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

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

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

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

仮想サーバの設定

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

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

限定されたクライアントの設定

次に、仮想サーバ RESTRICTED_HTTP の設定例を示します。

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

例：包括的な IOS SLB ネットワークの設定方法

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

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

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

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

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

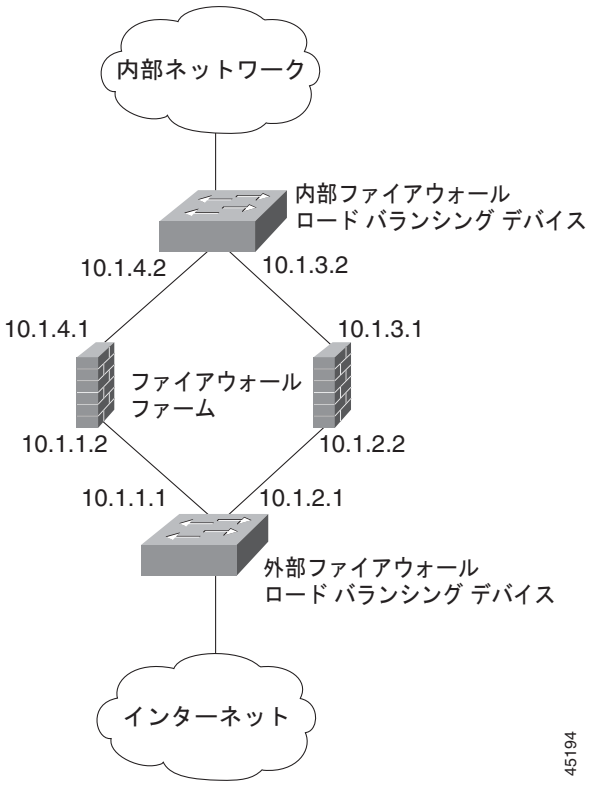
- 「例：基本的なファイアウォール ロード バランシングを使用した IOS SLB の設定方法」（P.125）
- 「例：サーバ ロード バランシングとファイアウォール ロード バランシングを使用した IOS SLB の設定方法」（P.127）
- 「例：複数のファイアウォール ファームを使用した IOS SLB の設定方法」（P.129）
- 「例：二重ファイアウォール ロード バランシング「サンドイッチ」を使用した IOS SLB の設定方法」（P.130）
- 「例：RADIUS ロード バランシング/ファイアウォール ロード バランシング「サンドイッチ」を使用した IOS SLB の設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

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

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

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

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



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

次のファイアウォール ファーム設定例の場合：

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

内部ファイアウォール ロード バランシング デバイス

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

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

外部ファイアウォール ロード バランシング デバイス

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

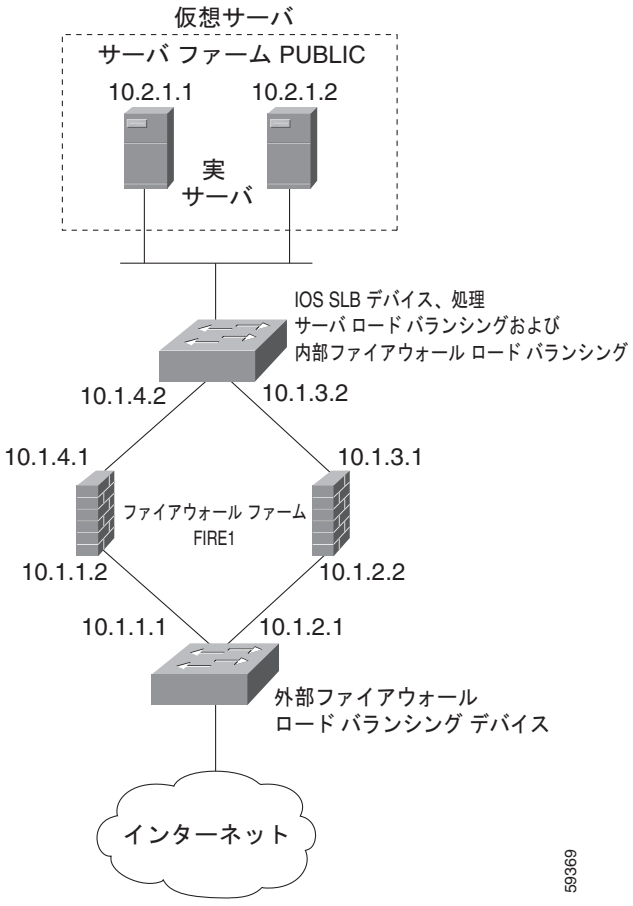
```
!-----Ping probe
ip slb probe PROBE1 ping
!-----IP address of other load-balancing device
  address 10.1.4.2
  faildetect 4
!-----HTTP probe
ip slb probe PROBE2 http
!-----IP address of other load-balancing device
  address 10.1.3.2
  expect status 401
!-----Firewall farm FIRE1
ip slb firewallfarm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

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

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

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

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

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



次のファイアウォール ファーム設定例の場合：

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

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

内部サーバおよびファイアウォール ロード バランシング デバイス

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

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

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

外部ファイアウォール ロード バランシング デバイス

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

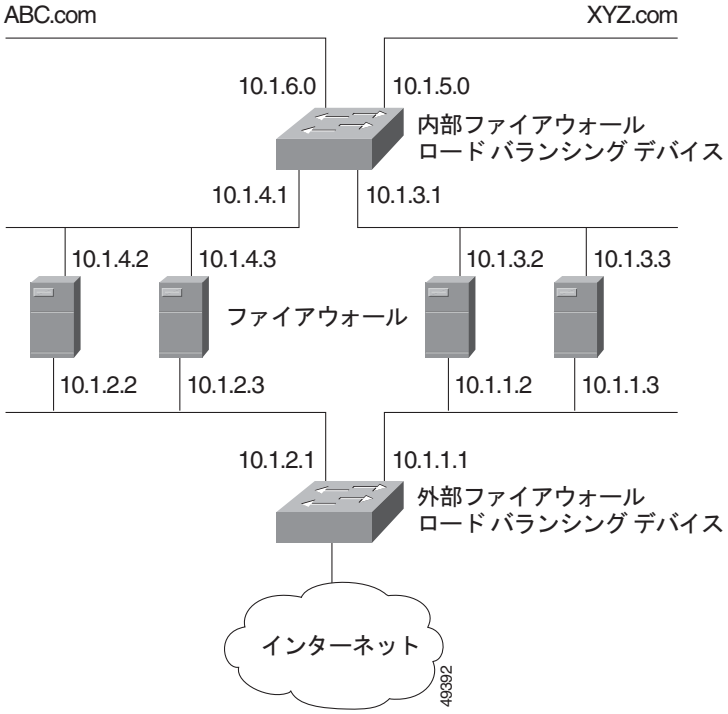
```
ip slb probe ABCPROBE ping
  address 10.1.4.2
  ip slb probe XYZPROBE ping
  address 10.1.3.2
  ip slb firewallfarm FIRE1
  real 10.1.1.2
    probe ABCPROBE
    inservice
    probe XYZPROBE
    inservice
```

例：複数のファイアウォール ファームを使用した IOS SLB の設定方法

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

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

図 5　　複数のファイアウォール ファームを使用した IOS SLB



次のファイアウォール ファーム設定例の場合：

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

内部ファイアウォール ロード バランシング デバイス

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

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

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

外部ファイアウォール ロード バランシング デバイス

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

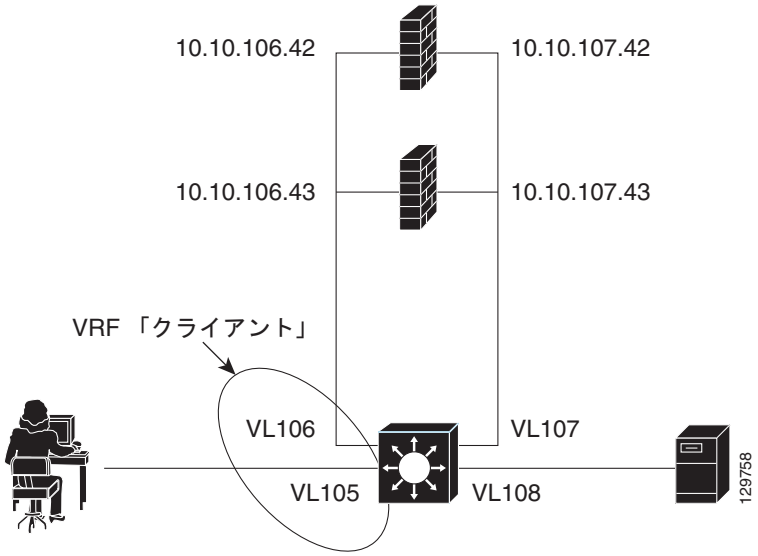
```
ip slb probe ABCPROBE ping
  address 10.1.4.1
ip slb probe XYZPROBE ping
  address 10.1.3.1
ip slb firewallfarm ABCFARM
  access destination 10.1.6.0 255.255.255.0
  inservice
  real 10.1.2.2
    probe ABCPROBE
    inservice
  real 10.1.2.3
    probe ABCPROBE
    inservice
ip slb firewallfarm XYZFARM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

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

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

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

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



次に、図 6 の設定の IOS SLB 設定文を示します。

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

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

例：プローブを使用した IOS SLB の設定方法

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

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

例：ping と HTTP プローブを使用した IOS SLB の設定方法

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

図 7　ping プローブおよび HTTP プローブ トポロジの例

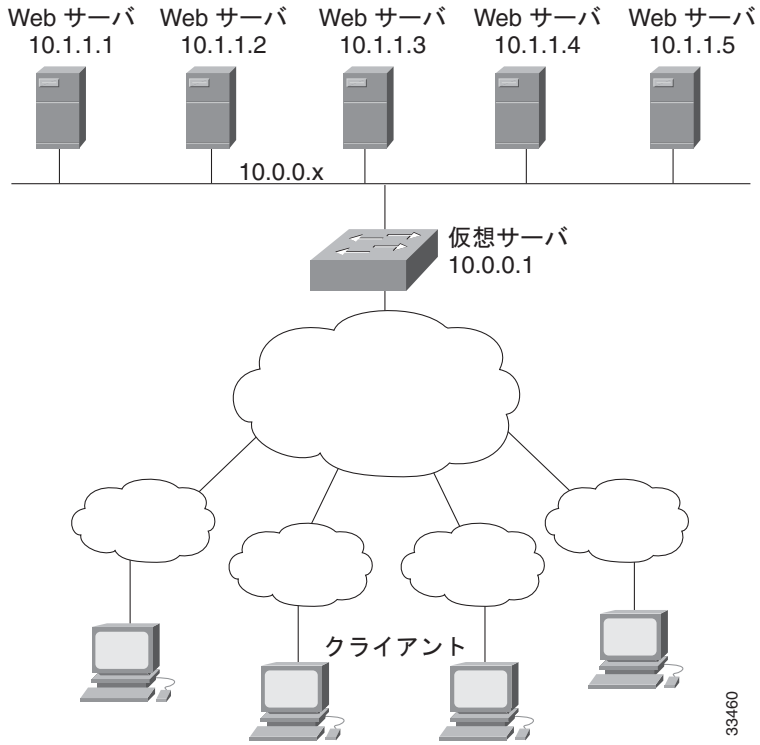


図 7 に示すトポロジは、1 つの仮想サーバにサービスを提供する異機種混合サーバ ファームです。次に、このトポロジの設定文を示します。トポロジには、PROBE1 という ping プローブと PROBE2 という HTTP プローブがあります。

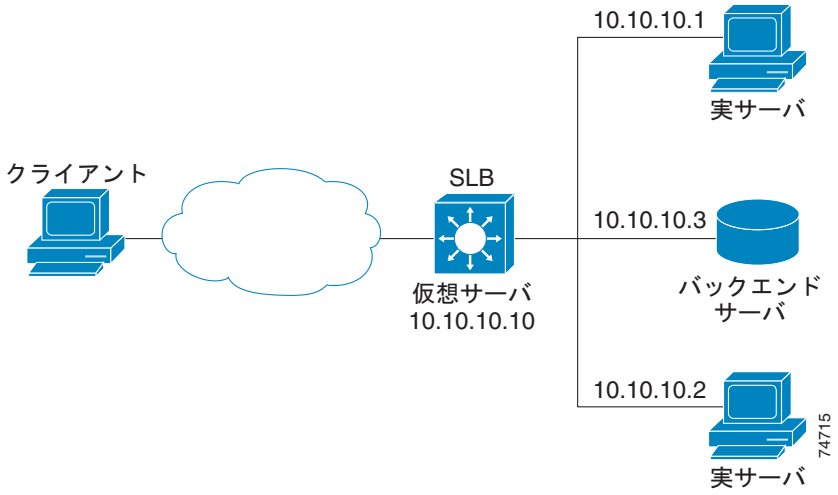
```
! Configure ping probe PROBE1, change CLI to IOS SLB probe configuration mode
ip slb probe PROBE1 ping
! Configure probe to receive responses from IP address 13.13.13.13
  address 13.13.13.13
! Configure unacknowledged ping threshold to 16
  faildetect 16
! Configure ping probe timer interval to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

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

例：ルーテッド プローブを使用した IOS SLB の設定方法

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

図 8　　ルーテッド ping プローブを使用した IOS SLB



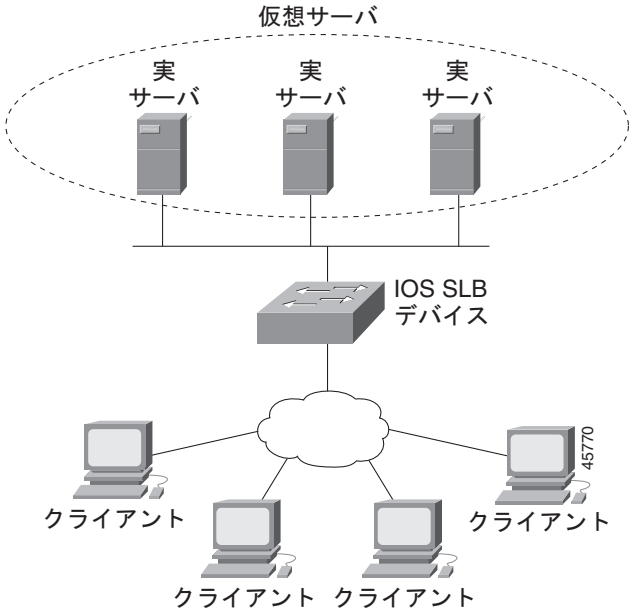
次に、図 8 の設定の IOS SLB 設定文を示します。

```
ip slb probe BACKEND ping
  address 10.10.10.3 routed

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

例：IOS SLB を備えたレイヤ 3 スイッチの設定方法

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

図 9　　IOS SLB のネットワーク設定



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

前述した IOS SLB 機能を備えるネットワーク設定は、次のとおりです。

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

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

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

例：NAT とスタティック NAT を使用した IOS SLB の設定方法

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

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

例：NAT を使用した IOS SLB の設定方法

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

図 10　IOS SLB NAT トポロジの例

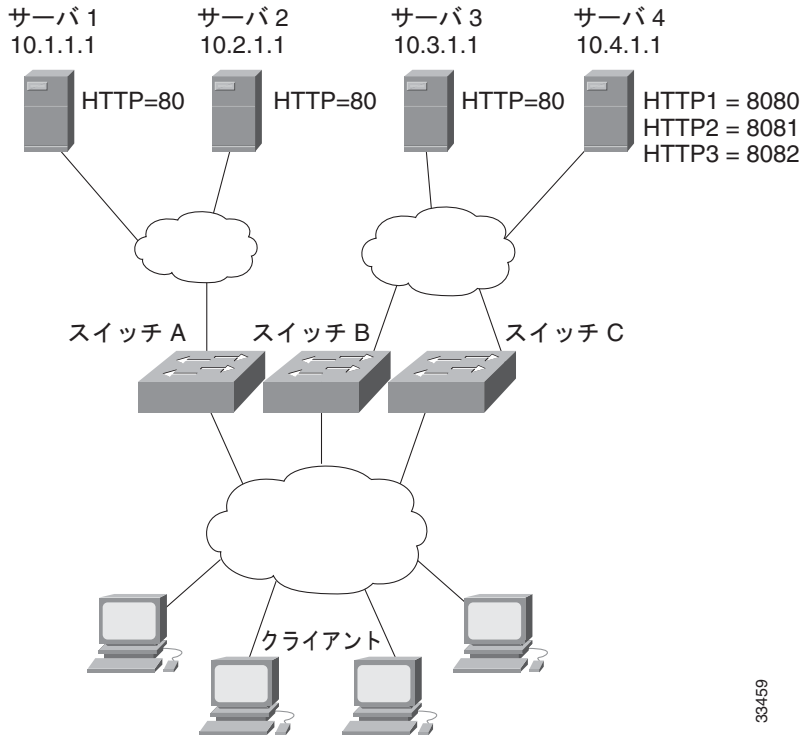


図 10 のトポロジには 4 つの Web サーバがあり、次のように設定されています。

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

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

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

スイッチ A の設定文

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

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

スイッチ B の設定文

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

スイッチ C の設定文

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

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

例：スタティック NAT を使用した IOS SLB の設定方法

次の例では、次のアイテムの設定文を示します。

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

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

例：冗長性を使用した IOS SLB の設定方法

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

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

例：ステートレス バックアップを使用した IOS SLB の設定方法

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

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

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

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

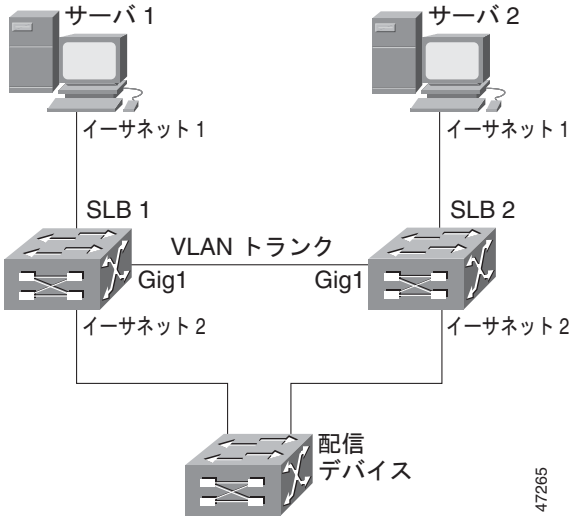
（注） 簡略化するために、この例ではステートフル バックアップを省略しています。ステートフル バックアップを使用する例については、「例：ステートフル バックアップを使用した IOS SLB の設定方法」（P.150）を参照してください。

例：ダイナミック ルーティングとトランキングの設定方法

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

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

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



SLB 1 の設定文

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

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

SLB 2 の設定文

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

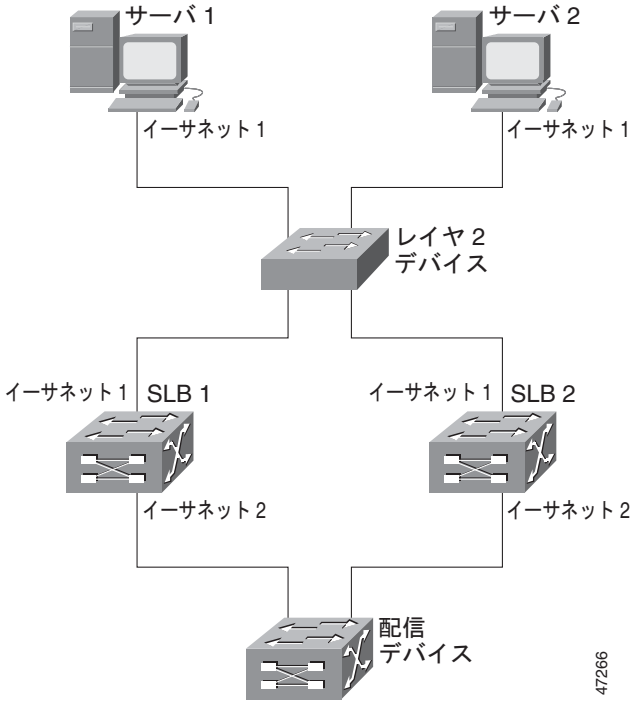
例：ダイナミック ルーティングとトランキングなしの設定方法

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

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

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

図 12　　レイヤ 3 あり、トランキングなしのステートレス バックアップ



SLB 1 の設定文

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

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

SLB 2 の設定文

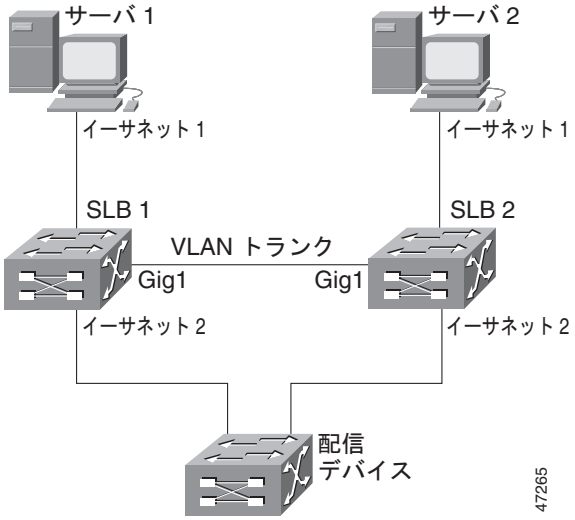
```
ip slb serverfarm SF1
  real 10.10.1.3
    reassign 2
    faildetect numconns 4
    retry 20
    inservice
  real 10.10.1.4
    reassign 2
    faildetect numconns 4
    retry 20
    inservice
ip slb vserver VS1
  virtual 10.10.14.1 tcp www
  serverfarm SF1
  idle 120
  delay 5
  inservice standby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

例：スタティック ルーティングとトランキングの設定方法

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

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

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



SLB 1 の設定文

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

SLB 2 の設定文

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

配信デバイスの設定文

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

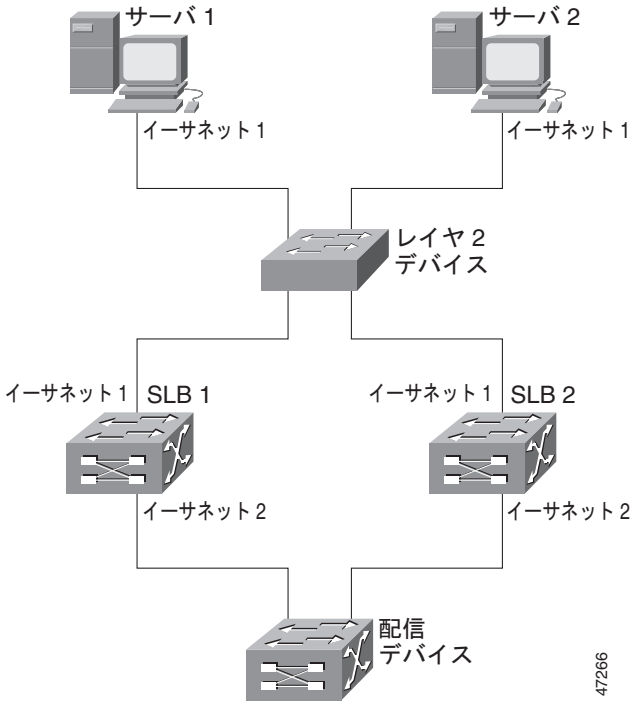
例：スタティック ルーティングとトランキングなしの設定方法

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

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

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

図 14　　レイヤ 2 あり、トランキングなしのステートレス バックアップ



SLB 1 の設定文

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

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

SLB 2 の設定文

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

配信デバイスの設定文

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

例：ステートフル バックアップを使用した IOS SLB の設定方法

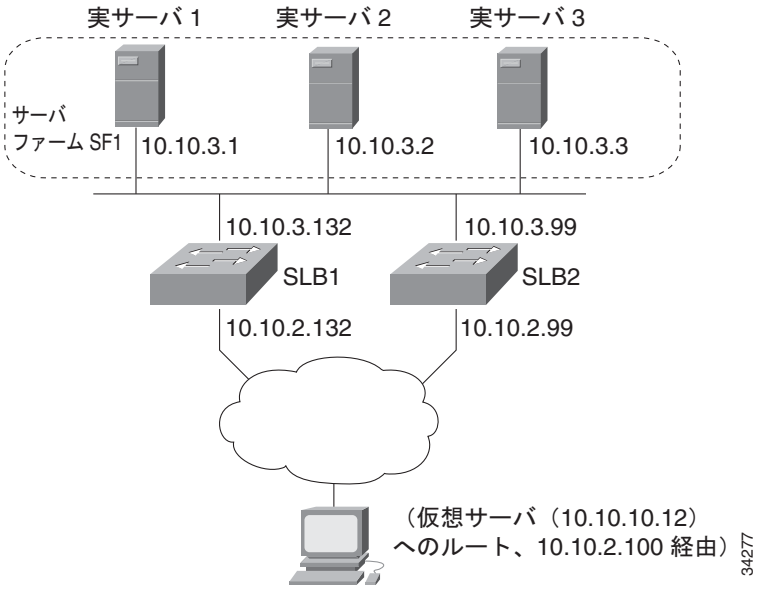
この設定例では、サーバ ファームの一部として設定されている IOS SLB 実サーバ接続と、ステートフル バックアップ スタンバイ接続を使用するファスト イーサネット インターフェイス上の実サーバおよび仮想サーバを中心に説明します。

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

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

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

図 15　　IOS SLB ステートフル環境



スイッチ SLB1 の設定文

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

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

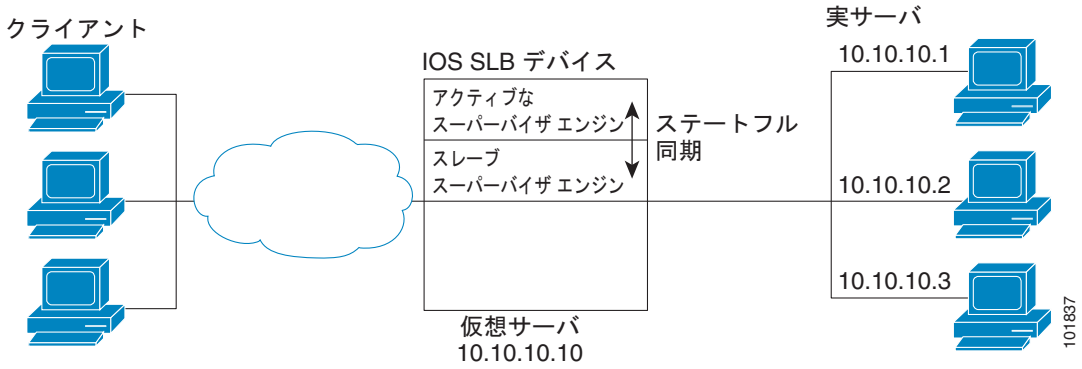
スイッチ SLB2 の設定文

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

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

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

図 16　　冗長ルート プロセッサを使用した IOS SLB



次に、図 16 の設定の IOS SLB 設定文を示します。

```
ip slb replicate slave rate 300

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

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

例：アクティブ スタンバイを使用した IOS SLB の設定方法

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

図 17　　IOS SLB アクティブ スタンバイ

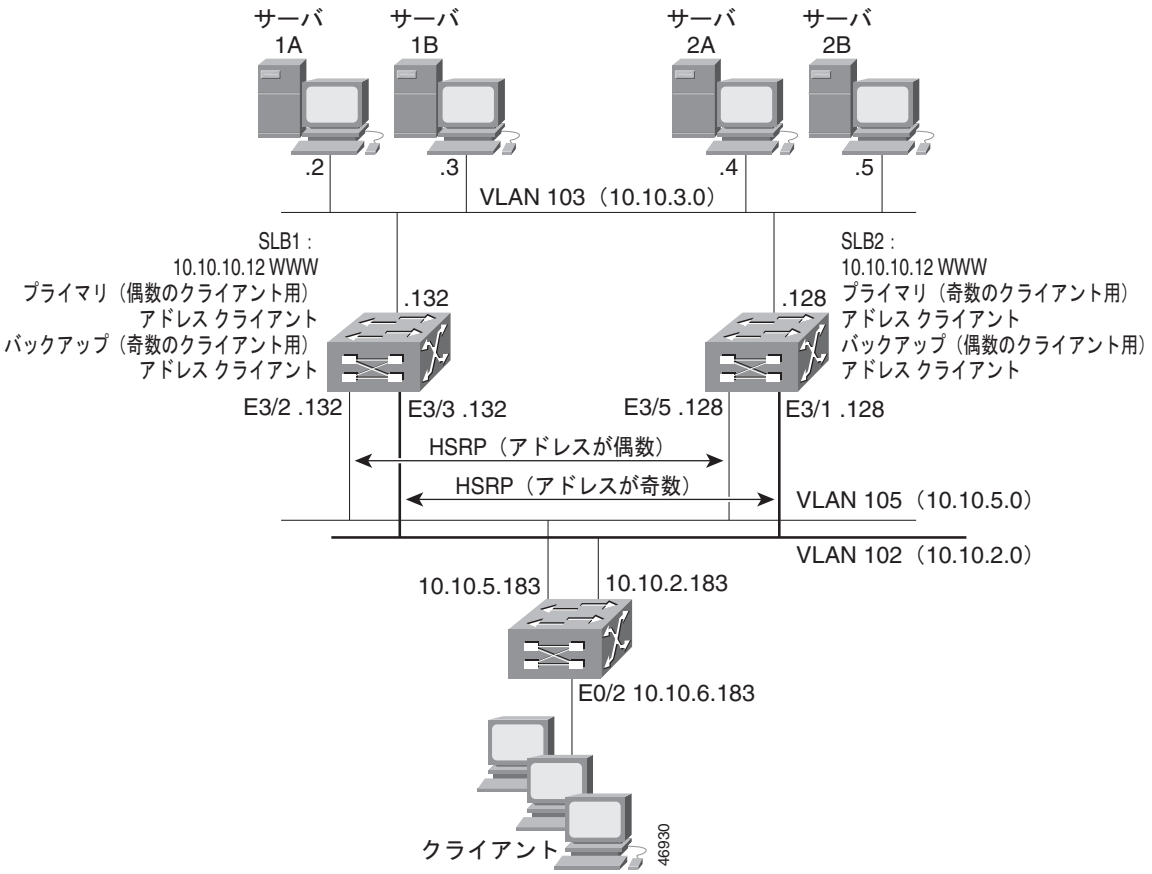


図 17 のネットワーク設定例には、次の特徴があります。

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

SLB 1 の設定文

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

SLB 2 の設定文

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

アクセス ルータの設定文

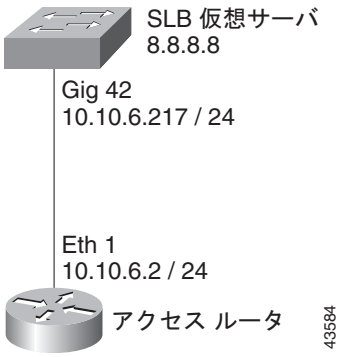
```
interface Ethernet0/0
 ip address 10.10.5.183 255.255.255.0
 no ip directed-broadcast
 no ip route-cache
 no ip mroute-cache
!
interface Ethernet0/1
 ip address 10.10.2.183 255.255.255.0
 no ip directed-broadcast
 no ip route-cache
 no ip mroute-cache
!
interface Ethernet0/2
 ip address 10.10.6.183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

例：スタティック ルートの再配布を使用した IOS SLB の設定方法

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

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

図 18　　スタティック ルートの IOS SLB 再配布



Routing Information Protocol（RIP）

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

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

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

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

Open Shortest Path First（OSPF）

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

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

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

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

Interior Gateway Routing Protocol（IGRP）

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

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

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

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

Enhanced Interior Gateway Routing Protocol（Enhanced IGRP）

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

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

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

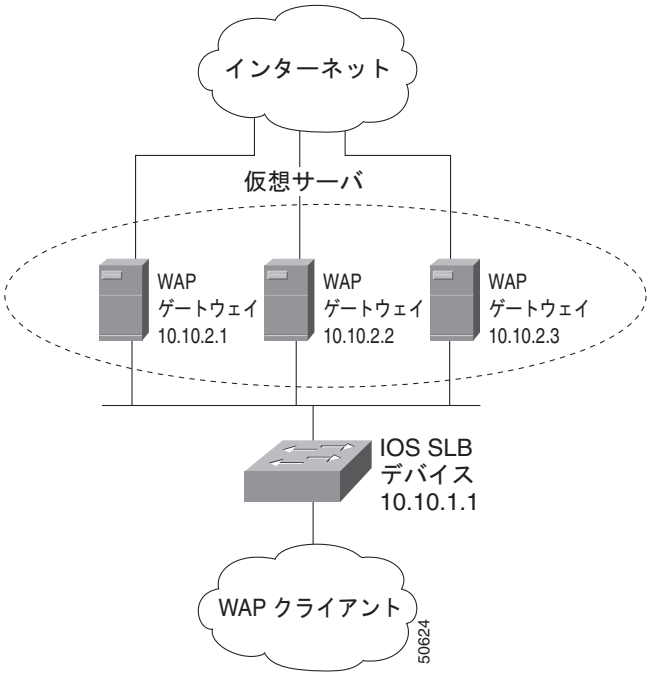
```
router eigrp 666
 network 10.0.0.0
 network 8.0.0.0
```

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

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

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

図 19　　WAP ロード バランシングを使用した IOS SLB



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

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

例：UDP ポート 9201 上での WAP フローのバランス方法

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

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

例：UDP ポート 9203 上での WAP フローのバランス方法

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

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

例：ルート ヘルス インジェクションを使用した IOS SLB の設定方法

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

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

例：1 台ずつの Web サーバを使用した 2 つの分散サイトの設定方法

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

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

図 20　　1 つずつ Web サーバがある 2 つの分散サイト

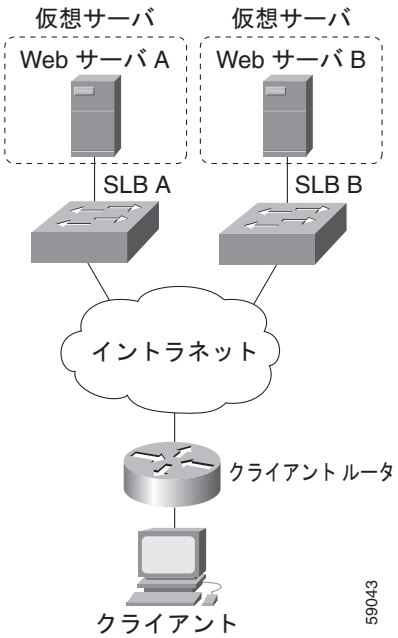


図 20 の両方の Web サーバが動作している場合、クライアント ルータは、両方の IOS SLB デバイスからホスト ルートを受信します。

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

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

例：2 台ずつの Web サーバを使用した 2 つの分散サイトの設定方法

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

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

図 21　　2 つずつ Web サーバがある 2 つの分散サイト

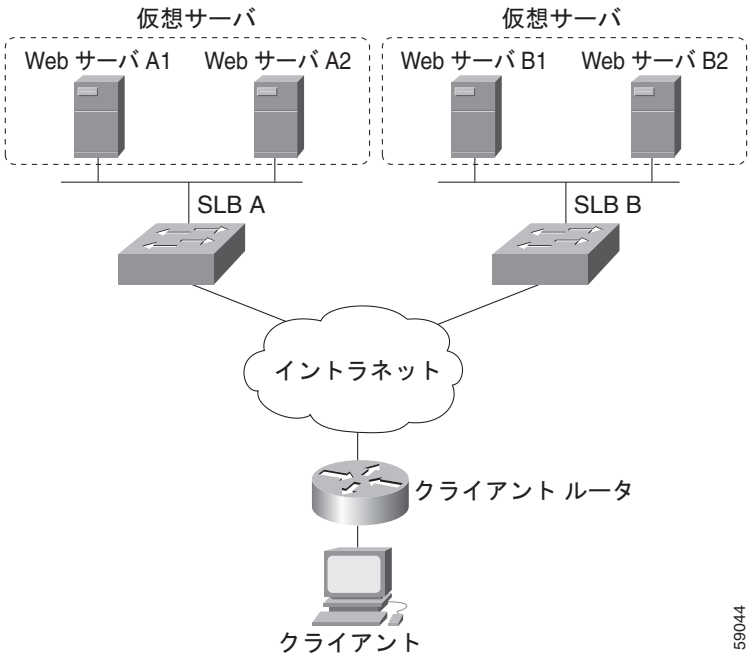


図 21 のすべての Web サーバが動作している場合、クライアント ルータは、両方の IOS SLB デバイスからホスト ルートを受信します。

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

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

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

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

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

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

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

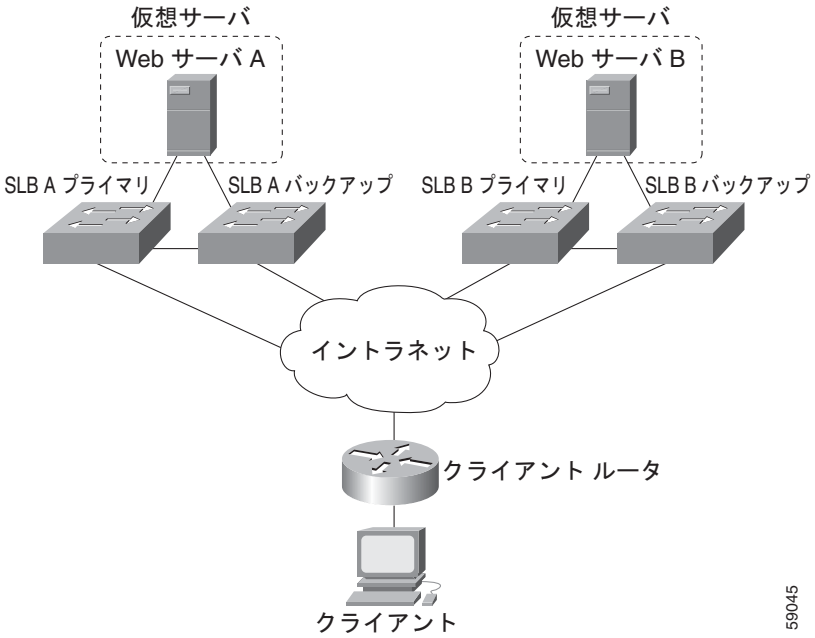


図 22 の両方の Web サーバが動作している場合、クライアント ルータは、SLB A プライマリおよび SLB B プライマリの両方からホスト ルートを受信します。

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

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

例：GPRS ロード バランシングを使用した IOS SLB の設定方法

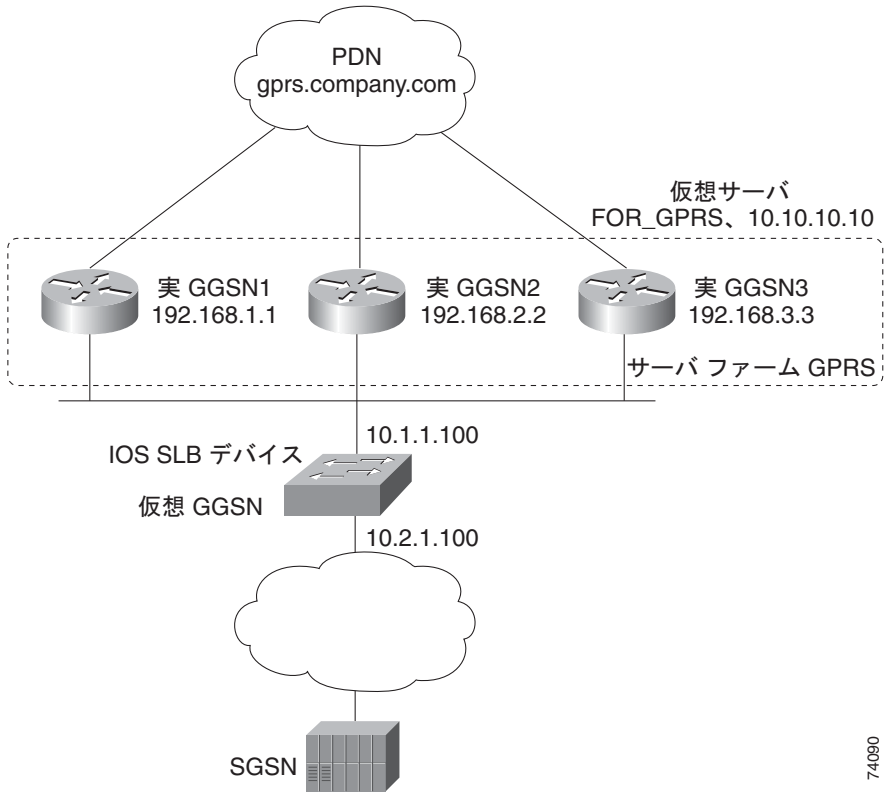
ここでは次の例を紹介し、冗長性を使用するさまざまな IOS SLB 設定を示します。

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

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

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

図 23　GPRS ロード バランシングを使用した IOS SLB



次に、図 23 の設定の設定文を示します。

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

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

IOS SLB の設定文

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

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

GGSN1 の設定文

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

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

GGSN2 の設定文

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

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

GGSN3 の設定文

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

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

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

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

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

IOS SLB の設定文

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

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

GGSN1 の設定文

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

GGSN2 の設定文

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

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

GGSN3 の設定文

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

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

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

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

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

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

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

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

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

IOS SLB の設定文

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

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

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

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

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

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

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

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

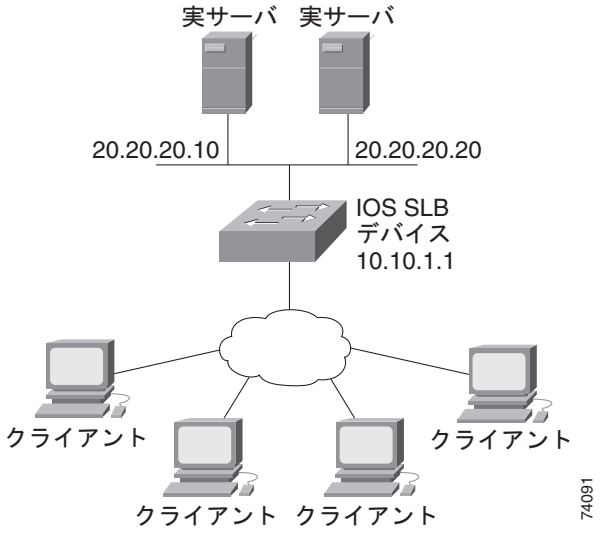
```
ip slb serverfarm SF1
 real 172.16.88.5
  weight 1
  inservice
!
ip slb serverfarm SF2
 real 172.16.88.6
  weight 1
  inservice
!
ip slb serverfarm SF3
 real 172.16.88.7 ipv6 2342:2342:2343:FF04:2388:BB03:3329:8612
  weight 1
  inservice
!
ip slb serverfarm SF4
 real 172.16.88.8 ipv6 2342:2342:2343:FF04:2388:BB03:3423:8912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

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

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

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

図 24　　VPN サーバ ロード バランシングを使用した IOS SLB



次に、図 24 の設定の IOS SLB 設定文を示します。

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

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

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

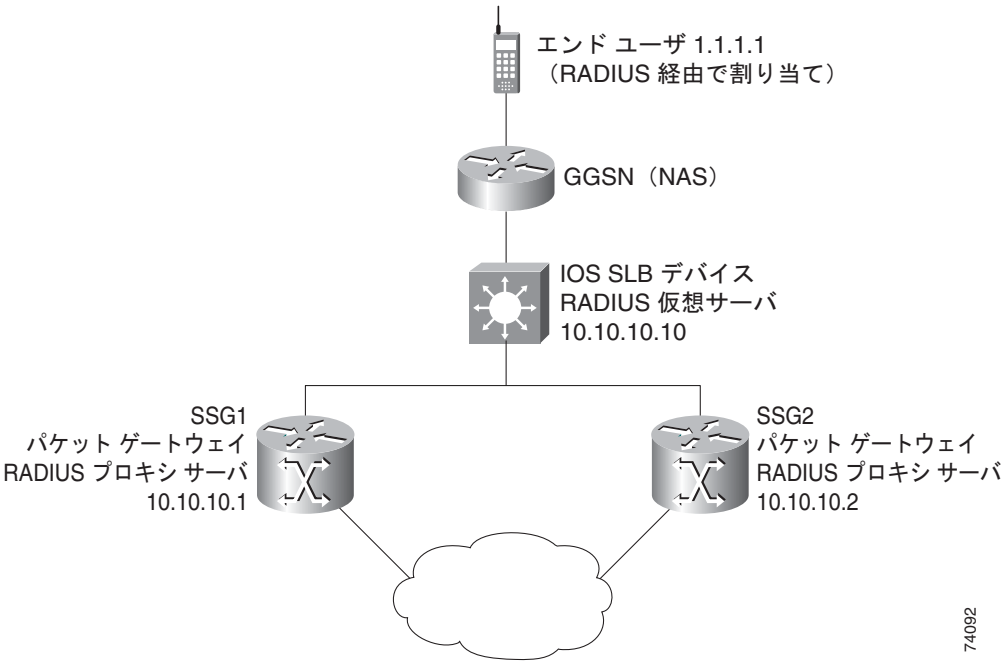
- 「例：GPRS ネットワーク用の RADIUS ロード バランシングを使用した IOS SLB の設定方法」（P.175）
- 「例：簡易 IP CDMA2000 ネットワーク用の RADIUS ロード バランシングを使用した IOS SLB の設定方法」（P.177）
- 「例：Mobile IP CDMA2000 ネットワーク用の RADIUS ロード バランシングを使用した IOS SLB の設定方法」（P.178）
- 「例：複数のサービス ゲートウェイ サーバ ファーム用の RADIUS ロード バランシングを使用した IOS SLB の設定方法」（P.179）
- 「例：RADIUS ロード バランシング/ファイアウォール ロード バランシング「サンドイッチ」を使用した IOS SLB の設定方法」（P.180）
- 「例：RADIUS ロード バランシング マップを使用した IOS SLB の設定方法」（P.182）
- 「例：RADIUS ロード バランシング加速データ プレーン フォワーディングを使用した IOS SLB の設定方法」（P.182）

例：GPRS ネットワーク用の RADIUS ロード バランシングを使用した IOS SLB の設定方法

図 25 に、GPRS ネットワークの一般的な IOS SLB RADIUS ロード バランシング設定を示します。この設定の場合：

- RADIUS 要求の負荷は、SSG RADIUS プロキシ サーバ 10.10.10.1 および 10.10.10.2 の間で分散されます。
- エンドユーザ データ パケットは、IOS SLB デバイスにルーティングされます。
- 1.1.1.0 サブネットからのエンドユーザ データ パケットは、IOS SLB から SSG1 に送信されます。
- 1.1.2.0 サブネットからのエンドユーザ データ パケットは、IOS SLB から SSG2 に送信されます。

図 25　GPRS ネットワーク用の RADIUS ロード バランシングを使用した IOS SLB



次に、図 25 の設定の IOS SLB 設定文を示します。

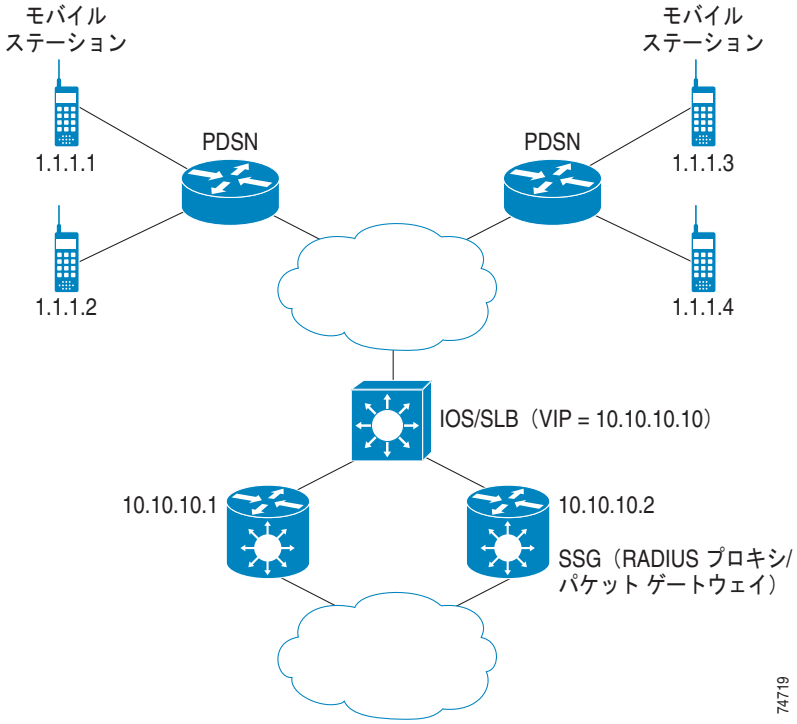
```
ip slb route 1.1.0.0 255.255.0.0 framed-ip
!
ip slb serverfarm SSGFARM
 nat server
 real 10.10.10.1
  inservice
 real 10.10.10.2
  inservice
!
ip slb vserver RADIUS_ACCT
 virtual 10.10.10.10 udp 1813 service radius
 serverfarm SSGFARM
 idle radius request 20
 idle radius framed-ip 7200
 sticky radius framed-ip group 1
 inservice
!
ip slb vserver RADIUS_AUTH
 virtual 10.10.10.10 udp 1812 service radius
 serverfarm SSGFARM
 idle radius request 20
 idle radius framed-ip 7200
 sticky radius framed-ip group 1
 inservice
```

例：簡易 IP CDMA2000 ネットワーク用の RADIUS ロード バランシングを使用した IOS SLB の設定方法

図 26 に、簡易 IP サービスを使用する CDMA2000 ネットワークの一般的な IOS SLB RADIUS ロード バランシング設定を示します。この設定の場合：

- PDSN の RADIUS 仮想サーバの IP アドレスは 10.10.10.10 です。
- RADIUS 要求の負荷は、SSG RADIUS プロキシ サーバ 10.10.10.1 および 10.10.10.2 の間で分散されます。
- エンドユーザ データ パケットは、IOS SLB デバイスにルーティングされます。
- 1.1.0.0 ネットワークからのエンドユーザ データ パケットは、SSG にルーティングされます。

図 26　簡易 IP CDMA2000 ネットワーク用の RADIUS ロード バランシングを使用した IOS SLB



次に、図 26 の設定の IOS SLB 設定文を示します。

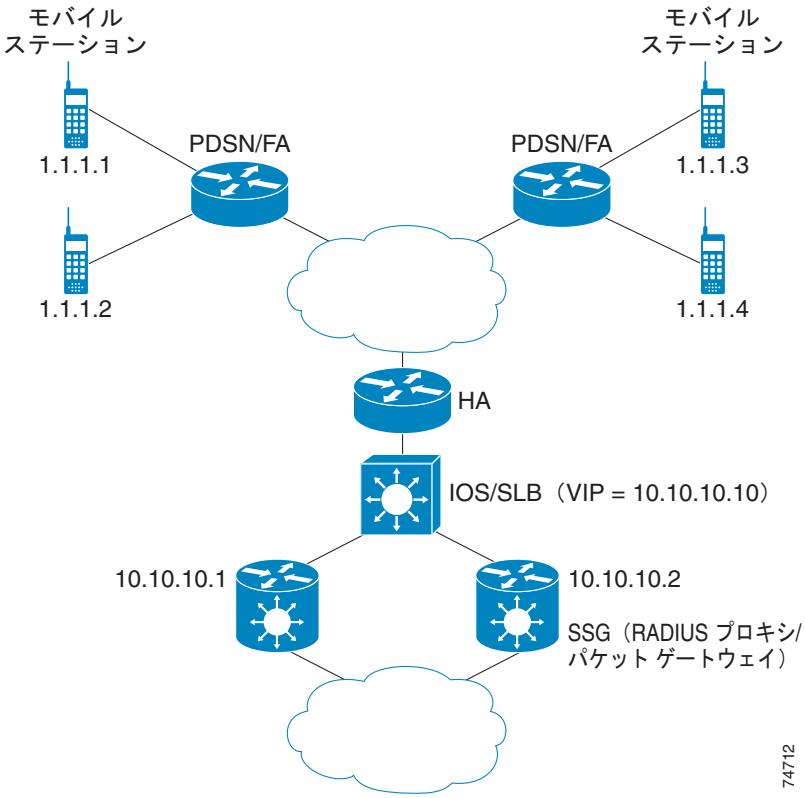
```
ip slb route 1.1.0.0 255.255.0.0 framed-ip
!
ip slb serverfarm SSGFARM
  nat server
  real 10.10.10.1
    inservice
  real 10.10.10.2
    inservice
!
ip slb vserver RADIUS_SIP
  virtual 10.10.10.10 udp 0 service radius
  serverfarm SSGFARM
  idle radius framed-ip 3600
  sticky radius username
  sticky radius framed-ip
  inservice
```

例：Mobile IP CDMA2000 ネットワーク用の RADIUS ロード バランシングを使用した IOS SLB の設定方法

図 27 に、Mobile IP サービスを使用する CDMA2000 ネットワークの一般的な IOS SLB RADIUS ロード バランシング設定を示します。この設定の場合：

- PDSN および HA の RADIUS 仮想サーバの IP アドレスは 10.10.10.10 です。
- RADIUS 要求の負荷は、SSG RADIUS プロキシ サーバ 10.10.10.1 および 10.10.10.2 の間で分散されます。
- エンドユーザ データ パケットは、IOS SLB デバイスにルーティングされます。
- 1.1.0.0 ネットワークからのエンドユーザ データ パケットは、SSG にルーティングされます。

図 27　Mobile IP CDMA2000 ネットワーク用の RADIUS ロード バランシングを使用した IOS SLB



次に、図 27 の設定の IOS SLB 設定文を示します。

```
ip slb route 1.1.0.0 255.255.0.0 framed-ip
!
ip slb serverfarm SSGFARM
  nat server
  real 10.10.10.1
    inservice
  real 10.10.10.2
    inservice
!
ip slb vserver RADIUS_SIP
  virtual 10.10.10.10 udp 0 service radius
  serverfarm SSGFARM
  idle radius framed-ip 3600
```

```
 sticky radius username
 sticky radius framed-ip
 inservice
```

例：複数のサービス ゲートウェイ サーバ ファーム用の RADIUS ロード バランシングを使用した IOS SLB の設定方法

IOS SLB は、次の設定例で複数のサービス ゲートウェイ サーバ ファーム（この例では、SSG のサーバ ファームと CSG のサーバ ファーム）のセットに対するパケット フローの負荷を分散できるようになります。

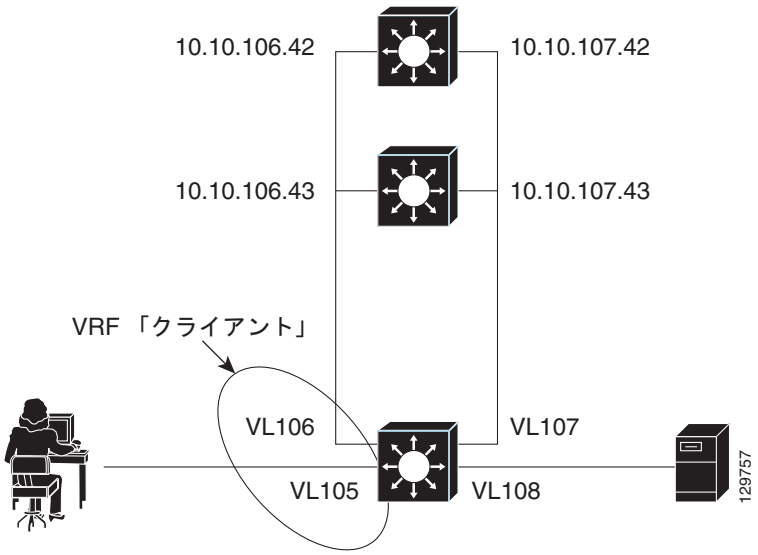
```
ip slb route 1.1.0.0 255.255.0.0 framed-ip
!
ip slb serverfarm SSGFARM
 nat server
 real 10.10.10.1
  inservice
 real 10.10.10.2
  inservice
!
ip slb serverfarm CSGFARM
 nat server
 real 20.20.20.1
  inservice
 real 20.20.20.2
  inservice
!
ip slb vserver SSG_AUTH
 virtual 10.10.10.10 udp 1812 service radius
 serverfarm SSGFARM
 idle radius request 20
 idle radius framed-ip 7200
 sticky radius framed-ip group 1
 access Vlan20 route framed-ip
 inservice
!
ip slb vserver SSG_ACCT
 virtual 10.10.10.10 udp 1813 service radius
 serverfarm SSGFARM
 idle radius request 20
 idle radius framed-ip 7200
 sticky radius framed-ip group 1
 access Vlan20 route framed-ip
 inservice
!
ip slb vserver CSG_ACCT
 virtual 20.20.20.20 udp 1813 service radius
 serverfarm CSGFARM
 idle radius request 25
 idle radius framed-ip 0
 sticky radius framed-ip
 access Vlan30 route framed-ip
 inservice
```

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

図 28 に、1 台の IOS SLB デバイス上の RADIUS ロード バランシング/ファイアウォール ロード バランシング「サンドイッチ」を示します。この設定例の場合：

- RADIUS ロード バランシングの仮想 IP アドレスは 5.5.5.5 です。
- 加入者の framed-IP ネットワークは 1.0.0.0/255.0.0.0 です。
- VL105、VL106、VL107、および VL108 は VLAN です。
- VLAN VL105 に到達する RADIUS 要求の負荷は、10.10.106.42 と 10.10.106.43 の間で分散されます。
- ユーザ トラフィックは、1.0.0.0 サブネットの framed-IP アドレスの割り当てに基づいて、スティッキ接続されます。
- 相手側（10.10.107.42/43）のファイアウォール ロード バランシングによって、加入者へのリターン パス トラフィックは、適切なゲートウェイに配信されます。

図 28　RADIUS ロード バランシング/ファイアウォール ロード バランシング「サンドイッチ」を使用した IOS SLB



次に、図 28 の設定の IOS SLB 設定文を示します。

```
ip vrf client
 rd 0:1
!
ip slb probe P742 ping
 address 10.10.107.42
 interval 120
!
ip slb probe P743 ping
 address 10.10.107.43
 interval 120
!
ip slb route 1.0.0.0 255.0.0.0 framed-ip
ip slb route framed-ip deny
!
ip slb firewallfarm SERVER
```

```
 access inbound Vlan108
 access outbound Vlan107
 inservice
 real 10.10.107.42
  probe P742
  inservice
 real 10.10.107.43
  probe P743
  inservice
 protocol tcp
  sticky 180 destination
 protocol datagram
  sticky 180 destination
 predictor hash address port
!

ip slb serverfarm SF1
 nat server
 access Vlan106
!
 real 10.10.106.42
  inservice
 real 10.10.106.43
  inservice
!
ip slb vserver VS1
 virtual 5.5.5.5 udp 0 service radius
 serverfarm SF1
 sticky radius framed-ip
 access Vlan105 route framed-ip
 access Vlan105
 inservice
!
mls flow ip interface-full
!
!************************************************
!* Switchports, port channels and trunks         *
!* added to vlans 105-108 (left out for brevity) *
!************************************************
!
interface Vlan105
 ip vrf forwarding client
 ip address 10.10.105.2 255.255.255.0
!
interface Vlan106
 ip vrf forwarding client
 ip address 10.10.106.2 255.255.255.0
!
interface Vlan107
 ip address 10.10.107.2 255.255.255.0
!
interface Vlan108
 ip address 10.10.108.2 255.255.255.0
!
ip route 10.10.105.0 255.255.255.0 10.10.107.42
ip route vrf client 10.10.108.0 255.255.255.0 10.10.106.42
```

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

次の設定例では、RADIUS 発信ステーション ID およびユーザ名を使用してサーバ ファームを選択し、RADIUS ロード バランシング仮想サーバの背後で、IOS SLB が複数のサーバ ファームをサポートできるようにします。サーバ ファーム **farm3** は関連マップなしで設定されているため、デフォルト サーバ ファームとして動作します。IOS SLB が他のサーバ ファーム マップのいずれもマッチングできない場合、IOS SLB はデフォルト サーバ ファームに RADIUS 要求を送信します。

```
ip slb serverfarm CSGFARM
 predictor route-map rlb-pbr
ip slb serverfarm AAAFARM
 nat server
 real 10.10.10.1
  inservice
 real 10.10.10.2
  inservice

ip slb vserver RADIUS_ACCT
 virtual 10.10.10.10 udp 1813 service radius
 serverfarm CSGFARM

 radius inject acct 1 key 0 cisco
 inservice

ip slb vserver RADIUS_AUTH
 virtual 10.10.10.10 udp 1812 service radius
 serverfarm AAAFARM
 radius inject auth 1 calling-station-id
 radius inject auth timer 45
 radius inject auth vsa cisco
 inservice

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

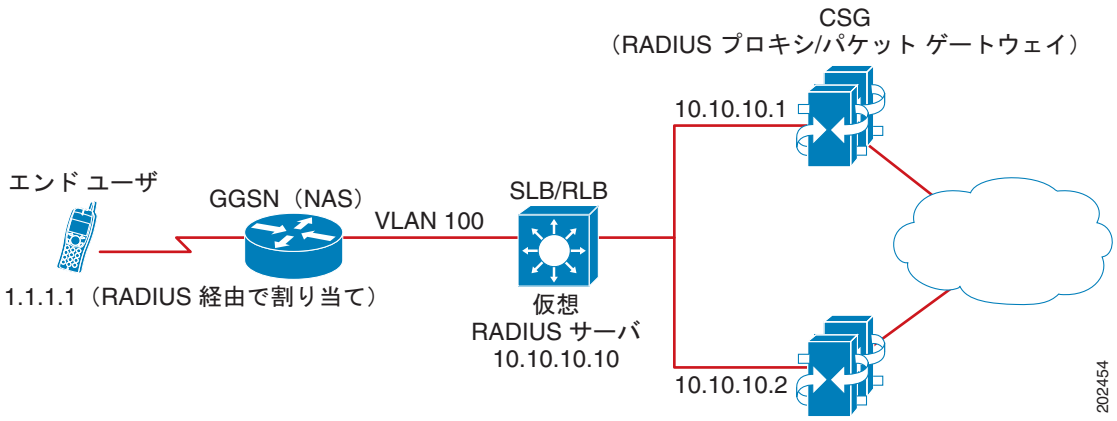
例：RADIUS ロード バランシング加速データ プレーン フォワーディングを使用した IOS SLB の設定方法

この IOS SLB 設定には、次の特徴があります。

- Network Access Server（NAS）デバイスを管理する IP アドレス 10.10.10.10 の仮想 RADIUS サーバが存在します。
- IP アドレス 10.10.10.1 および 10.10.10.2 という 2 つのパケット ゲートウェイがあります。
- 仮想 RADIUS サーバ宛ての RADIUS トラフィックは、ルート マップ **rlb-pbr** に従い、マップ済み framed-IP アドレスに基づいて、パケット ゲートウェイ間で分散されます。

- サーバ ファーム CSGFARM は、ルート マップ **rlb-pbr** の可能な結果に一致する実 IP アドレスを使用して設定されます。
- VLAN 100 に到達するエンドユーザ トラフィックは、アクセス コントロール リスト（ACL）に基づいて、適切な Cisco Content Services Gateway（CSG）にルーティングされます。
  - ACL 1 は、末尾が奇数の IP アドレスを、パケット ゲートウェイ 10.10.10.1 の背後にある CSG に送信します。
  - ACL 2 は、末尾が偶数の IP アドレスを、パケット ゲートウェイ 10.10.10.2 の背後にある CSG に送信します。

図 29　RADIUS ロード バランシング加速データ プレーン フォワーディングを使用した IOS SLB



次に、図 29 の設定の IOS SLB 設定文を示します。

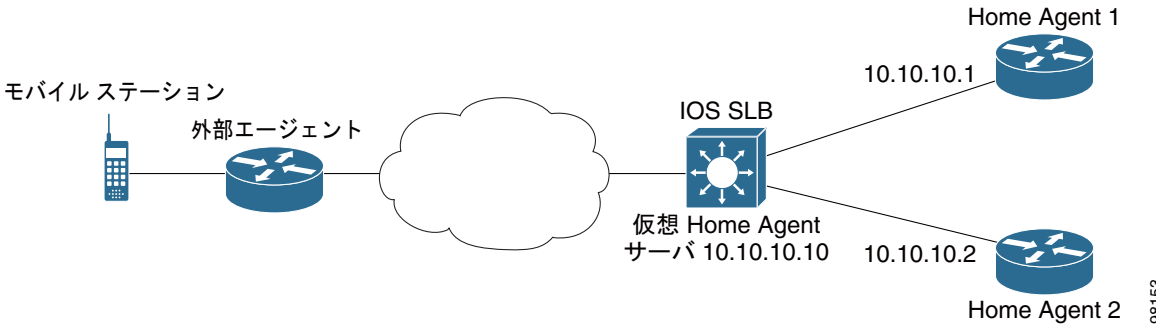
```
ip slb serverfarm CSGFARM
 predictor route-map rlb-pbr
ip slb serverfarm AAAFARM
 nat server
 real 10.10.10.1
  inservice
 real 10.10.10.2
  inservice
!
ip slb vserver RADIUS_ACCT
 virtual 10.10.10.10 udp 1813 service radius
 serverfarm CSGFARM
 radius inject acct 1 key 0 cisco
 inservice
!
ip slb vserver RADIUS_AUTH
 virtual 10.10.10.10 udp 1812 service radius
 serverfarm AAAFARM
 radius inject auth 1 calling-station-id
 radius inject auth timer 45
 radius inject auth vsa cisco
 inservice
!
interface vlan 100
 ip policy route-map rlb-pbr
!
access-list 1 permit 0.0.0.1 255.255.255.254
access-list 2 permit 0.0.0.0 255.255.255.254
!
route-map rlb-pbr permit 10
```

```
 match ip address 1
 set ip next-hop 10.10.10.1
!
route-map rlb-pbr permit 20
 match ip address 2
 set ip next-hop 10.10.10.2
```

例：Home Agent Director を使用した IOS SLB の設定方法

次の設定例では、IOS SLB が複数のホーム エージェントに Mobile IP RRQ の負荷を分散できるようにします。

図 30　　Home Agent Director を使用した IOS SLB



次に、図 30 の設定の IOS SLB 設定文を示します。

```
ip slb serverfarm HA_FARM
 nat server
 real 10.10.10.1
  inservice
 real 10.10.10.2
  inservice

ip slb vserver VIRTUAL_HA
 virtual 10.10.10.10 udp 434 service ipmobile
 serverfarm HA_FARM
 inservice
```

例：スティッキ接続を使用した IOS SLB の設定方法

次の設定例では、サブネットからのすべての HTTP 接続を、サーバ ファーム PUBLIC の同じ実サーバに割り当てます。

```
ip slb vserver http
  serverfarm PUBLIC
  sticky 30 group 1 netmask 255.255.255.248
  virtual 20.20.20.20 tcp 80
  inservice
```

次の設定例では、HTTP 接続を上記の設定に追加します。上記と同じスティッキ情報を使用しますが、仮想サーバは異なります。

```
ip slb vserver https
  serverfarm PUBLIC
  sticky 30 group 1 netmask 255.255.255.248
```

```
  virtual 20.20.20.20 tcp 443
  inservice
```

この例では、サブネットからのすべての HTTP 接続*および*HTTPS 接続は、同じ実サーバに割り当てられます。たとえば、あるユーザが HTTP に接続する場合、次のユーザは HTTPS に接続し、両方の接続は同じ実サーバに割り当てられます。

例：GTP IMSI スティッキ データベースを使用した IOS SLB の設定方法

次の設定例で、IOS SLB GTP IMSI スティッキ データベースをイネーブルにする方法を示します。

```
ip slb serverfarm GGSN_FARM
 failaction gtp purge
 real 10.20.10.1
  weight 1
  faildetect numconns 255 numclients 8
  inservice
!
 real 10.20.10.2
  weight 1
  faildetect numconns 255 numclients 8
  inservice
!
 real 10.20.10.3
  weight 1
  faildetect numconns 255 numclients 8
  inservice
!
ip slb vserver GGSN_SERVER1
 virtual 10.10.10.10 udp 3386 service gtp
 serverfarm GGSN_FARM backup GGSN_FARM
 idle gtp request 90
 idle gtp imsi 10000000
 sticky gtp imsi group 1
 gtp notification cac 3
 inservice
!
ip slb vserver GGSN_SERVER2
 virtual 10.10.10.10 udp 2123 service gtp
 serverfarm GGSN_FARM backup GGSN_FARM
 idle gtp request 90
 idle gtp imsi 10000000
 sticky gtp imsi group 1
 gtp notification cac 3
 inservice
```

例：ASN IMSI スティッキ データベースを使用した IOS SLB の設定方法

次の設定例は、IOS SLB ASN スティッキ データベースをイネーブルにする方法を示しています。

```
ip slb entries sticky 15000 800000
ip slb serverfarm ASNLB_FARM
 failaction asn purge
!
 real 10.20.10.1
  weight 1
  faildetect numconns 255 numclients 8
  inservice
!
```

```
 real 10.20.10.2
  weight 1
  faildetect numconns 255 numclients 8
  inservice
!
 real 10.20.10.3
  weight 1
  faildetect numconns 255 numclients 8
  inservice
!
ip slb vserver ASNLB_SERVER
 virtual 10.10.10.10 udp 0 service asn
 serverfarm ASNLB_FARM
 idle asn request 90
 idle asn msid 100000
 sticky asn msid group 1
 gw port 63082
 replicate casa 100.100.100.102 100.100.100.101 1024 password hello
 inservice
```

例：透過的 Web キャッシュ ロード バランシングを使用した IOS SLB の設定方法

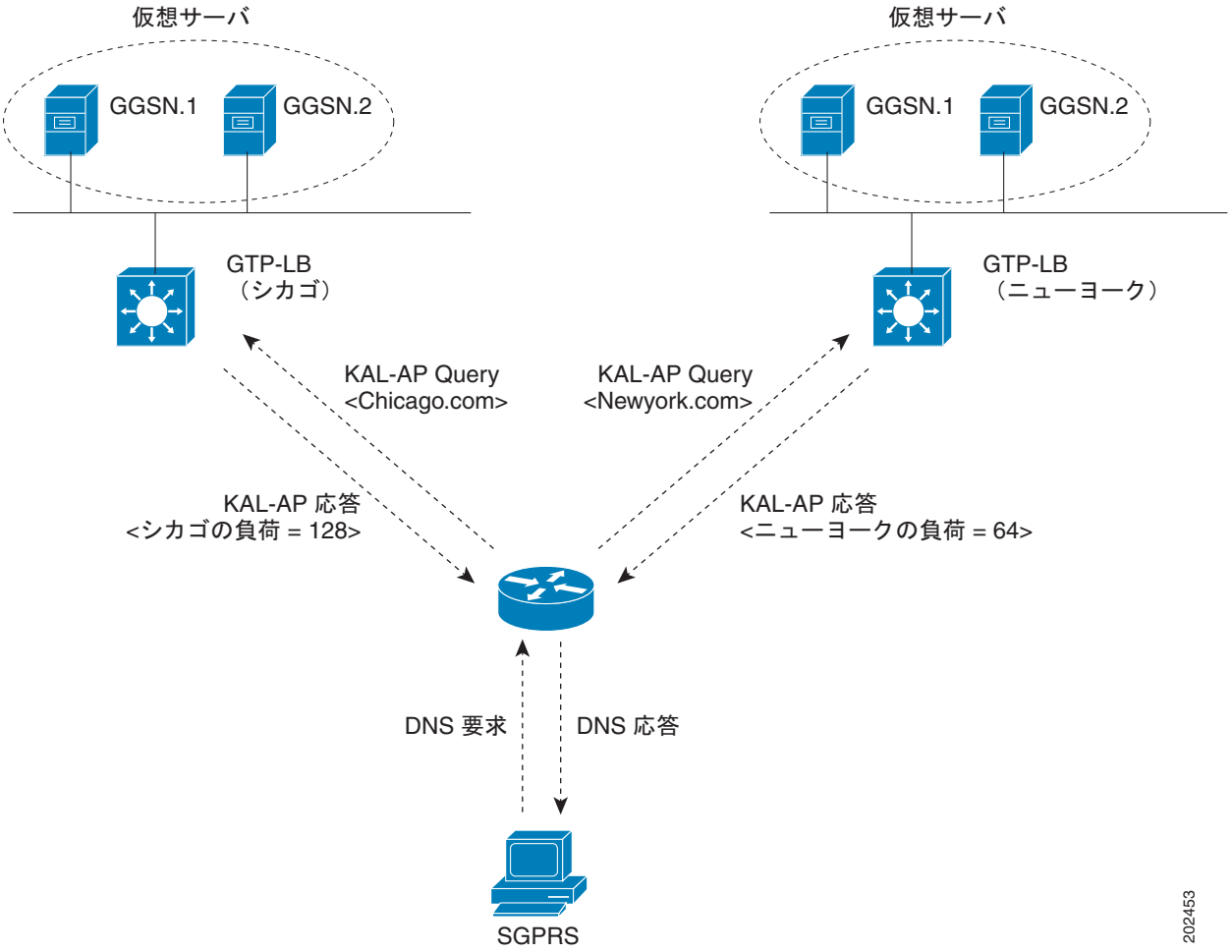
次の設定例では、仮想サーバ WEBCACHE によって、ロード バランシング デバイスを経由するすべての Web フローを確認し、サーバ ファーム WEBCACHE-FARM に送出します。**client exclude** 文によってサブネット 80.80.7.0 から発信されたフローを無視し、実サーバ 80.80.7.188 および 80.80.7.189 が必要に応じてインターネットと通信できるようにします。

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

例：KAL-AP エージェントを使用した IOS SLB の設定方法

次の設定例では、ドメイン ネーム システム（DNS）クエリー **abcd.com** を GSS に送信するようにクライアントを設定します。DUBLIN サイトの Global Site Selector（GSS）は、クライアントから要求を受信します。GSS は、仮想サーバからレポートされる負荷に基づき、CHICAGO（10.0.0.100）または NEWYORK（10.0.0.200）の仮想 IP アドレスを使用して DNS クエリーに応答します。

図 31　KAL-AP エージェントを使用した IOS SLB



次に、図 31 の設定の IOS SLB 設定文を示します。

GSS

```
shared-keepalive kalap 192.168.1.1 capp-secure enable key kap
shared-keepalive kalap 192.168.2.1 capp-secure enable key kap
!
answer vip 10.0.0.100 name CHICAGO activate
 keepalive type kalap tag 192.168.1.1 chicao.com
answer vip 10.0.0.200 name NEWYORK activate
 keepalive type kalap tag 192.168.2.1 newyork.com
!

answer-group ABCD owner System type vip
answer-add 10.0.0.100 name CHICAGO weight 1 order 0 load-threshold 254 activate
answer-add 10.0.0.200 name NEWYORK weight 1 order 0 load-threshold 254 activate
dns rule ABCDGPRS owner System source-address-list Anywhere domain-list abcd.com query a
 clause 1 vip-group method least-loaded ttl 20 count 1 sticky disable
```

サイト 1：IOS SLB - CHICAGO

```
ip slb capp udp
 peer port 6000 secret 0 kap
!
ip slb serverfarm SF
 kal-ap domain chicago.com
 farm-weight 200
 real 10.10.10.1
  inservice
 real 10.10.10.2
  inservice
!
ip slb vserver chicago
 virtual 10.0.0.100 udp 0
 serverfarm SF
 inservice
!
ip slb dfp
 agent 10.10.10.1 5000 30 0 10
 agent 10.10.10.2 5000 30 0 10
!
int vlan100
 ip address 192.168.1.1 255.255.255.0
```

GGSN-1

```
gprs dfp max-weight 100
gprs maximum-pdp-context-allowed 20000
!
ip dfp agent gprs
 port 5000
 inservice
```

GGSN-2

```
gprs dfp max-weight 100
gprs maximum-pdp-context-allowed 20000
!
ip dfp agent gprs
 port 5000
 inservice
```

サイト 2：IOS SLB - NEWYORK

```
ip slb capp udp
 peer port 6000
 peer 192.1.1.1 secret 0 test
 peer 10.100.100.100 port 1234
!
ip slb serverfarm SF
 kal-ap domain newyork.com
 farm-weight 6200
 real 10.20.20.1
  inservice
 real 10.20.20.2
  inservice
 real 10.20.20.3
  inservice
 real 10.20.20.4
  inservice
```

```
!
ip slb vserver chicago
 virtual 10.0.0.200 udp 0
 serverfarm SF
 inservice
!
ip slb dfp
 agent 10.10.10.1 5000 30 0 10
 agent 10.10.10.2 5000 30 0 10
!
int vlan200
 ip address 192.168.2.1 255.255.255.0
```

GGSN-1

```
gprs dfp max-weight 100
gprs maximum-pdp-context-allowed 20000
!
ip dfp agent gprs
 port 5000
 inservice
```

GGSN-2

```
gprs dfp max-weight 100
gprs maximum-pdp-context-allowed 20000
!
ip dfp agent gprs
 port 5000
 inservice
```

関連情報

次のセクションで、IOS SLB に関するその他の情報を提供します。

- 「トラブルシューティング」（P.190）
- 「サポートされているプラットフォーム」（P.192）

トラブルシューティング

質問	回答
IOS SLB を使用して、同じ LAN または VLAN 上にあるクライアントおよび実サーバの負荷を分散できますか。	**いいえ。** **IOS SLB は、同じ LAN または VLAN 上にあるクライアントおよび実サーバ間のフローのロード バランシングをサポートしていません。同じインターフェイス上のロード バランシング デバイスには、ロード バランシング対象のパケットを入出力できません。**
データを転送しているのに、IOS SLB で接続が ESTABLISHED とマークされないのはなぜですか。	dispatched モードを使用している場合、発信フローが IOS SLB をバイパスできる代替パスがないようにします。また、クライアントと実サーバが同じ IP サブネット上にない（つまり、同じ LAN または VLAN 上にない）ようにします。
実サーバに直接接続できるのに、仮想サーバに接続できないのはなぜですか。	仮想 IP アドレスが、各実サーバでループバックとして設定されていることを確認します（dispatched モードで実行している場合）。
ネットワークから実サーバの接続を解除しても、IOS SLB で実サーバが FAILED とマークされないのはなぜですか。	**numclients**、**numconns**、および **delay** の各キーワードの値を調整します。 クライアント数がごく少数の場合（たとえば、テスト環境）、**numclients** キーワードを使用すると問題が発生する可能性があります。これは、IOS SLB が少数のクライアントの障害を実サーバの障害と取り違えないようにするパラメータです。
実サーバを終了したり、物理的に接続を解除しても、IOS SLB で INSERVICE とマークされないのはなぜですか。	INSERVICE 状態および OUTOFSERVICE 状態は、ネットワーク管理者が、実サーバの動作時にその実サーバを使用する*意図*があるかどうかを示します。INSERVICE 状態で、IOS SLB の自動障害検出によって動的に選択リストから削除された実サーバは、FAILED とマークされます。これらの実サーバを表示するには、**show ip slb reals detail** コマンドを使用します。 リリース 12.1(1)E 以降、サーバ動作の実態を反映するために、INSERVICE は OPERATIONAL に変更されました。
IOS SLB スティッキ接続が適切に動作していることは、どのように確認できますか。	次の手順を使用します。 **1.** スティッキ接続を設定します。 **2.** クライアント接続を開始します。 **3.** **show ip slb reals detail** および **show ip slb conns** コマンドを入力します。 **4.** 実サーバの接続カウントを確認します。カウントが増える実サーバは、クライアント接続が割り当てられた実サーバです。 **5.** **show ip slb sticky** コマンドを入力して、IOS SLB に格納されているスティッキの関係を表示します。 **6.** 接続を終了します。 **7.** 実サーバの接続カウントが減ることを確認します。 **8.** スティッキ タイムアウト値の間待ってから、接続を再開します。 **9.** もう一度 **show ip slb conns** コマンドを入力します。 **10.** 実サーバの接続カウントをもう一度調べて、スティッキ接続は以前と同じ実サーバに割り当てられていることを確認します。

質問	回答
サーバ障害が適切に検出されていることは、どのように確認できますか。	次の手順を使用します。 1. 大量のクライアント数を使用します。クライアント数がごく少数の場合、サーバが FAILED と表示されないように、**faildetect numconns**（実サーバ）コマンドで **numclients** キーワードを調整します。 2. **show ip slb reals detail** コマンドを入力して、実サーバのステータスを表示します。 3. 実サーバのステータスと接続カウントを確認します。 – 障害が発生したサーバは、コマンドの送信時にサーバがバックアップになったことを確認するかどうかに基づいて、FAILED、TESTING、または READY_TO_TEST のステータスを示します。 – 実サーバに障害が発生すると、割り当て済みで確立していない（SYN または ACK を受信していない）接続は、**reassign** しきい値に達した後、最初に受信した SYN で、別の実サーバに再割り当てされます。ただし、確立済みの接続は同じ実サーバに転送されます。これは、新しい接続を受け入れない可能性があり、さらに既存の接続を提供している可能性があるためです。 – 加重最小接続の場合、サービスが開始されたばかりの実サーバは、新しい接続で過負荷にならないように、低速で開始されます（詳細については、「スロー スタート」（P.23）を参照してください）。そのため、新しい実サーバについて表示される接続カウントは、（新しい実サーバの低いカウントに関係なく）他の実サーバに送信される接続を示します。また、接続カウントは、新しい実サーバに対して「ダミー接続」を示します。ダミー接続は、スロー スタート期間に、IOS SLB が実サーバの接続数を意図的につり上げるために使用されます。
no inservice コマンドで、リソースは直ちにアウト オブ サービスになりますか。	**inservice** コマンドの **no** 形式を使用して、ファイアウォール、ファイアウォール ファーム、実サーバ、または仮想サーバをサービスから削除すると、各リソースは通常の手順で削除を実行します。新しい接続が割り当てられなければ、既存の接続は完了できます。 ファイアウォール ファームまたは仮想サーバ全体について、すべての既存の接続を直ちに停止するには、**clear ip slb connections** コマンドを使用します。
同じ Catalyst 6500 ファミリ スイッチに IOS SLB と入力 ACL の両方を設定すると、「TCAM Capacity Exceeded」メッセージが表示されます。なぜですか。	1 台の Catalyst 6500 ファミリ スイッチ上で IOS SLB と、入力 ACL またはファイアウォール ロード バランシングのどちらかを設定すると、ポリシー フィーチャ カード（PFC）上の Telecommunications Access Method（TCAM）の容量を超える可能性があります。この問題を解決するには、**mls ip slb search wildcard rp** コマンドを使用して、IOS SLB で使用される TCAM スペースの量を減らします。ただし、このコマンドを使用すると、ルート プロセッサの使用率が若干増加する可能性があります。
IOS SLB VRF をサポートする IOS リリースおよびプラットフォームはどれですか。	IOS SLB の Virtual Private Network（VPN）Routing and Forwarding（VRF）は、Cisco 7600 シリーズ ルータ用の MSFC3（SUP720-MSFC3）を搭載した Supervisor Engine 720 上の IOS リリース 12.2(18)SXE 以降でサポートされます。

質問	回答
スーパーバイザで表示される IOS SLB out-of-sync メッセージによって何が起こる可能性がありますか。	**replicate slave** が設定された 1 つのスーパーバイザ エンジンを使用している場合は、そのスーパーバイザで out-of-sync メッセージを受信する可能性があります。
IOS SLB は、同じスーパーバイザにファイアウォール ロード バランシングと RADIUS ロード バランシングの両方を提供できますか。	IOS SLB は、同じ Supervisor Engine 720（SUP720-MSFC3）にファイアウォール ロード バランシングと RADIUS ロード バランシングの両方を提供できます。

サポートされているプラットフォーム

スイッチまたはルータ	サポートされているプラットフォーム
Cisco 7600 シリーズ ルータ	• MSFC2A を搭載した Supervisor Engine 32（SUP32-MSFC2A） • MSFC3 を搭載した Supervisor Engine 720（SUP720-MSFC3） • 2 つのギガビット イーサネット ポートを搭載した Distributed Forwarding Card DFC3CXL 付きの Cisco Route Switch Processor 720（RSP720-3CXL-GE）

その他の参考資料

ここでは、IOS SLB に関する参考資料について説明します。

- 「関連資料」（P.193）
- 「規格」（P.193）
- 「MIB」（P.193）
- 「RFC」（P.193）
- 「シスコのテクニカル サポート」（P.194）

関連資料

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

規格

規格	タイトル
この機能がサポートする新しい規格または変更された規格はありません。また、この機能による既存規格のサポートに変更はありません。	—

MIB

MIB	MIB リンク
CISCO-SLB-MIB CISCO-SLB-CAPABILITY **（注）** これらの MIB のオブジェクトは *read-create* と定義されていますが、SNMP SET コマンドを使用して変更することはできません。代わりに、コマンド ラインを使用して関連するコマンド ライン キーワードを設定します。その後に、新しい値が SNMP で反映されます。	選択されたプラットフォーム、シスコ ソフトウェア リリース、およびフィーチャ セットの MIB を検索してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
RFC 1631	「*The IP Network Address Translator (NAT)*」

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 ・テクニカル サポートを受ける ・ソフトウェアをダウンロードする ・セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける ・ツールおよびリソースへアクセスする - Product Alert の受信登録 - Field Notice の受信登録 - Bug Toolkit を使用した既知の問題の検索 ・Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する ・トレーニング リソースへアクセスする ・TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

IOS SLB の機能情報

表 2 に、この章に記載されている機能および具体的な設定情報へのリンクを示します。この表には、Cisco IOS Release 12.2(1) 以降のリリースで導入または変更された機能だけを示します。

ご使用の Cisco IOS ソフトウェア リリースによっては、コマンドの中に一部使用できないものがあります。特定のコマンドのリリース情報については、『*Cisco IOS IP Application Services Command Reference*』を参照してください。

プラットフォーム サポートとソフトウェア イメージ サポートに関する情報を入手するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator を使用すると、特定のソフトウェア リリース、フィーチャ セット、またはプラットフォームをサポートするソフトウェア イメージを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 表 2 に、特定のソフトウェア リリース トレイン内の機能に対するサポートが導入されたソフトウェア リリースだけを示します。特に断りのないかぎり、そのソフトウェア リリース トレイン以降のリリースでもその機能がサポートされます。

表 2　IOS SLB の機能情報

機能名	リリース	機能情報
IOS SLB、12.2 の最初のリリース	12.2(1) 12.2(14)S 12.2(14)ZA2 12.2(14)ZA4 12.2(14)ZA5 12.2(14)ZA6 12.2(17d)SXB 12.2(17d)SXB1 12.2(17d)SXD 12.2(17d)SXE 12.2(18)SXF 12.2(18)SXF5 12.2(18)SXF7 12.2(33)SRB 12.2(33)SRC 12.2(33)SRC1 12.2(33)SRE 15.0(1)S	IOS SLB 機能は、多様なネットワーク デバイスおよびサービスに適したロード バランシングが用意されている IOS ベースのソリューションです。
AAA ロード バランシング	12.2(14)S 12.2(14)ZA2 12.2(14)ZA4 12.2(14)ZA5 12.2(14)ZA6 12.2(17d)SXB 12.2(17d)SXB1 12.2(17d)SXD 12.2(17d)SXE 12.2(18)SXF 12.2(18)SXF5 12.2(18)SXF7 12.2(33)SRB 12.2(33)SRC 12.2(33)SRC1 12.2(33)SRE 15.0(1)S	IOS SLB には、RADIUS の Authentication, Authorization, and Accounting（AAA; 認証、認可、アカウンティング）サーバ用の RADIUS ロード バランシング機能があります。 この機能については、次の項に説明があります。 • 「AAA ロード バランシング」（P.29）

表 2　IOS SLB の機能情報 （続き）

機能名	リリース	機能情報
アクティブ スタンバイ	12.2(1) 12.2(14)S 12.2(14)ZA2 12.2(14)ZA4 12.2(14)ZA5 12.2(14)ZA6 12.2(17d)SXB 12.2(17d)SXB1 12.2(17d)SXD 12.2(17d)SXE 12.2(18)SXF 12.2(18)SXF5 12.2(18)SXF7 12.2(33)SRB 12.2(33)SRC 12.2(33)SRC1 12.2(33)SRE 15.0(1)S	アクティブ スタンバイによって、2 つの IOS SLB は同じ仮想 IP アドレスの負荷を分散すると同時に、相互にバックアップとして動作できます。 この機能に関する詳細については、次の各項を参照してください。 • 「アクティブ スタンバイ」（P.31） • 「ステートレス バックアップの設定作業リスト」（P.106） • 「例：アクティブ スタンバイを使用した IOS SLB の設定方法」（P.153）
サーバ ロード バランシングのアルゴリズム	12.2(1) 12.2(14)S 12.2(14)ZA2 12.2(14)ZA4 12.2(14)ZA5 12.2(14)ZA6 12.2(17d)SXB 12.2(17d)SXB1 12.2(17d)SXD 12.2(17d)SXE 12.2(18)SXF 12.2(18)SXF5 12.2(18)SXF7 12.2(33)SRB 12.2(33)SRC 12.2(33)SRC1 12.2(33)SRE 15.0(1)S	IOS SLB には次のロード バランシング アルゴリズムがあります。 • 「加重ラウンド ロビン アルゴリズム」（P.13） • 「加重最小接続アルゴリズム」（P.13） • 「ルート マップ アルゴリズム」（P.14） この機能に関する詳細については、次の各項を参照してください。 • 「サーバ ロード バランシングのアルゴリズム」（P.12） • 「サーバ ファームと実サーバの設定方法」（P.41）

表 2　IOS SLB の機能情報 （続き）

機能名	リリース	機能情報
代替 IP アドレス	12.2(1) 12.2(14)S 12.2(14)ZA2 12.2(14)ZA4 12.2(14)ZA5 12.2(14)ZA6 12.2(17d)SXB 12.2(17d)SXB1 12.2(17d)SXD 12.2(17d)SXE 12.2(18)SXF 12.2(18)SXF5 12.2(18)SXF7 12.2(33)SRB 12.2(33)SRC 12.2(33)SRC1 12.2(33)SRE 15.0(1)S	IOS SLB を使用すると、代替 IP アドレスを使用して、ロード バランシング デバイスに Telnet を使用できます。 この機能については、次の項に説明があります。 • 「代替 IP アドレス」（P.23）
ASN ロード バランシング	12.2(33)SRC1 12.2(33)SRE 15.0(1)S	IOS SLB は、ASN ゲートウェイのセット全体にロード バランシングを提供します。ゲートウェイのクラスタが、ベース ステーションからは 1 つの ASN ゲートウェイとして見えます。 この機能に関する詳細については、次の各項を参照してください。 • 「Cisco IOS SLB に関する制約事項」（P.3） • 「ASN ロード バランシング」（P.31） • 「ASN ロード バランシングの設定作業リスト」（P.101） この機能によって、次のコマンドが変更されました。 **debug ip slb、idle（仮想サーバ）、show ip slb sessions、show ip slb stats、show ip slb vservers、virtual**
ASN ロード バランシング：ステートフルとスティッキのサポート	12.2(33)SRE 15.0(1)S	ASN ロード バランシングは、ステートフル冗長性とスティッキ接続をサポートします。 この機能に関する詳細については、次の各項を参照してください。 • 「Cisco IOS SLB に関する制約事項」（P.3） • 「ASN ロード バランシング」（P.31） • 「ASN ロード バランシングの設定作業リスト」（P.101） この機能に関連して、次の新しいコマンドが追加されています。 **clear ip slb sticky asn msid、gw port、show ip slb sticky** この機能によって、次のコマンドが変更されました。 **debug ip slb、failaction（サーバ ファーム）、idle（仮想サーバ）、show ip slb sticky、sticky（仮想サーバ）**

表 2　IOS SLB の機能情報 （続き）

機能名	リリース	機能情報
オーディオおよびビデオのロード バランシング	12.2(1) 12.2(14)S 12.2(14)ZA2 12.2(14)ZA4 12.2(14)ZA5 12.2(14)ZA6 12.2(17d)SXB 12.2(17d)SXB1 12.2(17d)SXD 12.2(17d)SXE 12.2(18)SXF 12.2(18)SXF5 12.2(18)SXF7 12.2(33)SRB 12.2(33)SRC 12.2(33)SRC1 12.2(33)SRE 15.0(1)S	IOS SLB は、RealNetworks アプリケーションを実行しているサーバに対して、Real-Time Streaming Protocol（RTSP; リアルタイム トランスポート ストリーミング プロトコル）経由の RealAudio ストリームと RealVideo ストリームのバランスを取ることができます。 この機能については、次の項に説明があります。 • 「オーディオおよびビデオのロード バランシング」（P.29）
自動サーバ障害検出	12.2(1) 12.2(14)S 12.2(14)ZA2 12.2(14)ZA4 12.2(14)ZA5 12.2(14)ZA6 12.2(17d)SXB 12.2(17d)SXB1 12.2(17d)SXD 12.2(17d)SXE 12.2(18)SXF 12.2(18)SXF5 12.2(18)SXF7 12.2(33)SRB 12.2(33)SRC 12.2(33)SRC1 12.2(33)SRE 15.0(1)S	IOS SLB は、実サーバに対して失敗した各 TCP 接続試行を自動的に検出し、そのサーバの障害カウンタを増加します。サーバの障害カウンタが設定可能な障害しきい値を超えると、サーバはアウト オブ サービスと見なされ、アクティブな実サーバ リストから削除されます。 この機能に関する詳細については、次の各項を参照してください。 • 「自動サーバ障害検出」（P.24） • 「自動サーバ障害検出のディセーブル方法」（P.115）

表 2　IOS SLB の機能情報 （続き）

機能名	リリース	機能情報
自動サーバ障害検出：自動サーバ障害検出のディセーブル化	12.2(14)ZA4 12.2(14)ZA5 12.2(14)ZA6 12.2(17d)SXB 12.2(17d)SXB1 12.2(17d)SXD 12.2(17d)SXE 12.2(18)SXF 12.2(18)SXF5 12.2(18)SXF7 12.2(33)SRB 12.2(33)SRC 12.2(33)SRC1 12.2(33)SRE 15.0(1)S	IOS SLB は、実サーバに対して失敗した各 TCP 接続試行を自動的に検出し、そのサーバの障害カウンタを増加します。サーバの障害カウンタが設定可能な障害しきい値を超えると、サーバはアウト オブ サービスと見なされ、アクティブな実サーバ リストから削除されます。 この機能に関する詳細については、次の各項を参照してください。 • 「自動サーバ障害検出」（P.24） • 「自動サーバ障害検出のディセーブル方法」（P.115）
自動アンフェイル	12.2(1) 12.2(14)S 12.2(14)ZA2 12.2(14)ZA4 12.2(14)ZA5 12.2(14)ZA6 12.2(17d)SXB 12.2(17d)SXB1 12.2(17d)SXD 12.2(17d)SXE 12.2(18)SXF 12.2(18)SXF5 12.2(18)SXF7 12.2(33)SRB 12.2(33)SRC 12.2(33)SRC1 12.2(33)SRE 15.0(1)S	実サーバに障害が発生し、アクティブなサーバのリストから削除されると、設定可能な再試行タイマーに指定された期間、新しい接続は割り当てられません。タイマーの期限が切れると、そのサーバには新しい仮想サーバ接続を受ける資格ができ、IOS SLB から次の適格性確認の接続がサーバに送信されます。その接続が成功すると、失敗したサーバはアクティブな実サーバのリストに戻されます。接続に失敗すると、サーバはアウト オブ サービスのままで、再試行タイマーがリセットされます。失敗した接続は少なくとも 1 回は再試行が実行されます。実行されていない場合、次の適格性確認の接続もその失敗したサーバに送信されます。 この機能については、次の項に説明があります。 • 「自動アンフェイル」（P.25）

表 2　IOS SLB の機能情報 （続き）

機能名	リリース	機能情報
サーバ ファームおよびファイアウォール ファームに対する攻撃の回避	12.2(1) 12.2(14)S 12.2(14)ZA2 12.2(14)ZA4 12.2(14)ZA5 12.2(14)ZA6 12.2(17d)SXB 12.2(17d)SXB1 12.2(17d)SXD 12.2(17d)SXE 12.2(18)SXF 12.2(18)SXF5 12.2(18)SXF7 12.2(33)SRB 12.2(33)SRC 12.2(33)SRC1 12.2(33)SRE 15.0(1)S	高度なセキュア サイトであれば、特定の手順を使用して、サーバ ファームおよびファイアウォール ファームを攻撃から保護できます。 この機能については、次の項に説明があります。 • 「サーバ ファームおよびファイアウォール ファームに対する攻撃の回避」（P.23）
バックアップ サーバ ファーム	12.2(14)S 12.2(14)ZA2 12.2(14)ZA4 12.2(14)ZA5 12.2(14)ZA6 12.2(17d)SXB 12.2(17d)SXB1 12.2(17d)SXD 12.2(17d)SXE 12.2(18)SXF 12.2(18)SXF5 12.2(18)SXF7 12.2(33)SRB 12.2(33)SRC 12.2(33)SRC1 12.2(33)SRE 15.0(1)S	バックアップ サーバ ファームは、プライマリ サーバ ファームに定義されている実サーバで新しい接続を受け入れることができないときに使用できるサーバ ファームです。 この機能に関する詳細については、次の各項を参照してください。 • 「バックアップ サーバ ファーム」（P.25） • 「仮想サーバの設定方法」（P.45）

表 2　IOS SLB の機能情報 （続き）

機能名	リリース	機能情報
バインディング ID のサポート	12.2(1) 12.2(14)S 12.2(14)ZA2 12.2(14)ZA4 12.2(14)ZA5 12.2(14)ZA6 12.2(17d)SXB 12.2(17d)SXB1 12.2(17d)SXD 12.2(17d)SXE 12.2(18)SXF 12.2(18)SXF5 12.2(18)SXF7 12.2(33)SRB 12.2(33)SRC 12.2(33)SRC1 12.2(33)SRE 15.0(1)S	バインド ID を使用すれば、1 台の物理サーバを複数の仮想サーバにバインドして、サーバごとに加重を報告させることができます。したがって、単一の実サーバは、自身の複数インスタンスとして表現され、それぞれに異なるバインド ID が割り当てられます。Dynamic Feedback Protocol（DFP）はバインド ID を使用して、特定の加重が指定された実サーバのインスタンスを識別します。バインド ID が必要なのは、DFP を使用している場合だけです。 この機能に関する詳細については、次の各項を参照してください。 • 「バインディング ID のサポート」（P.14） • 「Cisco IOS SLB 用の DFP」（P.25） • 「サーバ ファームと実サーバの設定方法」（P.41）
Client-Assigned ロード バランシング	12.2(1) 12.2(14)S 12.2(14)ZA2 12.2(14)ZA4 12.2(14)ZA5 12.2(14)ZA6 12.2(17d)SXB 12.2(17d)SXB1 12.2(17d)SXD 12.2(17d)SXE 12.2(18)SXF 12.2(18)SXF5 12.2(18)SXF7 12.2(33)SRB 12.2(33)SRC 12.2(33)SRC1 12.2(33)SRE 15.0(1)S	Client-Assigned ロード バランシングでは、仮想サーバを使用する権限を持つクライアント IP サブネットのリストを指定することで、仮想サーバに対するアクセスを制限できます。この機能を使用すると、仮想 IP アドレスに接続する 1 セットのクライアント IP サブネット（内部サブネットなど）を、1 つのサーバ ファームまたはファイアウォール ファームに割り当て、別のクライアント セット（外部クライアントなど）を別のサーバ ファームまたはファイアウォール ファームに割り当てることができます。 この機能については、次の項に説明があります。 • 「Client-Assigned ロード バランシング」（P.14）
接続のレート制限	12.2(33)SRC 12.2(33)SRC1 12.2(33)SRE 15.0(1)S	IOS SLB を使用すると、サーバ ファームの 1 つの実サーバに許可する最大接続レートを指定できます。 この機能に関する詳細については、次の各項を参照してください。 • 「接続のレート制限」（P.14） • 「サーバ ファームと実サーバの設定方法」（P.41）

表 2　IOS SLB の機能情報 （続き）

機能名	リリース	機能情報
コンテンツ フロー モニタのサポート	12.2(1) 12.2(14)S 12.2(14)ZA2 12.2(14)ZA4 12.2(14)ZA5 12.2(14)ZA6 12.2(17d)SXB 12.2(17d)SXB1 12.2(17d)SXD 12.2(17d)SXE 12.2(18)SXF 12.2(18)SXF5 12.2(18)SXF7 12.2(33)SRB 12.2(33)SRC 12.2(33)SRC1 12.2(33)SRE 15.0(1)S	IOS SLB は Cisco Content Flow Monitor（CFM）をサポートします。CFM は、CiscoWorks2000 製品ファミリ内の Web ベース ステータス モニタリング アプリケーションです。CFM を使用すると、Cisco サーバ ロード バランシング デバイスを管理できます。CFM は Windows NT および Solaris ワークステーション上で動作します。CFM には Web ブラウザを使用してアクセスします。 この機能については、次の項に説明があります。 • 「コンテンツ フロー モニタのサポート」（P.15）
TCP 接続コンテキストの遅延削除	12.2(1) 12.2(14)S 12.2(14)ZA2 12.2(14)ZA4 12.2(14)ZA5 12.2(14)ZA6 12.2(17d)SXB 12.2(17d)SXB1 12.2(17d)SXD 12.2(17d)SXE 12.2(18)SXF 12.2(18)SXF5 12.2(18)SXF7 12.2(33)SRB 12.2(33)SRC 12.2(33)SRC1 12.2(33)SRE 15.0(1)S	IP パケットの順序異常が原因で、IOS SLB が、TCP 接続の終了（finish [FIN] または reset [RST]）後に、接続用の他のパケットが続いているのを検出する場合があります。一般的に、この問題は TCP 接続パケットがたどるパスが複数あるときに発生します。接続が終了した後に到着するパケットを適切にリダイレクトするために、IOS SLB が、指定された期間、TCP 接続情報（つまり、コンテキスト）を保持します。接続の終了後にコンテキストを保持する期間は、設定可能な遅延タイマーで制御されます。 この機能に関する詳細については、次の各項を参照してください。 • 「TCP 接続コンテキストの遅延削除」（P.15） • 「サーバ ファームと実サーバの設定方法」（P.41）

表 2　IOS SLB の機能情報 （続き）

機能名	リリース	機能情報
DFP のサポート	12.2(1) 12.2(14)S 12.2(14)ZA2 12.2(14)ZA4 12.2(14)ZA5 12.2(14)ZA6 12.2(17d)SXB 12.2(17d)SXB1 12.2(17d)SXD 12.2(17d)SXE 12.2(18)SXF 12.2(18)SXF5 12.2(18)SXF7 12.2(33)SRB 12.2(33)SRC 12.2(33)SRC1 12.2(33)SRE 15.0(1)S	IOS SLB は Dynamic Feedback Protocol（DFP）をサポートします。 この機能に関する詳細については、次の各項を参照してください。 • 「Cisco IOS SLB 用の DFP」（P.25） • 「DFP の設定方法」（P.70） • 「例：GPRS ロード バランシングを使用した IOS SLB の設定方法」（P.163） • 「例：KAL-AP エージェントを使用した IOS SLB の設定方法」（P.186）
DFP Agent Subsystem のサポート	12.2(14)S 12.2(14)ZA2 12.2(14)ZA4 12.2(14)ZA5 12.2(14)ZA6 12.2(17d)SXB 12.2(17d)SXB1 12.2(17d)SXD 12.2(17d)SXE 12.2(18)SXF 12.2(18)SXF5 12.2(18)SXF7 12.2(33)SRB 12.2(33)SRC 12.2(33)SRC1 12.2(33)SRE 15.0(1)S	IOS SLB は DFP Agent Subsystem 機能（グローバル ロード バランシングとも呼ばれます）をサポートします。そのため、IOS SLB 以外のクライアント サブシステムも DFP エージェントとして実行できます。DFP Agent Subsystem を利用すると、複数のクライアント サブシステムの複数の DFP エージェントを同時に使用できます。 この機能に関する詳細については、次の各項を参照してください。 • 「Dynamic Feedback Protocol（DFP）Agent Subsystem のサポート」（P.25） • 「DFP の設定方法」（P.70） • 「例：GTP Cause Code Inspection がイネーブルになっていない GPRS ロード バランシングを使用した IOS SLB の設定方法」（P.163） • 「例：GPRS ロード バランシングと NAT を使用した IOS SLB の設定方法」（P.168） • 「例：KAL-AP エージェントを使用した IOS SLB の設定方法」（P.186）

表 2　IOS SLB の機能情報 （続き）

機能名	リリース	機能情報
DFP および Home Agent Director	12.2(17d)SXD 12.2(17d)SXE 12.2(18)SXF 12.2(18)SXF5 12.2(18)SXF7 12.2(33)SRB 12.2(33)SRC 12.2(33)SRC1 12.2(33)SRE 15.0(1)S	Home Agent Director の場合、DFP マネージャとして IOS SLB を定義し、サーバ ファームの各ホーム エージェントに DFP エージェントを定義できます。また、DFP エージェントから、ホーム エージェントの加重をレポートできます。DFP エージェントは、CPU 使用率、プロセッサ メモリ、およびホーム エージェントごとにアクティブ化できるバインディングの最大数に基づいて、各ホーム エージェントの加重を計算します この機能に関する詳細については、次の各項を参照してください。 • 「Cisco IOS SLB 用の DFP」（P.25） • 「DFP および Home Agent Director」（P.26） • 「Home Agent Director」（P.34） • 「DFP の設定方法」（P.70） • 「Home Agent Director の設定作業リスト」（P.102） • 「例：GPRS ロード バランシングを使用した IOS SLB の設定方法」（P.163） • 「例：Home Agent Director を使用した IOS SLB の設定方法」（P.184） • 「例：KAL-AP エージェントを使用した IOS SLB の設定方法」（P.186）
Exchange Director 機能	12.2(14)ZA5 12.2(14)ZA6 12.2(17d)SXB 12.2(17d)SXB1 12.2(17d)SXD 12.2(17d)SXE 12.2(18)SXF 12.2(18)SXF5 12.2(18)SXF7 12.2(33)SRB 12.2(33)SRC 12.2(33)SRC1 12.2(33)SRE 15.0(1)S	IOS SLB は、Catalyst 7600 シリーズ ルータ用の mobile Service Exchange Framework（mSEF）の場合、Exchange Director をサポートします。 この機能については、次の項に説明があります。 • 「Exchange Director 機能」（P.31）

表 2　IOS SLB の機能情報 （続き）

機能名	リリース	機能情報
ファイアウォール ロード バランシング	12.2(1) 12.2(14)S 12.2(14)ZA2 12.2(14)ZA4 12.2(14)ZA5 12.2(14)ZA6 12.2(17d)SXB 12.2(17d)SXB1 12.2(17d)SXD 12.2(17d)SXE 12.2(18)SXF 12.2(18)SXF5 12.2(18)SXF7 12.2(33)SRB 12.2(33)SRC 12.2(33)SRC1 12.2(33)SRE 15.0(1)S	この名前が示すように、ファイアウォール ロード バランシングを使用すると、IOS SLB はフローの負荷をファイアウォールに分散します。ファイアウォール ロード バランシングでは、ファイアウォール グループ（ファイアウォール ファームと呼ばれます）の両側にあるロード バランシング デバイスを使用して、各フローのトラフィックが同じファイアウォールに送信されるように確保しているため、セキュリティ ポリシーは保護されます。 この機能に関する詳細については、次の各項を参照してください。 • 「ファイアウォール ロード バランシング」（P.15） • 「ファイアウォール ロード バランシングの設定方法」（P.53） • 「例：ファイアウォール ロード バランシングを使用した IOS SLB の設定方法」（P.124）
ファイアウォール ロード バランシング：複数のファイアウォール ファームのサポート	12.2(14)S 12.2(14)ZA2 12.2(14)ZA4 12.2(14)ZA5 12.2(14)ZA6 12.2(17d)SXB 12.2(17d)SXB1 12.2(17d)SXD 12.2(17d)SXE 12.2(18)SXF 12.2(18)SXF5 12.2(18)SXF7 12.2(33)SRB 12.2(33)SRC 12.2(33)SRC1 12.2(33)SRE 15.0(1)S	各ロード バランシング デバイスに複数のファイアウォール ファームを設定できます。 この機能に関する詳細については、次の各項を参照してください。 • 「複数ファイアウォール ファームのサポート」（P.17） • 「ファイアウォール ロード バランシングの設定方法」（P.53） • 「例：複数のファイアウォール ファームを使用した IOS SLB の設定方法」（P.129）

表 2　IOS SLB の機能情報 （続き）

機能名	リリース	機能情報
ファイアウォール ロード バランシング：性能の向上	12.2(33)SRE 15.0(1)S	IOS SLB ファイアウォールのロード バランシングによって、CPU 使用率が高くなる可能性がある、特定の条件を回避できます。 この機能に関する詳細については、次の各項を参照してください。 • 「ファイアウォール ロード バランシングの設定方法」（P.53） • 「MLS エントリのプロトコルレベル消去の設定方法」（P.98） • 「接続消去要求動作の設定方法」（P.98） • 「スティッキ接続消去要求動作の設定方法」（P.99） この機能に関連して、次の新しいコマンドが追加されています。 **purge connection**、**purge sticky** この機能により次のコマンドが変更されました。 **access**（ファイアウォール ファーム）
フローの永続性	12.2(14)ZA5 12.2(14)ZA6 12.2(17d)SXB 12.2(17d)SXB1 12.2(17d)SXD 12.2(17d)SXE 12.2(18)SXF 12.2(18)SXF5 12.2(18)SXF7 12.2(33)SRB 12.2(33)SRC 12.2(33)SRC1 12.2(33)SRE 15.0(1)S	フローの永続性には、負荷分散された IP フローを適切なノードに返す、高度なリターン ルーティング機能があります。負荷分散されたデータ パスの両側でハッシュ メカニズムを調整する必要はありません。また、ネットワーク アドレス変換（NAT）やプロキシを使用して、クライアントまたはサーバの IP アドレスを変更する必要もありません。 この機能については、次の項に説明があります。 • 「フローの永続性」（P.39）

表 2　IOS SLB の機能情報 （続き）

機能名	リリース	機能情報
GPRS ロード バランシング：GTP ロード バランシングに対するデュアルスタック サポート	15.0(1)S	IPv6 サポートによって、IOS SLB ですべてのバージョンの GTP（v0、v1、v2）に対する GTP ロード バランシング用の IPv6 アドレスを管理することができます。 デュアルスタック サポートを使用すれば、IOS SLB で GTP ロード バランシング用のデュアルスタック実装を管理することができます。デュアルスタック実装とは、IPv4 アドレスと IPv6 アドレスの両方を使用する実装です。 この機能に関する詳細については、次の各項を参照してください。 • 「GTP ロード バランシングに対するデュアルスタック サポート」（P.34） • 「GPRS ロード バランシングの設定作業リスト」（P.71） • 「例：GTP ロード バランシング用のデュアルスタック アドレスを使用した IOS SLB の設定方法」（P.173） この機能では、次のコマンドが追加されました。 **show ip slb wildcard** この機能によって、次のコマンドが変更されました。 **client（仮想サーバ）、real（サーバ ファーム）、serverfarm、show ip slb reals、show ip slb serverfarms、show ip slb sessions、show ip slb sticky、show ip slb vservers、show ip slb wildcard**
GPRS ロード バランシング：GGSN-IOS SLB メッセージング	12.2(17d)SXB1 12.2(17d)SXD 12.2(17d)SXE 12.2(18)SXF 12.2(18)SXF5 12.2(18)SXF7 12.2(33)SRB 12.2(33)SRC 12.2(33)SRC1 12.2(33)SRE 15.0(1)S	特定の状況が発生した場合、GGSN ではこの機能を使用して IOS SLB に通知できます。IOS SLB では通知によって適切な判断を下すことができます。結果として、GPRS ロード バランシングと障害検出が改善されます。 この機能に関する詳細については、次の各項を参照してください。 • 「GGSN-IOS SLB メッセージング」（P.26） • 「GGSN-IOS SLB メッセージング作業リスト」（P.74）

表 2　IOS SLB の機能情報 （続き）

機能名	リリース	機能情報
GPRS ロード バランシング：GTP Cause Code Inspection	12.2(14)ZA2 12.2(14)ZA4 12.2(14)ZA5 12.2(14)ZA6 12.2(17d)SXB 12.2(17d)SXB1 12.2(17d)SXD 12.2(17d)SXE 12.2(18)SXF 12.2(18)SXF5 12.2(18)SXF7 12.2(33)SRB 12.2(33)SRC 12.2(33)SRC1 12.2(33)SRE 15.0(1)S	GTP Cause Code Inspection をイネーブルにした GPRS ロード バランシングを使用すると、IOS SLB は、GGSN サーバ ファームとの間で送受信するすべての PDP コンテキスト シグナリング フローをモニタできます。それによって、GTP 障害の原因コードをモニタし、Cisco GGSN と非 Cisco GGSN の両方について、システム レベルの問題を検出できます。 この機能に関する詳細については、次の各項を参照してください。 • 「GTP Cause Code Inspection ありの GPRS ロード バランシング」（P.33） • 「GPRS ロード バランシングの設定作業リスト」（P.71） • 「例：GPRS ロード バランシング、NAT、および GTP Cause Code Inspection を使用した IOS SLB の設定方法」（P.171）
GPRS ロード バランシング：GTP IMSI スティッキ データベース	12.2(17d)SXE 12.2(18)SXF 12.2(18)SXF5 12.2(18)SXF7 12.2(33)SRB 12.2(33)SRC 12.2(33)SRC1 12.2(33)SRE 15.0(1)S	IOS SLB では、特定の International Mobile Subscriber ID（IMSI）に Gateway General Packet Radio Service（GPRS）Support Node（GGSN）を選択し、同じ IMSI から送信される以降の Packet Data Protocol（PDP）作成要求すべてを、選択した GGSN に転送できます。 この機能に関する詳細については、次の各項を参照してください。 • 「GTP IMSI スティッキ データベース」（P.16） • 「例：GTP IMSI スティッキ データベースを使用した IOS SLB の設定方法」（P.185）
GPRS ロード バランシング：GTP Sticky-Only のサポート	12.2(33)SRE 15.0(1)S	IOS SLB は、すべてのバージョンの GTP（v0、v1、v2）に対して sticky-only をサポートします。 この機能については、次の項に説明があります。 • 「仮想サーバの設定方法」（P.45） この機能では、次のコマンドが追加されました。 **gtp session (virtual server)** この機能により次のコマンドが変更されました。 **show ip slb sticky**

表 2　IOS SLB の機能情報 （続き）

機能名	リリース	機能情報
GPRS ロード バランシング：GTP v0 のサポート	12.2(14)S 12.2(14)ZA2 12.2(14)ZA4 12.2(14)ZA5 12.2(14)ZA6 12.2(17d)SXB 12.2(17d)SXB1 12.2(17d)SXD 12.2(17d)SXE 12.2(18)SXF 12.2(18)SXF5 12.2(18)SXF7 12.2(33)SRB 12.2(33)SRC 12.2(33)SRC1 12.2(33)SRE 15.0(1)S	IOS SLB は GTP version 0（GTP v0）をサポートします。GTP のサポートによって、IOS SLB は、「GTP 認識」になり、レイヤ 5 に対する知識を拡張することができます。 この機能に関する詳細については、次の各項を参照してください。 • 「GPRS ロード バランシング」（P.32） • 「仮想サーバの設定方法」（P.45） • 「GPRS ロード バランシングの設定作業リスト」（P.71） • 「例：GPRS ロード バランシングを使用した IOS SLB の設定方法」（P.163）
GPRS ロード バランシング：GTP v1 のサポート	12.2(14)ZA2 12.2(14)ZA4 12.2(14)ZA5 12.2(14)ZA6 12.2(17d)SXB 12.2(17d)SXB1 12.2(17d)SXD 12.2(17d)SXE 12.2(18)SXF 12.2(18)SXF5 12.2(18)SXF7 12.2(33)SRB 12.2(33)SRC 12.2(33)SRC1 12.2(33)SRE 15.0(1)S	IOS SLB は、GTP version 0（GTP v0）および GTP version 1（GTP v1）の両方をサポートします。GTP のサポートによって、IOS SLB は、「GTP 認識」になり、レイヤ 5 に対する知識を拡張することができます。 この機能に関する詳細については、次の各項を参照してください。 • 「GPRS ロード バランシング」（P.32） • 「仮想サーバの設定方法」（P.45） • 「GPRS ロード バランシングの設定作業リスト」（P.71） • 「例：GPRS ロード バランシングを使用した IOS SLB の設定方法」（P.163）
GPRS ロード バランシング：GTP v2 のサポート	12.2(33)SRE 15.0(1)S	IOS SLB は GTP version 2（GTP v2）をサポートします。 この機能に関する詳細については、次の各項を参照してください。 • 「Cisco IOS SLB に関する制約事項」（P.3） • 「プロトコル サポート」（P.28） • 「仮想サーバの設定方法」（P.45） • 「GPRS ロード バランシングの設定作業リスト」（P.71）

表 2　IOS SLB の機能情報 （続き）

機能名	リリース	機能情報
GPRS ロード バランシング：マップ	12.2(33)SRB 12.2(33)SRC 12.2(33)SRC1 12.2(33)SRE 15.0(1)S	GPRS ロード バランシング マップによって、IOS SLB は Access Point Name（APN）に基づいてユーザ トラフィックを分類し、ルーティングできます。 この機能に関する詳細については、次の各項を参照してください。 • 「GPRS ロード バランシング」（P.32） • 「GPRS ロード バランシング マップの設定方法」（P.75） • 「例：GPRS ロード バランシング マップを使用した IOS SLB の設定方法」（P.172）
Home Agent Director	12.2(14)ZA2 12.2(14)ZA4 12.2(14)ZA5 12.2(14)ZA6 12.2(17d)SXB 12.2(17d)SXB1 12.2(17d)SXD 12.2(17d)SXE 12.2(18)SXF 12.2(18)SXF5 12.2(18)SXF7 12.2(33)SRB 12.2(33)SRC 12.2(33)SRC1 12.2(33)SRE 15.0(1)S	Home Agent Director は、ホーム エージェント セット（サーバ ファームの実サーバとして設定されます）の中で、Mobile IP Registration Request（RRQ）のロード バランシングを実行します。ホーム エージェントは、モバイル ノードのアンカー ポイントです。ホーム エージェントは、モバイル ノードのフローを現在の外部エージェント（接続ポイント）にルーティングします。 この機能に関する詳細については、次の各項を参照してください。 • 「Home Agent Director」（P.34） • 「Home Agent Director の設定作業リスト」（P.102） • 「例：Home Agent Director を使用した IOS SLB の設定方法」（P.184）
Hot ICE 準拠	12.2(33)SRE 15.0(1)S	すべての IOS SLB コマンドが Hot ICE 準拠です。Hot ICE は、Cisco IOS 設定管理の運用堅牢性、スケーラビリティ、およびプログラム可能性を向上させるように設計された Cisco IOS 設定機能強化のセットです。
仮想サーバの INOP_REAL 状態	12.2(33)SRC 12.2(33)SRC1 12.2(33)SRE 15.0(1)S	仮想サーバに関連付けられているすべての実サーバが非アクティブの場合、次のアクションを実行するように、仮想サーバを設定できます。 • 仮想サーバを INOP_REAL 状態に設定します。 • 仮想サーバの状態遷移について SNMP トラップを生成します。 • 仮想サーバは ICMP 要求に対する応答を停止します。 この機能に関する詳細については、次の各項を参照してください。 • 「仮想サーバの INOP_REAL 状態」（P.26） • 「仮想サーバの設定方法」（P.45）

表 2　IOS SLB の機能情報 （続き）

機能名	リリース	機能情報
インターフェイス認識	12.2(17d)SXE 12.2(18)SXF 12.2(18)SXF5 12.2(18)SXF7 12.2(33)SRB 12.2(33)SRC 12.2(33)SRC1 12.2(33)SRE 15.0(1)S	環境によっては、CSG、SSG、またはファイアウォールのファームの両側に IOS SLB が必要です。たとえば、ファームの一方で RADIUS ロード バランシングを実行し、もう一方でファイアウォール ロード バランシングを実行できます。また、ファイアウォール ファームの両側でファイアウォール ロード バランシングを実行することもできます。 このような「サンドイッチ」環境では、仮想サーバ、ファイアウォール ファーム、接続、およびセッションにパケットをマッピングするときに、IOS SLB で入力インターフェイスを考慮する必要があります。IOS SLB では、この機能はインターフェイス認識と呼ばれます。インターフェイス認識を設定すると、設定したアクセス インターフェイスに到達したトラフィックのみが処理されます（アクセス インターフェイスは任意のレイヤ 3 インターフェイスです）。 この機能に関する詳細については、次の各項を参照してください。 • 「インターフェイス認識」（P.17） • 「例：二重ファイアウォール ロード バランシング「サンドイッチ」を使用した IOS SLB の設定方法」（P.130） • 「例：RADIUS ロード バランシング / ファイアウォール ロード バランシング「サンドイッチ」を使用した IOS SLB の設定方法」（P.180）
KAL-AP エージェントのサポート	12.2(33)SRC 12.2(33)SRC1 12.2(33)SRE 15.0(1)S	KAL-AP エージェントのサポートによって、IOS SLB は Global Server Load Balancing（GSLB; グローバル サーバ ロード バランシング）環境でロード バランシングを実行できます。KAL-AP は、負荷情報とキープアライブ応答メッセージを KAL-AP マネージャまたは GSLB デバイス（Global Site Selector（GSS）など）に提供します。また、GSLB デバイスが、最も負荷が少ない IOS SLB デバイスにクライアント要求の負荷を分散できるように支援します。 この機能に関する詳細については、次の各項を参照してください。 • 「KeepAlive Application Protocol（KAL-AP）エージェントのサポート」（P.35） • 「KAL-AP エージェント サポートの設定方法」（P.77） • 「例：KAL-AP エージェントを使用した IOS SLB の設定方法」（P.186）

表 2　IOS SLB の機能情報 （続き）

機能名	リリース	機能情報
最大接続	12.2(1) 12.2(14)S 12.2(14)ZA2 12.2(14)ZA4 12.2(14)ZA5 12.2(14)ZA6 12.2(17d)SXB 12.2(17d)SXB1 12.2(17d)SXD 12.2(17d)SXE 12.2(18)SXF 12.2(18)SXF5 12.2(18)SXF7 12.2(33)SRB 12.2(33)SRC 12.2(33)SRC1 12.2(33)SRE 15.0(1)S	IOS SLB では、サーバおよびファイアウォール ロード バランシングの最大接続数を設定できます。この機能に関する詳細については、次の各項を参照してください。 • 「最大接続」（P.17） • 「サーバ ファームと実サーバの設定方法」（P.41） • 「ファイアウォール ファームの設定方法」（P.54） • 「例：包括的な IOS SLB ネットワークの設定方法」（P.123）
NAT：クライアント NAT	12.2(1) 12.2(14)S 12.2(14)ZA2 12.2(14)ZA4 12.2(14)ZA5 12.2(14)ZA6 12.2(17d)SXB 12.2(17d)SXB1 12.2(17d)SXD 12.2(17d)SXE 12.2(18)SXF 12.2(18)SXF5 12.2(18)SXF7 12.2(33)SRB 12.2(33)SRC 12.2(33)SRC1 12.2(33)SRE 15.0(1)S	ネットワークで複数のロード バランシング デバイスを使用している場合、クライアント IP アドレスを、デバイスのいずれかに関連付けられている IP アドレスで置換することで、発信フローが適切なデバイスにルーティングされます。また、クライアント NAT の場合、多数のクライアントが同じ一時ポートを使用できるため、一時クライアント ポートを変更する必要があります。複数のロード バランシング デバイスを使用しない場合でも、負荷が分散された接続のパケットがデバイス中をルーティングされないようにするには、クライアント NAT が便利です。 この機能に関する詳細については、次の各項を参照してください。 • 「クライアント NAT」（P.19） • 「NAT の設定方法」（P.104） • 「例：NAT とスタティック NAT を使用した IOS SLB の設定方法」（P.137）

表 2　IOS SLB の機能情報 （続き）

機能名	リリース	機能情報
NAT：サーバ NAT	12.2(1) 12.2(14)S 12.2(14)ZA2 12.2(14)ZA4 12.2(14)ZA5 12.2(14)ZA6 12.2(17d)SXB 12.2(17d)SXB1 12.2(17d)SXD 12.2(17d)SXE 12.2(18)SXF 12.2(18)SXF5 12.2(18)SXF7 12.2(33)SRB 12.2(33)SRC 12.2(33)SRC1 12.2(33)SRE 15.0(1)S	サーバ NAT には、仮想サーバの IP アドレスを実サーバの IP アドレスに置換する処理（およびその逆の処理）があります。 この機能に関する詳細については、次の各項を参照してください。 • 「サーバ NAT」（P.19） • 「NAT の設定方法」（P.104） • 「例：NAT とスタティック NAT を使用した IOS SLB の設定方法」（P.137）
NAT：スタティック NAT	12.2(14)S 12.2(14)ZA2 12.2(14)ZA4 12.2(14)ZA5 12.2(14)ZA6 12.2(17d)SXB 12.2(17d)SXB1 12.2(17d)SXD 12.2(17d)SXE 12.2(18)SXF 12.2(18)SXF5 12.2(18)SXF7 12.2(33)SRB 12.2(33)SRC 12.2(33)SRC1 12.2(33)SRE 15.0(1)S	スタティック NAT の場合、スタティック NAT コマンドを設定すると、アドレス変換は NAT 変換テーブルに登録され、スタティック NAT コマンドを削除するまで変換テーブルに保存されます。 この機能に関する詳細については、次の各項を参照してください。 • 「スタティック NAT」（P.19） • 「NAT の設定方法」（P.104） • 「例：スタティック NAT を使用した IOS SLB の設定方法」（P.140）

表 2　IOS SLB の機能情報 （続き）

機能名	リリース	機能情報
ポートバインド サーバ	12.2(1) 12.2(14)S 12.2(14)ZA2 12.2(14)ZA4 12.2(14)ZA5 12.2(14)ZA6 12.2(17d)SXB 12.2(17d)SXB1 12.2(17d)SXD 12.2(17d)SXE 12.2(18)SXF 12.2(18)SXF5 12.2(18)SXF7 12.2(33)SRB 12.2(33)SRC 12.2(33)SRC1 12.2(33)SRE 15.0(1)S	仮想サーバを定義するときに、そのサーバで管理する TCP ポートまたは UDP ポートを指定する必要があります。ただし、サーバ ファームで NAT を設定する場合、ポートバインド サーバを設定することもできます。ポートバインド サーバを使用すると、1 つの仮想サーバの IP アドレスで、HTTP などのサービス用の実サーバ セットと、Telnet などのサービス用の実サーバ セットを表現できます。 この機能に関する詳細については、次の各項を参照してください。 • 「ポートバインド サーバ」（P.21） • 「仮想サーバの設定方法」（P.45）
プローブ：カスタム UDP プローブ	12.2(14)ZA2 12.2(14)ZA4 12.2(14)ZA5 12.2(14)ZA6 12.2(17d)SXB 12.2(17d)SXB1 12.2(17d)SXD 12.2(17d)SXE 12.2(18)SXF 12.2(18)SXF5 12.2(18)SXF7 12.2(33)SRB 12.2(33)SRC 12.2(33)SRC1 12.2(33)SRE 15.0(1)S	IOS SLB プローブで、サーバ ファーム内の各実サーバのステータスと、ファイアウォール ファーム内の各ファイアウォールを判断します。 この機能に関する詳細については、次の各項を参照してください。 • 「プローブ」（P.27） • 「プローブの設定方法」（P.60） • 「例：プローブを使用した IOS SLB の設定方法」（P.132）

表 2　IOS SLB の機能情報 （続き）

機能名	リリース	機能情報
プローブ：DNS プローブ、Routed プローブ、および TCP プローブ	12.2(14)S 12.2(14)ZA2 12.2(14)ZA4 12.2(14)ZA5 12.2(14)ZA6 12.2(17d)SXB 12.2(17d)SXB1 12.2(17d)SXD 12.2(17d)SXE 12.2(18)SXF 12.2(18)SXF5 12.2(18)SXF7 12.2(33)SRB 12.2(33)SRC 12.2(33)SRC1 12.2(33)SRE 15.0(1)S	IOS SLB プローブで、サーバ ファーム内の各実サーバのステータスと、ファイアウォール ファーム内の各ファイアウォールを判断します。 この機能に関する詳細については、次の各項を参照してください。 • 「プローブ」（P.27） • 「プローブの設定方法」（P.60） • 「例：プローブを使用した IOS SLB の設定方法」（P.132）
プローブ：HTTP プローブ、ping プローブ、および WSP プローブ	12.2(1) 12.2(14)S 12.2(14)ZA2 12.2(14)ZA4 12.2(14)ZA5 12.2(14)ZA6 12.2(17d)SXB 12.2(17d)SXB1 12.2(17d)SXD 12.2(17d)SXE 12.2(18)SXF 12.2(18)SXF5 12.2(18)SXF7 12.2(33)SRB 12.2(33)SRC 12.2(33)SRC1 12.2(33)SRE 15.0(1)S	IOS SLB プローブで、サーバ ファーム内の各実サーバのステータスと、ファイアウォール ファーム内の各ファイアウォールを判断します。 この機能に関する詳細については、次の各項を参照してください。 • 「プローブ」（P.27） • 「プローブの設定方法」（P.60） • 「例：プローブを使用した IOS SLB の設定方法」（P.132）

表 2　IOS SLB の機能情報 （続き）

機能名	リリース	機能情報
プロトコル サポート	12.2(1) 12.2(14)S 12.2(14)ZA2 12.2(14)ZA4 12.2(14)ZA5 12.2(14)ZA6 12.2(17d)SXB 12.2(17d)SXB1 12.2(17d)SXD 12.2(17d)SXE 12.2(18)SXF 12.2(18)SXF5 12.2(18)SXF7 12.2(33)SRB 12.2(33)SRC 12.2(33)SRC1 12.2(33)SRE 15.0(1)S	IOS SLB がサポートするプロトコル セットは固定です。 この機能については、次の項に説明があります。 • 「プロトコル サポート」（P.28）
RADIUS ロード バランシング：加速データ プレーン フォワーディング	12.2(33)SRC 12.2(33)SRC1 12.2(33)SRE 15.0(1)S	RADIUS ロード バランシング加速データ プレーン フォワーディング（Turbo RADIUS ロード バランシングとも呼ばれる）は、CSG 環境で基本的な Policy-Based Routing（PBR; ポリシーベース ルーティング）ルート マップを使用して加入者のデータプレーン トラフィックを管理する高性能ソリューションです。Turbo RADIUS ロード バランシングが RADIUS ペイロードを受信すると、そのペイロードを検査して、framed-IP アトリビュートを抽出し、ルート マップを IP アドレスに適用してから、加入者を管理する CSG を決定します。 この機能に関する詳細については、次の各項を参照してください。 • 「RADIUS ロード バランシング加速データ プレーン フォワーディング」（P.38） • 「RADIUS ロード バランシング加速データ プレーン フォワーディングの設定方法」（P.86） • 「例：RADIUS ロード バランシング加速データ プレーン フォワーディングを使用した IOS SLB の設定方法」（P.182）

表 2　IOS SLB の機能情報 （続き）

機能名	リリース	機能情報
RADIUS ロード バランシング：CDMA2000	12.2(14)S 12.2(14)ZA2 12.2(14)ZA4 12.2(14)ZA5 12.2(14)ZA6 12.2(17d)SXB 12.2(17d)SXB1 12.2(17d)SXD 12.2(17d)SXE 12.2(18)SXF 12.2(18)SXF5 12.2(18)SXF7 12.2(33)SRB 12.2(33)SRC 12.2(33)SRC1 12.2(33)SRE 15.0(1)S	IOS SLB は、サービス ゲートウェイ（Cisco Service Selection Gateway（SSG）または Cisco Content Services Gateway（CSG））を使用するモバイル ワイヤレス ネットワークに RADIUS ロード バランシング機能を提供します。IOS SLB は、次の CDMA2000 モバイル ワイヤレス ネットワークについて RADIUS ロード バランシングをサポートします。 • 簡易 IP CDMA2000 ネットワーク。CDMA2000 は Third-Generation（3-G; 第 3 世代）バージョンの Code Division Multiple Access（CDMA; 符号分割多重接続）です。簡易 IP CDMA2000 モバイル ワイヤレス ネットワークの場合、RADIUS クライアントは Packet Data Service Node（PDSN）です。 • Mobile IP CDMA2000 ネットワーク。Mobile IP CDMA2000 モバイル ワイヤレス ネットワークの場合、Home Agent（HA）および PDSN/Foreign Agent（PDSN/FA）の両方が RADIUS クライアントです。 この機能に関する詳細については、次の各項を参照してください。 • 「RADIUS ロード バランシング」（P.36） • 「RADIUS ロード バランシングの設定作業リスト」（P.79） • 「例：簡易 IP CDMA2000 ネットワーク用の RADIUS ロード バランシングを使用した IOS SLB の設定方法」（P.177） • 「例：Mobile IP CDMA2000 ネットワーク用の RADIUS ロード バランシングを使用した IOS SLB の設定方法」（P.178）
RADIUS ロード バランシング：GPRS ネットワーク	12.2(14)S 12.2(14)ZA2 12.2(14)ZA4 12.2(14)ZA5 12.2(14)ZA6 12.2(17d)SXB 12.2(17d)SXB1 12.2(17d)SXD 12.2(17d)SXE 12.2(18)SXF 12.2(18)SXF5 12.2(18)SXF7 12.2(33)SRB 12.2(33)SRC 12.2(33)SRC1 12.2(33)SRE 15.0(1)S	IOS SLB は、サービス ゲートウェイ（Cisco Service Selection Gateway（SSG）または Cisco Content Services Gateway（CSG））を使用するモバイル ワイヤレス ネットワークに RADIUS ロード バランシング機能を提供します。IOS SLB は、GPRS ネットワークの場合、RADIUS ロード バランシングをサポートします。GPRS モバイル ワイヤレス ネットワークでは、RADIUS クライアントは通常 GGSN です。 この機能に関する詳細については、次の各項を参照してください。 • 「RADIUS ロード バランシング」（P.36） • 「RADIUS ロード バランシングの設定作業リスト」（P.79） • 「例：GPRS ネットワーク用の RADIUS ロード バランシングを使用した IOS SLB の設定方法」（P.175）

表 2　IOS SLB の機能情報 （続き）

機能名	リリース	機能情報
RADIUS ロード バランシング：マップ	12.2(33)SRB 12.2(33)SRC 12.2(33)SRC1 12.2(33)SRE 15.0(1)S	RADIUS ロード バランシング マップによって、IOS SLB は RADIUS 発信側ステーション ID とユーザ名に基づいてユーザ トラフィックを分類し、ルーティングすることができます。RADIUS ロード バランシング マップは、Turbo RADIUS ロード バランシングおよび RADIUS ロード バランシング アカウンティングのローカル ACK と同時に使用できません。 この機能に関する詳細については、次の各項を参照してください。 • 「RADIUS ロード バランシング」（P.36） • 「RADIUS ロード バランシング マップの設定方法」（P.84） • 「例 : RADIUS ロード バランシング マップを使用した IOS SLB の設定方法」（P.182）
RADIUS ロード バランシング：複数のサービス ゲートウェイ サーバ ファーム	12.2(14)S 12.2(14)ZA2 12.2(14)ZA4 12.2(14)ZA5 12.2(14)ZA6 12.2(17d)SXB 12.2(17d)SXB1 12.2(17d)SXD 12.2(17d)SXE 12.2(18)SXF 12.2(18)SXF5 12.2(18)SXF7 12.2(33)SRB 12.2(33)SRC 12.2(33)SRC1 12.2(33)SRE 15.0(1)S	IOS SLB は、サービス ゲートウェイ（Cisco Service Selection Gateway（SSG）または Cisco Content Services Gateway（CSG））を使用するモバイル ワイヤレス ネットワークに RADIUS ロード バランシング機能を提供します。IOS SLB は、複数のサービス ゲートウェイ サーバ ファームの場合に RADIUS ロード バランシングをサポートします（たとえば、SSG ファームと CSG ファーム）。 この機能に関する詳細については、次の各項を参照してください。 • 「RADIUS ロード バランシング」（P.36） • 「RADIUS ロード バランシングの設定作業リスト」（P.79） • 「例 : 複数のサービス ゲートウェイ サーバ ファーム用の RADIUS ロード バランシングを使用した IOS SLB の設定方法」（P.179）
RADIUS ロード バランシング：RADIUS IMSI スティッキ データベース	12.2(17d)SXE 12.2(18)SXF 12.2(18)SXF5 12.2(18)SXF7 12.2(33)SRB 12.2(33)SRC 12.2(33)SRC1 12.2(33)SRE 15.0(1)S	IOS SLB RADIUS International Mobile Subscriber ID（IMSI）は、各ユーザの IMSI アドレスを対応するゲートウェイにルーティングします。その結果、同じユーザに対する以降のすべてのフローを同じゲートウェイに転送できるようになります。 この機能に関する詳細については、次の各項を参照してください。 • 「RADIUS ロード バランシング」（P.36） • 「RADIUS ロード バランシングの設定作業リスト」（P.79）

表 2　IOS SLB の機能情報 （続き）

機能名	リリース	機能情報
ルート ヘルス インジェクション	12.2(14)S 12.2(14)ZA2 12.2(14)ZA4 12.2(14)ZA5 12.2(14)ZA6 12.2(17d)SXB 12.2(17d)SXB1 12.2(17d)SXD 12.2(17d)SXE 12.2(18)SXF 12.2(18)SXF5 12.2(18)SXF7 12.2(33)SRB 12.2(33)SRC 12.2(33)SRC1 12.2(33)SRE 15.0(1)S	（**inservice** コマンドを使用して）仮想サーバをサービスに登録すると、デフォルトで、仮想サーバの IP アドレスがアドバタイズされます（ルーティング テーブルに追加されます）。Web サイトの仮想 IP アドレスに対して希望のホスト ルートがある場合、そのホスト ルートをアドバタイズできますが、その IP アドレスを使用できるという保証はありません。ただし、IP アドレスを使用できると IOS SLB で検証された場合にだけ、ホスト ルートをアドバタイズするように、**advertise** コマンドで IOS SLB を設定できます。IP アドレスを使用できなくなると、IOS SLB はアドバタイズメントを撤回します。この機能はルート ヘルス インジェクションと呼ばれます。 この機能に関する詳細については、次の各項を参照してください。 • 「ルート ヘルス インジェクション」（P.21） • 「仮想サーバの設定方法」（P.45） • 「例：ルート ヘルス インジェクションを使用した IOS SLB の設定方法」（P.160）
スロー スタート	12.2(1) 12.2(14)S 12.2(14)ZA2 12.2(14)ZA4 12.2(14)ZA5 12.2(14)ZA6 12.2(17d)SXB 12.2(17d)SXB1 12.2(17d)SXD 12.2(17d)SXE 12.2(18)SXF 12.2(18)SXF5 12.2(18)SXF7 12.2(33)SRB 12.2(33)SRC 12.2(33)SRC1 12.2(33)SRE 15.0(1)S	加重最小接続ロード バランシングを使用する環境では、起動した直後の実サーバには接続がないため、新しい接続が多数割り当てられ、過負荷になる可能性があります。このような過負荷を回避するために、スロー スタートによって、起動した直後の実サーバに割り当てられる新しい接続数を制御します。 この機能については、次の項に説明があります。 • 「スロー スタート」（P.23）

表 2　IOS SLB の機能情報 （続き）

機能名	リリース	機能情報
ステートフル バックアップ	12.2(1) 12.2(14)S 12.2(14)ZA2 12.2(14)ZA4 12.2(14)ZA5 12.2(14)ZA6 12.2(17d)SXB 12.2(17d)SXB1 12.2(17d)SXD 12.2(17d)SXE 12.2(18)SXF 12.2(18)SXF5 12.2(18)SXF7 12.2(33)SRB 12.2(33)SRC 12.2(33)SRC1 12.2(33)SRE 15.0(1)S	ステートフル バックアップを使用すると、ロード バランシングの決定を段階的にバックアップするか、プライマリ スイッチとバックアップ スイッチ間で「状態を維持」できます。バックアップ スイッチは、HSRP がフェールオーバーを検出するまで、仮想サーバを休止状態にしたままにします。検出後、バックアップ（現在はプライマリ）スイッチは、仮想アドレスのアドバタイズとフローの処理を開始します。 この機能に関する詳細については、次の各項を参照してください。 • 「ステートフル バックアップ」（P.30） • 「冗長ルート プロセッサのステートフル バックアップの設定作業リスト」（P.108） • 「例：ステートフル バックアップを使用した IOS SLB の設定方法」（P.150） • 「例：冗長ルート プロセッサのステートフル バックアップを使用した IOS SLB の設定方法」（P.152）
ステートフル バックアップ：冗長ルート プロセッサ	12.2(14)ZA5 12.2(14)ZA6 12.2(17d)SXB 12.2(17d)SXB1 12.2(17d)SXD 12.2(17d)SXE 12.2(18)SXF 12.2(18)SXF5 12.2(18)SXF7 12.2(33)SRB 12.2(33)SRC 12.2(33)SRC1 12.2(33)SRE 15.0(1)S	Cisco 7600 シリーズ ルータで、RPR+ を併用する場合、IOS SLB は mSEF について冗長ルート プロセッサのステートフル バックアップをサポートします。これによって、IOS SLB と同じシャーシに、Cisco Multiprocessor WAN Application Module（MWAN）を配置し、さらにロード バランシング割り当てのハイ アベイラビリティを維持できます。 この機能に関する詳細については、次の各項を参照してください。 • 「冗長ルート プロセッサのステートフル バックアップ」（P.39） • 「冗長ルート プロセッサのステートフル バックアップの設定作業リスト」（P.108） • 「例：冗長ルート プロセッサのステートフル バックアップを使用した IOS SLB の設定方法」（P.152）

表 2　IOS SLB の機能情報 （続き）

機能名	リリース	機能情報
ステートレス バックアップ	12.2(1) 12.2(14)S 12.2(14)ZA2 12.2(14)ZA4 12.2(14)ZA5 12.2(14)ZA6 12.2(17d)SXB 12.2(17d)SXB1 12.2(17d)SXD 12.2(17d)SXE 12.2(18)SXF 12.2(18)SXF5 12.2(18)SXF7 12.2(33)SRB 12.2(33)SRC 12.2(33)SRC1 12.2(33)SRE 15.0(1)S	ステートレス バックアップは、1 台のレイヤ 3 スイッチの可用性に依存せずに、イーサネット ネットワーク上のホストからの IP フローをルーティングすることによって、ネットワークの高可用性を実現します。Router Discovery Protocol（System-to-Intermediate System（IS-IS）Interdomain Routing Protocol（IDRP）など）をサポートしないホストで、新しいレイヤ 3 スイッチにシフトする機能がない場合は特に、ステートレス バックアップが有効です。 この機能に関する詳細については、次の各項を参照してください。 • 「ステートレス バックアップ」（P.30） • 「ステートレス バックアップの設定作業リスト」（P.106） • 「例：ステートレス バックアップを使用した IOS SLB の設定方法」（P.141）
スティッキ接続	12.2(1) 12.2(14)S 12.2(14)ZA2 12.2(14)ZA4 12.2(14)ZA5 12.2(14)ZA6 12.2(17d)SXB 12.2(17d)SXB1 12.2(17d)SXD 12.2(17d)SXE 12.2(18)SXF 12.2(18)SXF5 12.2(18)SXF7 12.2(33)SRB 12.2(33)SRC 12.2(33)SRC1 12.2(33)SRE 15.0(1)S	クライアント トランザクションには、複数の連続する接続が必要なことがあります。つまり、同じクライアントの IP アドレスまたはサブネットからの新しい接続を、同じ実サーバに割り当てる必要があります。オプションの **sticky** コマンドを使用すると、同じクライアントからの発信を、サーバ ファーム内の同じロード バランシング サーバに強制的に接続できます。ファイアウォール ロード バランシングの場合、同じクライアント - サーバ ペア間の接続は、同じファイアウォールに割り当てられます。 この機能に関する詳細については、次の各項を参照してください。 • 「スティッキ接続」（P.21） • 「サーバ ファームと実サーバの設定方法」（P.41） • 「仮想サーバの設定方法」（P.45） • 「ファイアウォール ファームの設定方法」（P.54） • 「例：スティッキ接続を使用した IOS SLB の設定方法」（P.184）
サブインターフェイスのサポート	12.2(33)SRE 15.0(1)S	IOS SLB は、**access** コマンドについてサブインターフェイスのサポートを提供しています。 この機能に関する詳細については、次の各項を参照してください。 • 「サーバ ファームと実サーバの設定方法」（P.41） • 「仮想サーバの設定方法」（P.45） • 「ファイアウォール ファームの設定方法」（P.54） この機能によって、次のコマンドが変更されました。 **access**（ファイアウォール ファーム）、**access**（サーバ ファーム）、**access**（仮想サーバ）

表 2　IOS SLB の機能情報 （続き）

機能名	リリース	機能情報
12.2(1) と 12.2(14)S に対してサポートされているプラットフォーム	12.2(1) 12.2(14)S	次のプラットフォームに対するサポートのみが含まれる一覧表示されたリリースの IOS SLB： • Cisco 7200 シリーズ ルータ
12.2(14)ZA2、 12.2(14)ZA2、 12.2(14)ZA4、 12.2(14)ZA5、および 12.2(14)ZA6 に対してサポートされているプラットフォーム	12.2(14)ZA2 12.2(14)ZA4 12.2(14)ZA5 12.2(14)ZA6	次のプラットフォームに対するサポートのみが含まれる一覧表示されたリリースの IOS SLB： • Cisco 7100 シリーズ ルータ • Cisco 7200 シリーズ ルータ • Cisco Catalyst 6500 シリーズ スイッチ用の MSFC2 が搭載された Supervisor Engine 1 • Cisco Catalyst 6500 シリーズ スイッチ用の MSFC2 が搭載された Supervisor Engine 2（SUP2-MSFC2） • Cisco 7600 シリーズ ルータ用の MSFC2 搭載の Supervisor Engine 1 • Cisco 7600 シリーズ ルータ用の MSFC2 搭載の Supervisor Engine 2（SUP2-MSFC2）
12.2(17d)SXB と 12.2(17d)SXB1 に対してサポートされているプラットフォーム	12.2(17d)SXB 12.2(17d)SXB1	次のプラットフォームに対するサポートのみが含まれる一覧表示されたリリースの IOS SLB： • Cisco Catalyst 6500 シリーズ スイッチ用の MSFC2 が搭載された Supervisor Engine 2（SUP2-MSFC2） • Cisco 7600 シリーズ ルータ用の MSFC2 搭載の Supervisor Engine 2（SUP2-MSFC2）
12.2(17d)SXD、 12.2(17d)SXE、および 12.2(18)SXF に対してサポートされているプラットフォーム	12.2(17d)SXD 12.2(17d)SXE 12.2(18)SXF	次のプラットフォームに対するサポートのみが含まれる一覧表示されたリリースの IOS SLB： • Cisco Catalyst 6500 シリーズ スイッチ用の MSFC2 が搭載された Supervisor Engine 2（SUP2-MSFC2） • Cisco Catalyst 6500 シリーズ スイッチ用の MSFC3 が搭載された Supervisor Engine 720（SUP720-MSFC3） • Cisco 7600 シリーズ ルータ用の MSFC2 搭載の Supervisor Engine 2（SUP2-MSFC2） • Cisco 7600 シリーズ ルータ用の MSFC3 搭載の Supervisor Engine 720（SUP720-MSFC3）

表 2　IOS SLB の機能情報 （続き）

機能名	リリース	機能情報
12.2(17d)SXF5 と 12.2(18)SXF7 に対してサポートされているプラットフォーム	12.2(18)SXF5 12.2(18)SXF7	次のプラットフォームに対するサポートのみが含まれる一覧表示されたリリースの IOS SLB： • Cisco Catalyst 6500 シリーズ スイッチ用の MSFC2 が搭載された Supervisor Engine 2（SUP2-MSFC2） • Cisco Catalyst 6500 シリーズ スイッチ用の MSFC2A が搭載された Supervisor Engine 32（SUP32-MSFC2A） • Cisco Catalyst 6500 シリーズ スイッチ用の MSFC3 が搭載された Supervisor Engine 720（SUP720-MSFC3） • Cisco 7600 シリーズ ルータ用の MSFC2 搭載の Supervisor Engine 2（SUP2-MSFC2） • Cisco 7600 シリーズ ルータ用の MSFC2A 搭載の Supervisor Engine 32（SUP32-MSFC2A） • Cisco 7600 シリーズ ルータ用の MSFC3 搭載の Supervisor Engine 720（SUP720-MSFC3）
12.2(33)SRB に対してサポートされているプラットフォーム	12.2(33)SRB	次のプラットフォームに対するサポートのみが含まれる一覧表示されたリリースの IOS SLB： • Cisco 7600 シリーズ ルータ用の MSFC2A 搭載の Supervisor Engine 32（SUP32-MSFC2A） • Cisco 7600 シリーズ ルータ用の MSFC3 搭載の Supervisor Engine 720（SUP720-MSFC3）
12.2(33)SRC、12.2(33)SRC1、12.2(33)SRE、および 15.0(1)S に対してサポートされているプラットフォーム	12.2(33)SRC 12.2(33)SRC1 12.2(33)SRE 15.0(1)S	次のプラットフォームに対するサポートのみが含まれる一覧表示されたリリースの IOS SLB： • Cisco 7600 シリーズ ルータ用の MSFC2A 搭載の Supervisor Engine 32（SUP32-MSFC2A） • Cisco 7600 シリーズ ルータ用の MSFC3 搭載の Supervisor Engine 720（SUP720-MSFC3） • 2 つのギガビット イーサネット ポートを搭載した Distributed Forwarding Card DFC3CXL 付きの Cisco Route Switch Processor 720（RSP720-3CXL-GE）

表 2　IOS SLB の機能情報 （続き）

機能名	リリース	機能情報
SynGuard	12.2(1) 12.2(14)S 12.2(14)ZA2 12.2(14)ZA4 12.2(14)ZA5 12.2(14)ZA6 12.2(17d)SXB 12.2(17d)SXB1 12.2(17d)SXD 12.2(17d)SXE 12.2(18)SXF 12.2(18)SXF5 12.2(18)SXF7 12.2(33)SRB 12.2(33)SRC 12.2(33)SRC1 12.2(33)SRE 15.0(1)S	SynGuard は、仮想サーバによって管理される TCP start-of-connection パケット（SYN）のレートを制限して、SYN フラッド サービス拒否攻撃と呼ばれるネットワーク上の問題を阻止します。ユーザが大量の SYN をサーバに送信することもあり、それによってサーバの過負荷やクラッシュが発生し、他のユーザへのサービスが停止する可能性があります。SynGuard によって、IOS SLB または実サーバを停止させる攻撃などを回避します。SynGuard は、仮想サーバによって管理される SYN 数を一定間隔でモニタして、その数が、設定された SYN しきい値を超えないようにします。しきい値に達すると、新しい SYN はドロップされます。 この機能に関する詳細については、次の各項を参照してください。 • 「SynGuard」（P.24） • 「仮想サーバの設定方法」（P.45） • 「例：包括的な IOS SLB ネットワークの設定方法」（P.123）
TCP セッションの再割り当て	12.2(1) 12.2(14)S 12.2(14)ZA2 12.2(14)ZA4 12.2(14)ZA5 12.2(14)ZA6 12.2(17d)SXB 12.2(17d)SXB1 12.2(17d)SXD 12.2(17d)SXE 12.2(18)SXF 12.2(18)SXF5 12.2(18)SXF7 12.2(33)SRB 12.2(33)SRC 12.2(33)SRC1 12.2(33)SRE 15.0(1)S	クライアントが実サーバに対して新しい接続を開こうとしている場合、そのサーバに送信される各 TCP SYN は IOS SLB によって追跡されます。複数の連続する SYN に応答がない場合、または SYN が RST で応答される場合、TCP セッションは新しい実サーバに再割り当てされます。SYN の試行回数は、設定可能な再割り当てしきい値で制御されます。 この機能に関する詳細については、次の各項を参照してください。 • 「TCP セッションの再割り当て」（P.22） • 「サーバ ファームと実サーバの設定方法」（P.41） • 「GPRS ロード バランシングの設定作業リスト」（P.71）

表 2　IOS SLB の機能情報 （続き）

機能名	リリース	機能情報
透過的 Web キャッシュ ロード バランシング	12.2(1) 12.2(14)S 12.2(14)ZA2 12.2(14)ZA4 12.2(14)ZA5 12.2(14)ZA6 12.2(17d)SXB 12.2(17d)SXB1 12.2(17d)SXD 12.2(17d)SXE 12.2(18)SXF 12.2(18)SXF5 12.2(18)SXF7 12.2(33)SRB 12.2(33)SRC 12.2(33)SRC1 12.2(33)SRE 15.0(1)S	IOS SLB は、透過的 Web キャッシュのクラスタ全体で HTTP フローの負荷を分散できます。この機能をセットアップするには、透過的 Web キャッシュで処理するサブネット IP アドレス、または何らかの共通するサブセットを仮想サーバとして設定します。透過的 Web キャッシュ ロード バランシングに使用する仮想サーバは、サブネット IP アドレスの代理で ping に応答しません。また、トレースルートに影響がありません。 この機能に関する詳細については、次の各項を参照してください。 • 「透過的 Web キャッシュ ロード バランシング」（P.22） • 「仮想サーバの設定方法」（P.45） • 「例：透過的 Web キャッシュ ロード バランシングを使用した IOS SLB の設定方法」（P.186）
VPN サーバ ロード バランシング	12.2(14)S 12.2(14)ZA2 12.2(14)ZA4 12.2(14)ZA5 12.2(14)ZA6 12.2(17d)SXB 12.2(17d)SXB1 12.2(17d)SXD 12.2(17d)SXE 12.2(18)SXF 12.2(18)SXF5 12.2(18)SXF7 12.2(33)SRB 12.2(33)SRC 12.2(33)SRC1 12.2(33)SRE 15.0(1)S	IOS SLB は、VPN フローのバランスを取ることができます。 この機能に関する詳細については、次の各項を参照してください。 • 「VPN サーバ ロード バランシング」（P.30） • 「VPN サーバ ロード バランシングの設定作業リスト」（P.99） • 「例 : VPN サーバ ロード バランシングを使用した IOS SLB の設定方法」（P.174）

表 2　IOS SLB の機能情報 （続き）

機能名	リリース	機能情報
WAP ロード バランシング	12.2(1) 12.2(14)S 12.2(14)ZA2 12.2(14)ZA4 12.2(14)ZA5 12.2(14)ZA6 12.2(17d)SXB 12.2(17d)SXB1 12.2(17d)SXD 12.2(17d)SXE 12.2(18)SXF 12.2(18)SXF5 12.2(18)SXF7 12.2(33)SRB 12.2(33)SRC 12.2(33)SRC1 12.2(33)SRE 15.0(1)S	IOS SLB を使用すると、IP ベアラ ネットワークの WAP ゲートウェイまたはサーバのグループ内で、Wireless Session Protocol（WSP）セッションの負荷を分散できます。 この機能に関する詳細については、次の各項を参照してください。 • 「WAP ロード バランシング」（P.39） • 「仮想サーバの設定方法」（P.45） • 「WSP プローブの設定方法」（P.67） • 「例：WAP および UDP ロード バランシングを使用した IOS SLB の設定方法」（P.158）
—	12.2(14)ZA6 12.2(18)SXF 12.2(18)SXF5 12.2(18)SXF7	これらのリリースには、マイナーな修正と明確化が施されているだけです。新しい機能は導入されていません。

拡張オブジェクト トラッキングの設定

Enhanced Object Tracking（EOT; 拡張オブジェクト トラッキング）機能が導入される前は、Hot Standby Router Protocol（HSRP; ホット スタンバイ ルータ プロトコル）がシンプルなトラッキング メカニズムを提供していました。HSRP では、インターフェイス ライン プロトコル ステートのみの追跡が可能でした。インターフェイスのライン プロトコル ステートがダウンすると、ルータの HSRP プライオリティが低くなり、よりプライオリティの高い他の HSRP ルータがアクティブになります。

拡張オブジェクト トラッキング機能は、HSRP からトラッキング メカニズムを分離させて、独立したトラッキング プロセスを別途生成します。これにより、HSRP 以外の Cisco IOS プロセスがこのトラッキング プロセスを使用できます。この機能を使用すると、インターフェイスのラインプロトコル ステートに加えて他のオブジェクトも追跡できます。

HSRP、Virtual Router Redundancy Protocol（VRRP; 仮想ルータ冗長プロトコル）、Gateway Load Balancing Protocol（GLBP; ゲートウェイ ロード バランシング プロトコル）などのクライアント プロセスは、オブジェクトのトラッキングを登録し、トラッキング対象オブジェクトのステートが変化したときに通知を得ることができるようになっています。

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、「拡張オブジェクト トラッキングの機能情報」（P.32）を参照してください。

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

この章の構成

拡張オブジェクト トラッキングの制約事項

拡張オブジェクト トラッキングはステートフル スイッチオーバー（SSO）を認識しないため、SSO モードで Hot Standby Routing Protocol（HSRP; ホット スタンバイ ルーティング プロトコル）、Virtual Router Redundancy Protocol（VRRP; 仮想ルータ冗長プロトコル）、または Gateway Load Balancing Protocol（GLBP; ゲートウェイ ロード バランシング プロトコル）と併用することはできません。

拡張オブジェクト トラッキングの概要

拡張オブジェクト トラッキングの機能設計

拡張オブジェクト トラッキングでは、追跡対象のオブジェクトと、追跡対象のオブジェクトのステートが変化したときにクライアントがとるアクションを完全に分離します。このため、HSRP、VRRP、GLPB のようなクライアントは、対象とするトラッキング プロセスを登録し、同じオブジェクトを追跡して、オブジェクトが変更されたときにそれぞれ異なるアクションを実行できます。

各追跡対象オブジェクトには、トラッキング CLI（コマンドライン インターフェイス）で指定される一意の番号があります。クライアント プロセスは、この番号を使用して特定のオブジェクトを追跡します。

トラッキング プロセスは、追跡対象オブジェクトを定期的にポーリングし、値に変化がないかどうかを確認します。追跡対象オブジェクトに変化があれば登録されているクライアント プロセスに通知します。ただちに通知する場合と、指定された時間遅延後に通知する場合があります。オブジェクトの値は、アップまたはダウンとして報告されます。

複数のオブジェクトを組み合わせて 1 つのリストにして追跡することもできます。オブジェクトの組み合わせにはブール ロジックを使用して、柔軟性をもたせることができます。この機能性には、次の機能が含まれます。

- しきい値：追跡リストは、リストのステート判定に重みしきい値またはパーセントを使用するように設定できます。追跡リスト内の各オブジェクトに、重みしきい値を割り当てることができます。追跡リストのステートは、しきい値が満たされているかどうかで判断されます。
- 「AND」ブール関数：「AND」ブール関数を使用する追跡リストの場合、サブセット内に定義されている各オブジェクトがアップ ステートでないと追跡対象オブジェクトはアップになりません。

- 「OR」ブール関数：「OR」ブール関数を使用する追跡リストの場合、サブセット内に定義されている中で少なくとも 1 つのオブジェクトがアップ ステートであれば追跡対象オブジェクトはアップになります。

Cisco IOS Release 15.1(3)T 以降は、最大 1000 個のオブジェクトを追跡することができます。1000 個の追跡対象オブジェクトを設定できますが、オブジェクトごとに CPU リソースが使用されます。ルータ上で使用可能な CPU リソースの量は、トラフィックの負荷やその他のプロトコルがどのように設定され、実行されているかなどの変数に依存します。1000 個の追跡対象オブジェクトが使用できるかどうかは、使用可能な CPU によって異なります。特定のサイト トラフィック条件下でサービスが機能することを保証するには、サイト上でテストを実施する必要があります。

数値化ルート メトリック

track ip route コマンドを使用すると、ルーティング テーブル内のルートを追跡できます。ルートがテーブルに存在する場合、メトリック値が数値に変換されます。追跡クライアントに共通インターフェイスを提供するために、ルート メトリック値が 0 ～ 255 の範囲に正規化されます。ここで、0 は接続されていることを示し、255 はアクセス不可であることを示します。数値化メトリックは、しきい値を設定することで追跡できます。しきい値を超えると、アップ/ダウン ステートが通知されます。結果の値は、しきい値と比較され、次のようにトラッキング ステートが決定されます。

- 対象ルートの数値化メトリックがアップ ステートのしきい値以下のときは、ステートはアップになります。
- 対象ルートの数値化メトリックがダウン ステートのしきい値以上のときは、ステートはダウンになります。

追跡では、プロトコルごとに設定可能な解析値を使用して、実メトリックが数値化メトリックに変換されます。表 1 に、この変換に使用されるデフォルト値を示します。**track resolution** コマンドを使用して、メトリック解析のデフォルト値を変更できます。

表 1　　メトリック変換

ルート タイプ[1]	メトリック解析
スタティック	10
Enhanced Interior Gateway Routing Protocol（EIGRP）	2560
Open Shortest Path First（OSPF）	1
Intermediate System-to-Intermediate System（IS-IS）	10

1. RIP は、0 ～ 255 の範囲に直接数値化されます。これは、最大メトリックが 255 未満であるためです。

たとえば、IS-IS メトリックの変化が 10 の場合は、数値化メトリックの変化が 1 になります。デフォルトの解析値は、パス内の大体 1 つの 2-Mbps リンクが 255 の数値化メトリックになるように設計されています。

EIGRP のメトリック範囲を大きく設定し、IS-IS のメトリック範囲を 0 ～ 255 に設定することで、調整を行っています。デフォルトの解析値によって、数値化メトリックが 2-Mbps リンクの上限を超える可能性があります。ただし、この数値化により、3 つのファスト イーサネット リンクで構成されるルートと、4 つのファスト イーサネット リンクで構成されるルートを区別できます。

IP SLA 動作トラッキング

IP SLA 動作のオブジェクト トラッキングでは、追跡クライアントが IP SLA オブジェクトからの出力を追跡し、提供された情報を使用してアクションをトリガーすることができます。

Cisco IOS IP SLA は、アクティブ モニタリングを使用してネットワーク パフォーマンスの測定および診断を行うツールです。アクティブ モニタリングは信頼性のある予測可能な方法でトラフィックを生成し、ネットワーク パフォーマンスを測定します。Cisco IOS ソフトウェアは IP SLA を使用して、応答時間、ネットワーク リソースの可用性、アプリケーション パフォーマンス、ジッタ（パケット内遅延の分散）、接続時間、スループット、パケット損失などのリアルタイム メトリックを収集します。

これらのメトリックは、トラブルシューティング、問題発生前の予防的分析、ネットワーク トポロジの設計などに使用できます。

動作の戻りコード値は、すべての IP SLA 動作で保持されます。この戻りコードは、トラッキング プロセスによって解釈されます。返される戻りコードには、OK、OverThreshold などがあります。戻りコードの値は動作によって異なる場合があるため、すべての動作タイプに共通する値だけが使用されます。

IP SLA 動作の 2 つの側面（状態および到達可能性）をトラッキングできます。両者の違いは、OverThreshold 戻りコードを受信できるかどうかです。表 2 に、トラッキング可能な IP SLA 動作の状態および到達可能性を示します。

表 2　状態動作と到達可能性動作の比較

トラッキング	戻りコード	トラッキングの状態
状態	OK	アップ
	（その他のすべての戻りコード）	ダウン
到達可能性	OK または OverThreshold	アップ
	（その他のすべての戻りコード）	ダウン

拡張オブジェクト トラッキングおよび Embedded Event Manager

Cisco IOS Release 12.4(2)T 以降、拡張オブジェクト トラッキング（EOT）は Embedded Event Manager（EEM）と併用できるようになったため、追跡対象オブジェクトのステータス変更を EEM に報告させ、EOT に EEM オブジェクトを追跡させることができるようになりました。新たに導入されたタイプのトラッキング オブジェクト（スタブ オブジェクト）が作成されます。スタブ オブジェクトは、定義された Application Programming Interface（API; アプリケーション プログラミング インターフェイス）経由の外部プロセスによる変更が可能です。EOT がどのように EEM と連動するかの詳細については、『*Cisco IOS Network Management Configuration Guide*』の「Embedded Event Manager Overview」を参照してください。

EOT によるキャリア遅延サポート

EOT によるキャリア遅延サポート機能により、拡張オブジェクト トラッキング（EOT）はインターフェイスのステータスを追跡するときにキャリア遅延タイマーを考慮に入れることができます。

リンクがダウンした場合、デフォルトでは、2 秒タイマーが作動してから、インターフェイスおよび関連付けられたルートのダウンが宣言されます。リンクがダウンしても、キャリア遅延タイマーが切れる前に再度アップ ステートに戻った場合は、ダウン ステートは効率的にフィルタリングされ、スイッチ上の他のソフトウェアは発生したリンクダウン イベントを認識しません。インターフェイス コンフィギュレーション モードで carrier-delay seconds コマンドを設定し、タイマーを最大 60 秒まで延長できます。

インターフェイスに EOT が設定されている場合、追跡によって、設定済みのキャリア遅延タイマーが切れる前にダウンしたインターフェイスが検出されることがあります。この状況は、EOT がキャリア遅延タイマーを考慮せず、インターフェイス ステートを監視しているために発生します。このような場合は、トラッキング コンフィギュレーション モードで **carrier-delay** コマンドを使用して、インターフェイスに設定されているキャリア遅延タイマーが追跡で考慮されるようにします。

Mobile IP アプリケーションの拡張オブジェクト トラッキング

Enhanced Object Tracking Support for Mobile IP 機能を使用すると、EOT がルータ上にモバイル ワイヤレス アプリケーション用の Home Agent、Packet Data Serving Node（PDSN）、または Gateway GPRS Support Node（GGSN）トラフィックのプレゼンスをモニタできます。

ノード間で HSRP を実行している Home Agent の冗長ペアの接続が失われると、両方の HSRP ノードがアクティブになります。2 つのノード間の接続が復元すると、Home Agent のバインディングを失わずに適切な HSRP ステートを復元するための方法が必要になります。接続が失われている間は、一方のノードでは Home Agent、GGSN、または PDSN トラフィックの処理が継続して行われますが、もう一方のノードでの処理は行われません。トラフィック処理を継続するノードは、接続が復元された後もアクティブの状態を保つ必要があります。アクティブなノードが確実にアクティブ ステートを保持できるように、Home Agent トラフィック処理を行わない HSRP グループ メンバーのプライオリティは低く設定されます。Home Agent トラフィック処理を行わないノードのプライオリティを下げることで、このノードは、接続が復元するとスダンバイ モードになるように設定されます。接続が復元すると、通常の Home Agent ステート同期により、すべてのバインディングは非アクティブ ノードになります。プリエンプト コンフィギュレーションによっては、再び切り替えが生じることがあります。このステート同期により、Mobile IP、GGSN、または PDSN バインディングが失われなくなります。

Mobile IP サービスの設定の詳細については、次の Cisco IOS コンフィギュレーション ガイドを参照してください。

- 『*Cisco IOS Mobile Wireless Home Agent Configuration Guide*』
- 『*Cisco IOS Mobile Wireless Gateway GPRS Support Node Configuration Guide*』
- 『*Cisco IOS Mobile Wireless Packet Data Serving Node Configuration Guide*』
- 『*Cisco IOS IP Mobility Configuration Guide*』

拡張オブジェクト トラッキングの利点

- ネットワークの可用性および復元速度を高める。
- ネットワークが停止する頻度が少なくなり、また、停止時間が短くなる。
- VRRP や GLBP などのクライアント プロセスがオブジェクトを個別に追跡したり、オブジェクトのリストとして追跡したりできるような、スケーラブルなソリューションを提供する。この機能を導入する前に、トラッキング プロセスは HSRP に組み込まれています。

拡張オブジェクト トラッキングの設定方法

インターフェイスのライン プロトコル ステートの追跡

インターフェイスのライン プロトコル ステートを追跡するには、次の手順を実行します。

track interface ip routing コマンドを使用してインターフェイスの IP ルーティング ステートを追跡する方法は、**track interface line-protocol** コマンドを使用してライン プロトコル ステートを追跡する方法と比較して、状況によっては、より効果的になることがあります。アドレスのネゴシエーションが行われるインターフェイスでは、特に役立ちます。詳細については、「インターフェイスの IP ルーティング ステートの追跡」を参照してください。

また、インターフェイスのライン プロトコル ステートを追跡する場合に、トラッキング コンフィギュレーション モードで **carrier-delay** コマンドを使用することで、EOT がキャリア遅延タイマーを考慮するように設定することもできます。

手順の概要

1. **enable**
2. **configure terminal**
3. **track timer interface** *seconds* | **msec** *milliseconds*}
4. **track** *object-number* **interface** *type number* **line-protocol**
5. **carrier-delay**
6. **delay** {**up** *seconds* [**down** *seconds*] | [**up** *seconds*] **down** *seconds*}
7. **end**
8. **show track** *object-number*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**track timer interface** *seconds* | **msec** *milliseconds*} **例：** `Router(config)# track timer interface 5`	（任意）トラッキング プロセスが追跡対象オブジェクトをポーリングする間隔を指定します。 • トラッキング プロセスがインターフェイス オブジェクトをポーリングするデフォルトのインターバルは 1 秒です。 **（注）** すべてのポーリング頻度は、以前 **msec** キーワードと *milliseconds* 引数を使用して設定された最小 1 秒インターバルを上回る 500 ミリ秒に下げて設定することができます。
ステップ 4	**track** *object-number* **interface** *type number* **line-protocol** **例：** `Router(config)# track 3 interface ethernet 0/1 line-protocol`	インターフェイスのライン プロトコル ステートを追跡し、トラッキング 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	**carrier-delay** **例：** `Router(config-track)# carrier-delay`	（任意）インターフェイスのステータスを追跡するときに、EOT がキャリア遅延タイマーを考慮するように設定します。
ステップ 6	**delay** {**up** *seconds* [**down** *seconds*] | [**up** *seconds*] **down** *seconds*} **例：** `Router(config-track)# delay up 30`	（任意）追跡対象オブジェクトのステート変更の通信を遅延させる時間（秒）を指定します。
ステップ 7	**end** **例：** `Router(config-track)# end`	特権 EXEC モードに戻ります。
ステップ 8	**show track** *object-number* **例：** `Router# show track 3`	（任意）トラッキング情報を表示します。 • このコマンドを使用して、設定を確認します。「例」の出力を参照してください。

例

次に、インターフェイスでライン プロトコルのステートを追跡した場合の例を示します。

```
Router# show track 3

Track 3
   Interface Ethernet0/1 line-protocol
   Line protocol is Up
     1 change, last change 00:00:05
   Tracked by:
     HSRP Ethernet0/3 1
```

インターフェイスの IP ルーティング ステートの追跡

インターフェイスの IP ルーティング ステートを追跡するには、次の手順を実行します。次の条件が満たされる場合、IP ルーティング オブジェクトはアップ ステートにあると見なされます。

- IP ルーティングがインターフェイス上でイネーブルになっていて、アクティブである。
- インターフェイス ライン プロトコル ステートがアップである。
- インターフェイス IP アドレスが認識されている。IP アドレスが Dynamic Host Configuration Protocol（DHCP）または IP Control Protocol（IPCP）ネゴシエーションを通して設定または受信されている。

次のいずれかの条件が満たされると、インターフェイス IP ルーティングはダウンになります。

- IP ルーティングがグローバルにディセーブルになっている。
- インターフェイス ライン プロトコル ステートがダウンである。
- インターフェイス IP アドレスが不明である。IP アドレスが DHCP または IPCP ネゴシエーションを通して設定または受信されていない。

track interface ip routing コマンドを使用してインターフェイスの IP ルーティング ステートを追跡する方法は、**track interface line-protocol** コマンドを使用してライン プロトコル ステートを追跡する方法と比較して、状況によっては、より効果的になることがあります。アドレスのネゴシエーションが行われるインターフェイスでは、特に役立ちます。たとえば、Point-to-Point Protocol（PPP; ポイントツーポイント プロトコル）を使用するシリアル インターフェイス上では、ライン プロトコルはアップになることができます（Link Control Protocol（LCP; リンク制御プロトコル）は成功裏にネゴシエーションされます）が、IP はダウンになることがあります（IPCP ネゴシエーションは失敗します）。

track interface ip routing コマンドでは、次のいずれかの方法で取得した IP アドレスを持つインターフェイスの追跡がサポートされます。

- 従来の IP アドレス設定
- PPP/IPCP
- DHCP
- 番号付けされていないインターフェイス

また、インターフェイスの IP ルーティング ステートを追跡する場合に、トラッキング コンフィギュレーション モードで **carrier-delay** コマンドを使用することで、EOT がキャリア遅延タイマーを考慮するように設定することもできます。

手順の概要

1. **enable**
2. **configure terminal**
3. **track timer interface** {*seconds* | **msec** *milliseconds*}
4. **track** *object-number* **interface** *type number* **ip routing**
5. **carrier-delay**
6. **delay** {**up** *seconds* [**down** *seconds*] | [**up** *seconds*] **down** *seconds*}
7. **end**
8. **show track** *object-number*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**track timer interface** {*seconds* | **msec** *milliseconds*} 例： `Router(config)# track timer interface 5`	（任意）トラッキング プロセスが追跡対象オブジェクトをポーリングする間隔を指定します。 • トラッキング プロセスがインターフェイス オブジェクトをポーリングするデフォルトのインターバルは 1 秒です。 **（注）** すべてのポーリング頻度は、以前 **msec** キーワードと *milliseconds* 引数を使用して設定された最小 1 秒インターバルを上回る 500 ミリ秒に下げて設定することができます。
ステップ 4	**track** *object-number* **interface** *type number* **ip routing** 例： `Router(config)# track 1 interface ethernet 0/1 ip routing`	インターフェイスの IP ルーティング ステートを追跡し、トラッキング コンフィギュレーション モードを開始します。 • IP ルート トラッキングは、ルーティング テーブルの IP ルートと、IP パケットをルーティングするインターフェイスの機能を追跡します。
ステップ 5	**carrier-delay** 例： `Router(config-track)# carrier-delay`	（任意）インターフェイスのステータスを追跡するときに、EOT がキャリア遅延タイマーを考慮するように設定します。

	コマンドまたはアクション	目的
ステップ 6	**delay** {**up** *seconds* [**down** *seconds*] | [**up** *seconds*] **down** *seconds*} **例：** `Router(config-track)# delay up 30`	（任意）追跡対象オブジェクトのステート変更の通信を遅延させる時間（秒）を指定します。
ステップ 7	**end** **例：** `Router(config-track)# end`	特権 EXEC モードに戻ります。
ステップ 8	**show track** *object-number* **例：** `Router# show track 1`	トラッキング情報を表示します。 • このコマンドを使用して、設定を確認します。「例」の出力を参照してください。

例

次に、インターフェイスで IP ルーティングのステートを追跡した場合の例を示します。

```
Router# show track 1

Track 1
   Interface Ethernet0/1 ip routing
   IP routing is Up
     1 change, last change 00:01:08
   Tracked by:
     HSRP Ethernet0/3 1
```

IP ルートの到達可能性の追跡

IP ルートの到達可能性を追跡するには、次の手順を実行します。ルーティング テーブル エントリがルートに存在し、そのルートがアクセス可能であると、追跡対象オブジェクトはアップ ステートにあると見なされます。

手順の概要

1. **enable**
2. **configure terminal**
3. **track timer ip route** {*seconds* | **msec** *milliseconds*}
4. **track** *object-number* **ip route** *ip-address*/*prefix-length* **reachability**
5. **delay** {**up** *seconds* [**down** *seconds*] | [**up** *seconds*] **down** *seconds*}
6. **ip vrf** *vrf-name*
7. **end**
8. **show track** *object-number*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**track timer ip route** {*seconds* | **msec** *milliseconds*} **例：** `Router(config)# track timer ip route 20`	（任意）トラッキング プロセスが追跡対象オブジェクトをポーリングする間隔を指定します。 • トラッキング プロセスが IP ルート オブジェクトをポーリングするデフォルトのインターバルは 15 秒です。 **（注）** すべてのポーリング頻度は、以前 **msec** キーワードと *milliseconds* 引数を使用して設定された最小 1 秒インターバルを上回る 500 ミリ秒に下げて設定することができます。
ステップ 4	**track** *object-number* **ip route** *ip-address*/*prefix-length* **reachability** **例：** `Router(config)# track 4 ip route 10.16.0.0/16 reachability`	IP ルートの到達可能性を追跡し、トラッキング 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	**delay** {**up** *seconds* [**down** *seconds*] | [**up** *seconds*] **down** *seconds*} **例：** `Router(config-track)# delay up 30`	（任意）追跡対象オブジェクトのステート変更の通信を遅延させる時間（秒）を指定します。
ステップ 6	**ip vrf** *vrf-name* **例：** `Router(config-track)# ip vrf VRF2`	（任意）VPN Routing and Forwarding（VRF）テーブルを設定します。
ステップ 7	**end** **例：** `Router(config-track)# end`	特権 EXEC モードに戻ります。
ステップ 8	**show track** *object-number* **例：** `Router# show track 4`	（任意）トラッキング情報を表示します。 • このコマンドを使用して、設定を確認します。「例」の出力を参照してください。

例

次に、IP ルートの到達可能性のステートを追跡した場合の例を示します。

```
Router# show track 4

Track 4
   IP route 10.16.0.0 255.255.0.0 reachability
   Reachability is Up (RIP)
     1 change, last change 00:02:04
   First-hop interface is Ethernet0/1
   Tracked by:
     HSRP Ethernet0/3 1
```

IP ルート メトリックのしきい値の追跡

IP ルート メトリックのしきい値を追跡するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **track timer ip route** {*seconds* | **msec** *milliseconds*}
4. **track resolution ip route** {**eigrp** *resolution-value* | **isis** *resolution-value* | **ospf** *resolution-value* | **static** *resolution-value*}
5. **track** *object-number* **ip route** *ip-address*/*prefix-length* **metric threshold**
6. **delay** {**up** *seconds* [**down** *seconds*] | [**up** *seconds*] **down** *seconds*}
7. **ip vrf** *vrf-name*
8. **threshold metric** {**up** *number* [**down** *number*] | **down** *number* [**up** *number*]}
9. **end**
10. **show track** *object-number*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**track timer ip route** {*seconds* | **msec** *milliseconds*} **例：** `Router(config)# track timer ip route 20`	（任意）トラッキング プロセスが追跡対象オブジェクトをポーリングする間隔を指定します。 • トラッキング プロセスが IP ルート オブジェクトをポーリングするデフォルトのインターバルは 15 秒です。 **（注）** すべてのポーリング頻度は、以前 **msec** キーワードと *milliseconds* 引数を使用して設定された最小 1 秒インターバルを上回る 500 ミリ秒に下げて設定することができます。
ステップ 4	**track resolution ip route** {**eigrp** *resolution-value* | **isis** *resolution-value* | **ospf** *resolution-value* | **static** *resolution-value*} **例：** `Router(config)# track resolution ip route eigrp 300`	（任意）追跡対象オブジェクトの解析パラメータを指定します。 • このコマンドを使用して、デフォルトのメトリック解析値を変更します。
ステップ 5	**track** *object-number* **ip route** *ip-address/ prefix-length* **metric threshold** **例：** `Router(config)# track 6 ip route 10.16.0.0/16 metric threshold`	IP ルートの数値化メトリック値を追跡し、その値がしきい値を超えているかどうかを判断します。 • ダウン ステートのデフォルト値は 255 です。アクセス不可なルートであると見なされます。 • アップ ステートのデフォルト値は、254 です。
ステップ 6	**delay** {**up** *seconds* [**down** *seconds*] | [**up** *seconds*] **down** *seconds*} **例：** `Router(config-track)# delay up 30`	（任意）追跡対象オブジェクトのステート変更の通信を遅延させる時間（秒）を指定します。
ステップ 7	**ip vrf** *vrf-name* **例：** `Router(config-track)# ip vrf VRF1`	（任意）VRF テーブルを設定します。
ステップ 8	**threshold metric** {**up** *number* [**down** *number*] | **down** *number* [**up** *number*]} **例：** `Router(config-track)# threshold metric up 254 down 255`	（任意）メトリックのしきい値に、デフォルト値以外の値を設定します。
ステップ 9	**end** **例：** `Router(config-track)# end`	特権 EXEC モードに戻ります。
ステップ 10	**show track** *object-number* **例：** `Router# show track 6`	（任意）トラッキング情報を表示します。 • このコマンドを使用して、設定を確認します。「例」の出力を参照してください。

例

次に、IP ルートのメトリックのしきい値を追跡した場合の例を示します。

```
Router# show track 6

Track 6
   IP route 10.16.0.0 255.255.0.0 metric threshold
   Metric threshold is Up (RIP/6/102)
     1 change, last change 00:00:08
   Metric threshold down 255 up 254
   First-hop interface is Ethernet0/1
   Tracked by:
     HSRP Ethernet0/3 1
```

IP SLA 動作のステートの追跡

IP SLA 動作のステートを追跡するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **track** *object-number* **rtr** *operation-number* **state**
   または
   track *object-number* **ip sla** *operation-number* **state**
4. **delay** {**up** *seconds* [**down** *seconds*] | [**up** *seconds*] **down** *seconds*}
5. **end**
6. **show track** *object-number*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**12.4(20)T、12.2(33)SXI1、および 12.2(33)SRE よりも前の Cisco IOS リリース** **track** *object-number* **rtr** *operation-number* **state** **Cisco IOS Release 12.4(20)T、12.2(33)SXI1、12.2(33)SRE 以降のリリース** **track** *object-number* **ip sla** *operation-number* **state** **例：12.4(20)T、12.2(33)SXI1、および 12.2(33)SRE よりも前の Cisco IOS リリース** `Router(config)# track 2 rtr 4 state` **例：Cisco IOS Release 12.4(20)T、12.2(33)SXI1、12.2(33)SRE 以降のリリース** `Router(config)# track 2 ip sla 4 state`	IP SLA オブジェクトのステートを追跡し、トラッキング コンフィギュレーション モードを開始します。 **（注）** Cisco IOS Release 12.4(20)T、12.2(33)SXI1、および 12.2(33)SRE で有効な **track rtr** コマンドが **track ip sla** コマンドに置き換えられました。**track rtr** コマンドは将来のリリースで削除される予定です。現在は、既存の設定を **track ip sla** コマンド用に更新するために使用できるようになっています。
ステップ 4	**delay** {**up** *seconds* [**down** *seconds*] | [**up** *seconds*] **down** *seconds*} **例：** `Router(config-track)# delay up 60 down 30`	（任意）追跡対象オブジェクトのステート変更の通信を遅延させる時間（秒）を指定します。
ステップ 5	**end** **例：** `Router(config-track)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show track** *object-number* **例：** `Router# show track 2`	（任意）トラッキング情報を表示します。 • このコマンドを使用して、設定を確認します。「例」で、このタスクの出力を参照してください。

例

次に、IP SLA トラッキングのステートの例を示します。

```
Router# show track 2

Track 2
   IP SLA 1 state
   State is Down
     1 change, last change 00:00:47
   Latest operation return code: over threshold
   Latest RTT (millisecs) 4
   Tracked by:
     HSRP Ethernet0/1 3
```

IP SLA IP ホストの到達可能性の追跡

IP ホストの到達可能性を追跡するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **track** *object-number* **rtr** *operation-number* **reachability**

   または
   track *object-number* **ip sla** *operation-number* **reachability**
4. **delay** {**up** *seconds* [**down** *seconds*] | [**up** *seconds*] **down** *seconds*}
5. **end**
6. **show track** *object-number*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**12.4(20)T、12.2(33)SXI1、および 12.2(33)SRE よりも前の Cisco IOS リリース** **track** *object-number* **rtr** *operation-number* **reachability** **Cisco IOS Release 12.4(20)T、12.2(33)SXI1、12.2(33)SRE 以降のリリース** **track** *object-number* **ip sla** *operation-number* **reachability** **例：12.4(20)T、12.2(33)SRE、および 12.2(33)SXI1 よりも前の Cisco IOS リリース** `Router(config)# track 2 rtr 4 reachability` **例：Cisco IOS Release 12.4(20)T、12.2(33)SXI1、12.2(33)SRE 以降のリリース** `Router(config)# track 2 ip sla 4 reachability`	IP SLA IP ホストの到達可能性を追跡し、トラッキング コンフィギュレーション モードを開始します。 **（注）** Cisco IOS Release 12.4(20)T、12.2(33)SXI1、および 12.2(33)SRE で有効な **track rtr** コマンドが **track ip sla** コマンドに置き換えられました。**track rtr** コマンドは将来のリリースで削除される予定です。現在は、既存の設定を **track ip sla** コマンド用に更新するために使用できるようになっています。

	コマンドまたはアクション	目的
ステップ 4	**delay** {**up** *seconds* [**down** *seconds*] | [**up** *seconds*] **down** *seconds*} **例：** `Router(config-track)# delay up 30 down 10`	（任意）追跡対象オブジェクトのステート変更の通信を遅延させる時間（秒）を指定します。
ステップ 5	**end** **例：** `Router(config-track)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show track** *object-number* **例：** `Router# show track 3`	（任意）トラッキング情報を表示します。 • このコマンドを使用して、設定を確認します。「例」で、このタスクの出力を参照してください。

例

次に、ルートが到達可能であるかどうかを調べる例を示します。

```
Router# show track 3

Track 3
   IP SLA 1 reachability
   Reachability is Up
     1 change, last change 00:00:47
   Latest operation return code: over threshold
   Latest RTT (millisecs) 4
   Tracked by:
     HSRP Ethernet0/1 3
```

追跡リストおよびブール式の設定

オブジェクトの追跡リストとブール式を設定し、リストのステートを判断するには、次の手順を実行します。追跡リストには、1 つまたは複数のオブジェクトが含まれます。ブール式を使用すると、「and」または「or」演算子を使って 2 種類の計算を行うことができます。たとえば、「and」演算子を使用して 2 つのインターフェイスを追跡する場合、「up」は*両方の*インターフェイスがアップ ステートであることを意味し、「down」は*いずれかの*インターフェイスがダウン ステートであることを意味します。

重みしきい値またはパーセントしきい値を使用して、測定対象とする追跡リスト ステートを設定することもできます。「追跡リストと重みしきい値の設定」（P.19）および「追跡リストとパーセントしきい値の設定」（P.21）を参照してください。

（注） 「not」演算子は、1 つまたは複数のオブジェクトに指定し、オブジェクトのステートを否定します。

前提条件

追跡リストに追加するオブジェクトは、存在している必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **track** *track-number* **list boolean** {**and** | **or**}
4. **object** *object-number* [**not**]
5. **delay** {**up** *seconds* [**down** *seconds*] | [**up** *seconds*] **down** *seconds*}
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**track** *track-number* **list boolean** {**and** | **or**} **例：** `Router(config-track)# track 100 list boolean and`	追跡リストのオブジェクトを設定し、トラッキング コンフィギュレーション モードを開始します。次のキーワードがあります。 • **boolean**：追跡リストのステートがブール計算に基づくことを指定します。次のキーワードがあります。 – **and**：すべてのオブジェクトがアップしている場合にリストがアップし、1 つまたは複数のオブジェクトがダウンしている場合にリストがダウンすることを指定します。たとえば、2 つのインターフェイスを追跡する場合、アップは両方のインターフェイスがアップ ステートであることを意味し、ダウンはいずれかのインターフェイスがダウン ステートであることを意味します。 – **or**：少なくとも 1 つのオブジェクトがアップしている場合にリストがアップすることを指定します。たとえば、2 つのインターフェイスを追跡する場合、アップはいずれかのインターフェイスがアップ ステートであることを意味し、ダウンは両方のインターフェイスがダウン ステートであることを意味します。
ステップ 4	**object** *object-number* [**not**] **例：** `Router(config-track)# object 3 not`	追跡対象のオブジェクトを指定します。*object-number* 引数の有効範囲は 1 ～ 1000 です。デフォルトはありません。オプションの **not** キーワードは、オブジェクトのステートを否定します。 **（注）** 例では、object 3 がアップのときに、追跡リストでは object 3 はダウンとして検出されることを示しています。

	コマンドまたはアクション	目的
ステップ 5	**delay** {**up** *seconds* [**down** *seconds*] | [**up** *seconds*] **down** *seconds*} 例： `Router(config-track)# delay up 3`	（任意）アップ ステートとダウン ステートの追跡の遅延を秒単位で指定します。
ステップ 6	**end** 例： `Router(config-track)# end`	特権 EXEC モードに戻ります。

追跡リストと重みしきい値の設定

追跡対象オブジェクトのリストの設定、しきい値として使用する重みしきい値の指定、および各オブジェクトの重みしきい値の設定を行うには、次の手順を実行します。追跡リストには、1 つまたは複数のオブジェクトが含まれます。重みしきい値を使用すると、各オブジェクトのステートは、各オブジェクトの重みしきい値に対してアップ ステートにあるすべてのオブジェクトの全体的な重みしきい値を比較することで決定されます。

ブール計算またはパーセントしきい値を使用して、測定対象とする追跡リスト ステートを設定することもできます。「追跡リストおよびブール式の設定」（P.17）および「追跡リストとパーセントしきい値の設定」（P.21）を参照してください。

前提条件

追跡リストに追加するオブジェクトは、存在している必要があります。

制約事項

重みしきい値またはパーセントしきい値のリストでは、ブールの「not」演算子は使用できません。

手順の概要

1. **enable**
2. **configure terminal**
3. **track** *track-number* **list threshold weight**
4. **object** *object-number* [**weight** *weight-number*]
5. **threshold weight** {**up** *number* **down** *number* | **up** *number* | **down** *number*}
6. **delay** {**up** *seconds* [**down** *seconds*] | [**up** *seconds*] **down** *seconds*}
7. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**track** *track-number* **list threshold weight** **例：** `Router(config-track)# track 100 list threshold weight`	追跡リストのオブジェクトを設定し、トラッキング コンフィギュレーション モードを開始します。次のキーワードがあります。 • **threshold**：追跡リストのステートがしきい値に基づくことを指定します。 • **weight**：しきい値が、指定の重みしきい値に基づくことを指定します。
ステップ 4	**object** *object-number* [**weight** *weight-number*] **例：** `Router(config-track)# object 3 weight 30`	追跡対象のオブジェクトを指定します。*object-number* 引数の有効範囲は 1 ～ 1000 です。デフォルトはありません。オプションの **weight** キーワードで、各オブジェクトの重みしきい値を指定します。
ステップ 5	**threshold weight** {**up** *number* **down** *number* | **up** *number* | **down** *number*} **例：** `Router(config-track)# threshold weight up 30`	重みしきい値を指定します。次のキーワードと引数があります。 • **up** *number*：有効範囲は 1 ～ 255 です。 • **down** *number*：範囲は、**up** キーワードでの選択に応じて異なります。たとえば、up に 25 を設定した場合、ダウンの範囲は 0 ～ 24 になります。
ステップ 6	**delay** {**up** *seconds* [**down** *seconds*] | [**up** *seconds*] **down** *seconds*} **例：** `Router(config-track)# delay up 3`	（任意）アップ ステートとダウン ステートの追跡の遅延を秒単位で指定します。
ステップ 7	**end** **例：** `Router(config-track)# end`	特権 EXEC モードに戻ります。

追跡リストとパーセントしきい値の設定

オブジェクトの追跡リストの設定、しきい値として使用するパーセンテージの指定、およびリスト内の各オブジェクトのパーセンテージの指定を行うには、次の手順を実行します。追跡リストには、1 つまたは複数のオブジェクトが含まれます。パーセントしきい値を使用すると、リストのステートは、各オブジェクトに割り当てられたパーセンテージを比較することで決定されます。

ブール計算または重みしきい値を使用して、測定対象とする追跡リスト ステートを設定することもできます。「追跡リストおよびブール式の設定」（P.17）および「追跡リストと重みしきい値の設定」（P.19）を参照してください。

前提条件

追跡リストに追加するオブジェクトは、存在している必要があります。

制約事項

重みしきい値またはパーセントしきい値のリストでは、ブールの「not」演算子は使用できません。

手順の概要

1. **enable**
2. **configure terminal**
3. **track** *track-number* **list threshold percentage**
4. **object** *object-number*
5. **threshold percentage** {**up** *number* [**down** *number*] | **down** *number* [**up** *number*]}
6. **delay** {**up** *seconds* [**down** *seconds*] | [**up** *seconds*] **down** *seconds*}
7. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**track** *track-number* **list threshold percentage** 例： `Router(config-track)# track 100 list threshold percentage`	追跡リストのオブジェクトを設定し、トラッキング コンフィギュレーション モードを開始します。次のキーワードがあります。 • **threshold**：追跡リストのステートがしきい値に基づくことを指定します。 • **percentage**：しきい値がパーセンテージに基づくことを指定します。

	コマンドまたはアクション	目的
ステップ 4	**object** *object-number* 例： `Router(config-track)# object 3`	追跡対象のオブジェクトを指定します。*object-number* 引数の有効範囲は 1 ～ 1000 です。デフォルトはありません。
ステップ 5	**threshold percentage** {**up** *number* [**down** *number*] | **down** *number* [**up** *number*]} 例： `Router(config-track)# threshold percentage up 30`	パーセントしきい値を指定します。次のキーワードと引数があります。 • **up** *number*：有効範囲は 1 ～ 100 です。 • **down** *number*：範囲は、**up** キーワードでの選択に応じて異なります。たとえば、up に 25 を設定した場合、**down** キーワードの範囲には 26 ～ 100 が表示されます。
ステップ 6	**delay** {**up** *seconds* [**down** *seconds*] | [**up** *seconds*] **down** *seconds*} 例： `Router(config-track)# delay up 3`	（任意）アップ ステートとダウン ステートの追跡の遅延を秒単位で指定します。
ステップ 7	**end** 例： `Router(config-track)# end`	特権 EXEC モードに戻ります。

追跡リストのデフォルトの設定

追跡リストのデフォルトの遅延値、デフォルト オブジェクト、および追跡リストのデフォルトのしきい値パラメータの設定を行うには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **track** *track-number*
4. **default** {**delay** | **object** *object-number* | **threshold percentage**}
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**track** *track-number* 例： `Router(config)# track 3`	トラッキング 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	**default** {**delay** | **object** *object-number* | **threshold percentage**} 例： `Router(config-track)# default delay`	追跡リストのデフォルトの遅延値、デフォルト オブジェクト、および追跡リストのデフォルトのしきい値パラメータを指定します。次のキーワードと引数があります。 • **delay**：デフォルトの遅延値に戻します。 • **object** *object-number*：追跡リストのデフォルト オブジェクトを指定します。有効範囲は 1 ～ 1000 です。 • **threshold percentage**：デフォルトのパーセントしきい値を指定します。
ステップ 5	**end** 例： `Router(config-track)# end`	特権 EXEC モードに戻ります。

Mobile IP アプリケーションのトラッキングの設定

Mobile IP アプリケーション オブジェクトの追跡リストを設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **track** *track-number* **application home-agent**
4. **exit**
5. **track** *track-number* **application pdsn**
6. **exit**
7. **track** *track-number* **application ggsn**
8. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**track** *track-number* **application home-agent** **例：** `Router(config)# track 100 application home-agent`	（任意）ルータ上の Home Agent トラフィックのプレゼンスを追跡します。
ステップ 4	**exit** **例：** `Router(config-track)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 5	**track** *track-number* **application pdsn** **例：** `Router(config)# track 100 application pdsn`	（任意）ルータ上の PDSN トラフィックのプレゼンスを追跡します。
ステップ 6	**exit** **例：** `Router(config-track)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 7	**track** *track-number* **application ggsn** **例：** `Router(config)# track 100 application ggsn`	（任意）ルータ上の GGSN トラフィックのプレゼンスを追跡します。
ステップ 8	**end** **例：** `Router(config)# end`	特権 EXEC モードに戻ります。

拡張オブジェクト トラッキングの設定例

ここでは、次の設定例について説明します。

例：インターフェイス ライン プロトコル

次の例は、IP ルーティングの例に類似しています。ただし、トラッキング プロセスはシリアル インターフェイス 1/0 のライン プロトコル ステートを追跡するように設定されています。イーサネット インターフェイス 0/0 の HSRP は、シリアル インターフェイス 1/0 のライン プロトコル ステートに何らかの変更が生じた場合には通知されるように、トラッキング プロセスに登録します。シリアル インターフェイス 1/0 のライン プロトコルがダウンすると、HSRP グループのプライオリティは 10 だけ引き下げられます。

ルータ A の設定

```
RouterA(config)# track 100 interface serial1/0 line-protocol
RouterA(config-track)# exit
RouterA(config)# interface Ethernet0/0
RouterA(config-if)# ip address 10.1.0.21 255.255.0.0
RouterA(config-if)# standby 1 preempt
RouterA(config-if)# standby 1 ip 10.1.0.1
RouterA(config-if)# standby 1 priority 110
RouterA(config-if)# standby 1 track 100 decrement 10
```

ルータ B の設定

```
RouterB(config)# track 100 interface serial1/0 line-protocol
RouterB(config-track)# exit
RouterB(config)# interface Ethernet0/0
RouterB(config-if)# ip address 10.1.0.22 255.255.0.0
RouterB(config-if)# standby 1 preempt
RouterB(config-if)# standby 1 ip 10.1.0.1
RouterB(config-if)# standby 1 priority 105
RouterB(config-if)# standby 1 track 100 decrement 10
```

例：インターフェイス IP ルーティング

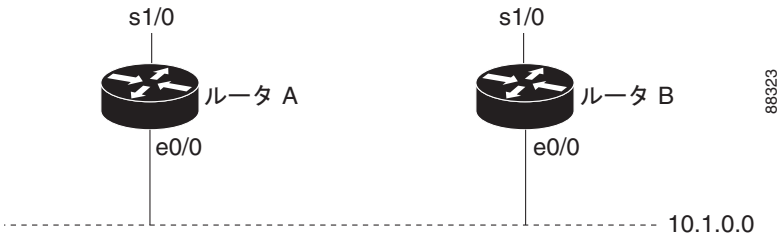
次の例では、トラッキング プロセスはシリアル インターフェイス 1/0 の IP ルーティング機能を追跡するように設定されています。イーサネット インターフェイス 0/0 の HSRP は、シリアル インターフェイス 1/0 の IP ルーティング ステートに何らかの変更が生じた場合には通知されるように、トラッキング プロセスに登録します。シリアル インターフェイス 1/0 の IP ルーティング ステートがダウンになると、HSRP グループのプライオリティは 10 だけ引き下げられます。

次の例では、シリアル インターフェイス 1/0 のステートを追跡するときに EOT がキャリア遅延タイマーを考慮するように設定しています。

両方のシリアル インターフェイスが動作している場合は、ルータ A はルータ B よりもプライオリティが高いので、ルータ A が HSRP アクティブ ルータになります。ただし、ルータ A でシリアル インターフェイス 1/0 の IP が失敗すると、HSRP グループ プライオリティは下がり、ルータ B がアクティブ ルータを引き継いで、10.1.0.0 サブネット上のホストに対するデフォルトの仮想ゲートウェイ サービスが維持されます。

サンプル トポロジについては、図 1 を参照してください。

図 1　　IP ルーティング サポートのトポロジ



ルータ A の設定

```
RouterA(config)# track 100 interface serial1/0 ip routing
RouterA(config-track)# carrier-delay
RouterA(config-track)# exit
RouterA(config)# interface Ethernet0/0
RouterA(config-if)# ip address 10.1.0.21 255.255.0.0
RouterA(config-if)# standby 1 preempt
RouterA(config-if)# standby 1 ip 10.1.0.1
RouterA(config-if)# standby 1 priority 110
RouterA(config-if)# standby 1 track 100 decrement 10
```

ルータ B の設定

```
RouterB(config)# track 100 interface serial1/0 ip routing
RouterB(config-track)# carrier-delay
RouterB(config-track)# exit
RouterB(config)# interface Ethernet0/0
RouterB(config-if)# ip address 10.1.0.22 255.255.0.0
RouterB(config-if)# standby 1 preempt
RouterB(config-if)# standby 1 ip 10.1.0.1
RouterB(config-if)# standby 1 priority 105
RouterB(config-if)# standby 1 track 100 decrement 10
```

例：IP ルート到達可能性

次の例では、トラッキング プロセスは IP ルート 10.2.2.0/24 の到達可能性を追跡するように設定されています。

ルータ A の設定

```
RouterA(config)# track 100 ip route 10.2.2.0/24 reachability
RouterA(config-track)# exit
RouterA(config)# interface Ethernet0/0
RouterA(config-if)# ip address 10.1.1.21 255.255.255.0
RouterA(config-if)# standby 1 preempt
RouterA(config-if)# standby 1 ip 10.1.1.1
RouterA(config-if)# standby 1 priority 110
RouterA(config-if)# standby 1 track 100 decrement 10
```

ルータ B の設定

```
RouterB(config)#track 100 ip route 10.2.2.0/24 reachability
RouterB(config-track)# exit
RouterB(config)# interface Ethernet0/0
RouterB(config-if)# ip address 10.1.1.22 255.255.255.0
RouterB(config-if)# standby 1 preempt
RouterB(config-if)# standby 1 ip 10.1.1.1
RouterB(config-if)# standby 1 priority 105
RouterB(config-if)# standby 1 track 100 decrement 10
```

例：IP ルートしきい値メトリック

次の例では、トラッキング プロセスは IP ルート 10.2.2.0/24 のしきい値メトリックを追跡するように設定されています。

ルータ A の設定

```
RouterA(config)# track 100 ip route 10.2.2.0/24 metric threshold
RouterA(config-track)# exit
RouterA(config)# interface Ethernet0/0
RouterA(config)# ip address 10.1.1.21 255.255.255.0
RouterA(config-if)# standby 1 preempt
RouterA(config-if)# standby 1 ip 10.1.1.1
RouterA(config-if)# standby 1 priority 110
RouterA(config-if)# standby 1 track 100 decrement 10
```

ルータ B の設定

```
RouterB(config)# track 100 ip route 10.2.2.0/24 metric threshold
RouterB(config-track)# exit
RouterB(config)# interface Ethernet0/0
RouterB(config-if)# ip address 10.1.1.22 255.255.255.0
RouterB(config-if)# standby 1 preempt
RouterB(config-if)# standby 1 ip 10.1.1.1
RouterB(config-if)# standby 1 priority 105
RouterB(config-if)# standby 1 track 100 decrement 10
```

例：IP SLA IP ホスト トラッキング

次に、Cisco IOS Release 12.4(20)T、12.2(33)SXI1、および 12.2(33)SRE よりも前の Cisco IOS リリースで IP SLA 動作 1 の IP ホスト トラッキングを設定する方法の例を示します。

```
Router(config)# ip sla 1
Router(config-ip-sla)# icmp-echo 10.51.12.4
Router(config-ip-sla-echo)# timeout 1000
Router(config-ip-sla-echo)# threshold 2
Router(config-ip-sla-echo)# frequency 3
Router(config-ip-sla-echo)# request-data-size 1400
Router(config-ip-sla-echo)# exit
Router(config)# ip sla schedule 1 start-time now life forever
Router(config-ip-sla)# track 2 rtr 1 state
Router(config-ip-sla)# exit
Router(config)# track 3 rtr 1 reachability
Router(config-track)# exit
Router(config)# interface ethernet0/1
Router(config-if)# ip address 10.21.0.4 255.255.0.0
Router(config-if)# no shutdown
Router(config-if)# standby 3 ip 10.21.0.10
Router(config-if)# standby 3 priority 120
Router(config-if)# standby 3 preempt
Router(config-if)# standby 3 track 2 decrement 10
Router(config-if)# standby 3 track 3 decrement 10
```

次に、Cisco IOS Release 12.4(20)T、12.2(33)SXI1、12.2(33)SRE、および以降のリリースで IP SLA 動作 1 の IP ホスト トラッキングを設定する方法の例を示します。

```
Router(config)# ip sla 1
Router(config-ip-sla)# icmp-echo 10.51.12.4
Router(config-ip-sla-echo)# threshold 2
Router(config-ip-sla-echo)# timeout 1000
Router(config-ip-sla-echo)# frequency 3
Router(config-ip-sla-echo)# request-data-size 1400
Router(config-ip-sla-echo)# exit
Router(config)# ip sla schedule 1 start-time now life forever
Router(config)# track 2 ip sla 1 state
Router(config-track)# exit
Router(config)# track 3 ip sla 1 reachability
Router(config-track)# exit
Router(config)# interface ethernet0/1
Router(config-if)# ip address 10.21.0.4 255.255.0.0
Router(config-if)# no shutdown
Router(config-if)# standby 3 ip 10.21.0.10
Router(config-if)# standby 3 priority 120
Router(config-if)# standby 3 preempt
Router(config-if)# standby 3 track 2 decrement 10
Router(config-if)# standby 3 track 3 decrement 10
```

例：追跡リストのブール式

次の例では、追跡リスト オブジェクトは、両方のシリアル インターフェイスがアップであるときと、いずれかのシリアル インターフェイスがダウンであるときに、2 つのシリアル インターフェイスを追跡するように設定されています。

```
Router(config)# track 1 interface serial2/0 line-protocol
Router(config-track)# track 2 interface serial2/1 line-protocol
Router(config-track)# exit
Router(config)# track 100 list boolean and
```

```
Router(config-track)# object 1
Router(config-track)# object 2
```

次の例では、追跡リスト オブジェクトは、いずれかのシリアル インターフェイスがアップであるときと、両方のシリアル インターフェイスがダウンであるときに、2 つのシリアル インターフェイスを追跡するように設定されています。

```
Router(config)# track 1 interface serial2/0 line-protocol
Router(config)# track 2 interface serial2/1 line-protocol
Router(config-track)# exit
Router(config)# track 101 list boolean or
Router(config-track)# object 1
Router(config-track)# object 2
```

次の設定例では、追跡リスト 4 に 2 つのオブジェクトがあり、1 つのオブジェクト ステートが否定されています（リストがアップのとき、このリストでは object 2 はダウンしていると検出します）。

```
Router(config)# track 4 list boolean and
Router(config-track)# object 1
Router(config-track)# object 2 not
```

例：追跡リストの重みしきい値

次の例では、追跡リスト 100 にある 3 つのシリアル インターフェイスに、それぞれ重みしきい値 20 が設定されています。ダウンのしきい値は 0 に設定され、アップのしきい値は 40 に設定されています。

```
Router(config)# track 1 interface serial2/0 line-protocol
Router(config-track)# track 2 interface serial2/1 line-protocol
Router(config-track)# track 3 interface serial2/2 line-protocol
Router(config-track)# exit
Router(config)# track 100 list threshold weight
Router(config-track)# object 1 weight 20
Router(config-track)# object 2 weight 20
Router(config-track)# object 3 weight 20
Router(config-track)# threshold weight down 0 up 40
```

上記の例は、track-list オブジェクトは 3 つのすべてのシリアル インターフェイスがダウン ステートになり、少なくとも 2 つのシリアル インターフェイスがアップするとアップ ステートに戻ることを意味します（20+20 >= 40 であるため）。この設定には、2 つのインターフェイスがダウンしていて、3 つ目のインターフェイスがフラッピングしているときに track-list オブジェクトがアップ ステートに戻ることを回避できるというメリットがあります。

次の設定例では、object 1 と object 2 がダウンしている場合に、追跡リスト 4 がアップすることを示しています。これは、object 3 が up 30 というアップのしきい値を満たすためです。ただし、object 3 がダウンであると、重みしきい値を満たすようにするため、object 1 と object 2 はアップになる必要があります。

```
Router(config)# track 4 list threshold weight
Router(config-track)# object 1 weight 15
Router(config-track)# object 2 weight 20
Router(config-track)# object 3 weight 30
Router(config-track)# threshold weight up 30 down 10
```

この設定は、帯域幅の小さい 2 つの接続（object 1 と object 2）と、帯域幅の大きい 1 つの接続（object 3）がある場合に役立つことがあります。また、down 10 という値は、追跡対象オブジェクトが一度アップになると、しきい値が 10 以下にならない限りダウン ステートにならないことを意味します。この例では、すべての接続がダウンしないとダウン ステートにならないことを意味します。

例：追跡リストのパーセントしきい値

次の例では、追跡リスト 100 の 4 つのシリアル インターフェイスはアップのパーセントしきい値が 75 に設定されています。シリアル インターフェイスの 75 パーセントがアップになると追跡リストはアップし、アップしているシリアル インターフェイスが 75 パーセント未満であると追跡リストはダウンになります。

```
Router(config)# track 1 interface serial2/0 line-protocol
Router(config-track)# track 2 interface serial2/1 line-protocol
Router(config-track)# track 3 interface serial2/2 line-protocol
Router(config-track)# track 4 interface serial2/3 line-protocol
Router(config-track)# exit
Router(config)# track 100 list threshold percentage
Router(config-track)# object 1
Router(config-track)# object 2
Router(config-track)# object 3
Router(config-track)# object 4
Router(config-track)# threshold percentage up 75
```

例：Mobile IP アプリケーション トラッキング

次に、ルータ上の Mobile IP、GGSN、および PDSN トラフィックを EOT が追跡するように設定する方法の例を示します。

```
Router(config)# track 1 application home-agent
Router(config-track)# exit
Router(config)# track 2 application ggsn
Router(config-track)# exit
Router(config)# track 3 application pdsn
```

その他の参考資料

関連資料

内容	参照先
Cisco IOS コマンド	『*Cisco IOS Master Commands List, All Releases*』
Embedded Event Manager（EEM）	「Embedded Event Manager Overview」モジュール
HSRP の概念と設定作業	「Configuring HSRP」モジュール
GLBP の概念と設定作業	「Configuring GLBP」モジュール
VRRP の概念と設定作業	「Configuring VRRP」モジュール
GLBP、HSRP および VRRP 設定コマンド：コマンド構文の詳細、コマンド モード、コマンド履歴、デフォルト設定、使用に関する注意事項および例	『*Cisco IOS IP Application Services Command Reference*』

規格

規格	タイトル
新しい規格または変更された規格はサポートされていません。また、既存の規格に対するサポートに変更はありません。	—

MIB

MIB	MIB リンク
新しい MIB または変更された MIB はサポートされていません。また、既存の MIB に対するサポートに変更はありません。	選択されたプラットフォーム、シスコ ソフトウェア リリース、およびフィーチャ セットの MIB を検索してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
新しい RFC または変更された RFC はサポートされていません。また、既存の RFC に対するサポートに変更はありません。	—

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。以下を含むさまざまな作業にこの Web サイトが役立ちます。 ・テクニカル サポートを受ける ・ソフトウェアをダウンロードする ・セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける ・ツールおよびリソースへアクセスする - Product Alert の受信登録 - Field Notice の受信登録 - Bug Toolkit を使用した既知の問題の検索 ・Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する ・トレーニング リソースへアクセスする ・TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

拡張オブジェクト トラッキングの機能情報

表 3 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。

プラットフォーム サポートとソフトウェア イメージ サポートに関する情報を入手するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator を使用すると、特定のソフトウェア リリース、フィーチャ セット、またはプラットフォームをサポートするソフトウェア イメージを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 表 3 に、特定のソフトウェア リリース トレイン内の機能に対するサポートが導入されたソフトウェア リリースだけを示します。特に断りのないかぎり、そのソフトウェア リリース トレイン以降のリリースでもその機能がサポートされます。

表 3　拡張オブジェクト トラッキングの機能情報

機能名	リリース	機能設定情報
拡張トラッキング サポート	Cisco IOS XE 3.1.0SG 12.2(15)T 12.2(25)S 12.2(28)SB 12.2(33)SRA 12.2(33)SXH	拡張トラッキング サポート機能は、HSRP からトラッキング メカニズムを分離させて、独立したトラッキング プロセスを別途生成します。これにより、HSRP 以外の Cisco IOS プロセスがこのトラッキング プロセスを使用できます。この機能を使用すると、インターフェイスのラインプロトコル ステートに加えて他のオブジェクトも追跡できます。 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。 • 「インターフェイスのライン プロトコル ステートの追跡」（P.6） • 「インターフェイスの IP ルーティング ステートの追跡」（P.8） • 「IP ルートの到達可能性の追跡」（P.10） • 「IP ルート メトリックのしきい値の追跡」（P.12） この機能により、次のコマンドが導入または変更されました。**debug track**、**delay tracking**、**ip vrf**、**show track**、**standby track**、**threshold metric**、**track interface**、**track ip route**、**track timer**
FHRP：拡張オブジェクト トラッキングと Embedded Event Manager	12.2(33)SRB 12.2(33)SXI 12.4(2)T	EOT が EEM と統合され、EEM は追跡対象オブジェクトのステータス変更を報告し、EOT は EEM オブジェクトを追跡できるようになりました。 この機能については、次の項に説明があります。 • 「拡張オブジェクト トラッキングおよび Embedded Event Manager」（P.4） この機能により、次のコマンドが導入または変更されました。**action track read**、**action track set**、**default-state**、**event resource**、**event rf**、**event track**、**show track**、**track stub**

表 3　拡張オブジェクト トラッキングの機能情報 （続き）

機能名	リリース	機能設定情報
FHRP：IP SLA 動作の拡張オブジェクト トラッキング	Cisco IOS XE 3.1.0SG 12.2(25)S 12.2(27)SBC 12.2(33)SRA 12.2(33)SXH 12.3(4)T 15.0(1)S	この機能により、First Hop Redundancy Protocol（FHRP）およびその他の拡張オブジェクト トラッキング（EOT）クライアントが、IP SLA オブジェクトの出力を追跡し、提供された情報を使用してアクションを開始できます。 この機能については、次の項に説明があります。 • 「IP SLA 動作トラッキング」（P.4） • 「IP SLA 動作のステートの追跡」（P.14） • 「IP SLA IP ホストの到達可能性の追跡」（P.16） • 「例：IP SLA IP ホスト トラッキング」（P.28） コマンド **track rtr** がこの機能により導入されました。
FHRP - Enhanced Object Tracking Support for Mobile IP	12.4(11)T	FHRP - Enhanced Object Tracking Support for Mobile IP 機能は、ルータ上の Home Agent、GGSN、または PDSN トラフィックのプレゼンスを追跡するためにモバイル ワイヤレス アプリケーションが必要とする新しいトラッキング オブジェクトを提供します。 この機能に関する詳細については、次の各項を参照してください。 • 「Mobile IP アプリケーションの拡張オブジェクト トラッキング」（P.5） • 「Mobile IP アプリケーションのトラッキングの設定」（P.23） • 「例：Mobile IP アプリケーション トラッキング」（P.30） コマンド **track application** がこの機能により導入されました。
FHRP：**rtr** キーワードの EOT の廃止	12.2(33)SRE 12.2(33)SXI1 12.4(20)T	この機能により、**track rtr** コマンドは **track ip sla** コマンドで置き変えられました。 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。 • 「IP SLA 動作トラッキング」（P.4） • 「IP SLA 動作のステートの追跡」（P.14） • 「IP SLA IP ホストの到達可能性の追跡」（P.16） • 「例：IP SLA IP ホスト トラッキング」（P.28） コマンド **track ip sla** がこの機能により導入されました。

表 3　拡張オブジェクト トラッキングの機能情報 （続き）

機能名	リリース	機能設定情報
FHRP：オブジェクト追跡リスト	Cisco IOS XE 3.1.0SG 12.2(30)S 12.2(31)SB2 12.2(33)SRA 12.2(33)SXH 12.3(8)T 15.0(1)S	この機能によりトラッキング機能が強化され、リスト内で追跡対象オブジェクトを組み合わせて設定したり、ブールロジックを使用した柔軟性のある方法でオブジェクトを組み合わせたりすることができます。 この機能に関する詳細については、次の各項を参照してください。 • 「追跡リストおよびブール式の設定」（P.17） • 「追跡リストと重みしきい値の設定」（P.19） • 「追跡リストとパーセントしきい値の設定」（P.21） • 「追跡リストのデフォルトの設定」（P.22） この機能により、次のコマンドが導入または変更されました。**show track**、**threshold percentage**、**threshold weight**、**track list**、**track resolution**
EOT によるキャリア遅延サポート	12.4(9)T	EOT によるキャリア遅延サポート機能により、拡張オブジェクト トラッキング（EOT）はインターフェイスのステータスを追跡するときにキャリア遅延タイマーを考慮に入れることができます。 この機能に関する詳細については、次の各項を参照してください。 • 「EOT によるキャリア遅延サポート」（P.4） • 「インターフェイスのライン プロトコル ステートの追跡」（P.6） • 「インターフェイスの IP ルーティング ステートの追跡」（P.8） • 「例：インターフェイス IP ルーティング」（P.26） **carrier-delay**（トラッキング）および **show track** の各コマンドがこの機能により導入または変更されました。

用語集

DHCP：Dynamic Host Configuration Protocol。DHCP は、ネットワーク クライアントに IP アドレスと設定情報を伝送するプロトコルです。

GLBP：Gateway Load Balancing Protocol。IEEE 802.3 LAN 上の単一のデフォルト ゲートウェイを使用して設定されている IP ホストの自動ルータ バックアップを提供します。LAN 上の複数のファーストホップ ルータを連結し、IP パケットの転送負荷を共有しながら単一の仮想ファーストホップ IP ルータを提供します。LAN 上にあるその他のルータは、冗長化された（GLBP）ルータとして動作できます。このルータは、既存のフォワーディング ルータが機能しなくなった場合にアクティブになります。

GGSN：Gateway GPRS Support Node。携帯電話ユーザがパブリック データ ネットワーク（PDN）や指定のプライベート IP ネットワークにアクセスできるようにするワイヤレス ゲートウェイ。GGSN 機能は、Cisco ルータに実装されています。

GPRS：General Packet Radio Service。モバイル ワイヤレス サービス プロバイダーがモバイル加入者に対し、GSM ネットワーク上でパケットベースのデータ サービスを提供することを可能にする 2.5G モバイル通信テクノロジー。

GSM ネットワーク：Global System for Mobile Communications ネットワーク。世界中で（主に欧州とアジアで）使用されているデジタル携帯電話テクノロジー。GSM は、デジタル ワイヤレス通信の世界標準です。

Home Agent：Home Agent は Mobile Node（MN; 移動ノード）のホーム ネットワーク上のルータで、MN のホーム IP アドレスと気付アドレス（外部ネットワークや訪問先ネットワークでの MN の現在の場所）間のアソシエーションを保持します。HA は、ホーム ネットワークから離れている間は、パケットを MN にトンネリングしてリダイレクトします。

HSRP：Hot Standby Router Protocol（ホット スタンバイ ルータ プロトコル）。高いネットワーク可用性と透過的なネットワーク トポロジ変更を提供します。HSRP は、Hot Standby アドレスに送信されるすべてのパケットにサービスを提供するリード ルータとともに、Hot Standby ルータ グループを作成します。リード ルータはグループ内の他のルータによってモニタされ、その機能が停止すると、いずれかのスタンバイ ルータがリード ルータの役割と Hot Standby グループ アドレスを引き継ぎます。

IPCP：IP Control Protocol（IP 制御プロトコル）。IP over PPP の確立と設定に使用するプロトコル。

LCP：Link Control Protocol（リンク制御プロトコル）。PPP によって使用されるデータリンク接続の確立、設定、およびテストに使用するプロトコル。

PDSN：Packet Data Serving Node。Cisco PDSN は、Code Division Multiplex Access（CDMA; 符号分割多重接続）環境でのパケット データ サービスを使用可能にする、標準準拠のワイヤレス ゲートウェイです。アクセス ゲートウェイとして動作する Cisco PDSN は、シンプルな IP および Mobile IP アクセス、外部エージェントのサポート、Virtual Private Network（VPN; バーチャル プライベート ネットワーク）用のパケット送信を提供します。

PPP：Point-to-Point Protocol（ポイントツーポイント プロトコル）。同期回路および非同期回路上での、ルータ間およびホストとネットワーク間の接続を提供します。PPP は、ダイヤルアップ インターネット アクセスに最も一般的に使用されています。その機能には、アドレス通知、CHAP や PAP での認証、複数のプロトコルのサポート、リンク モニタリングなどが含まれます。

VRF：VPN ルーティングおよび転送インスタンス。VRF は、IP ルーティング テーブル、取得された転送テーブル、その転送テーブルを使用する一連のインターフェイス、転送テーブルに登録されるものを決定する一連のルールおよびルーティング プロトコルで構成されています。一般に、VRF には、Provider Edge（PE; プロバイダー エッジ）ルータに付加されるカスタマー VPN サイトが定義されたルーティング情報が格納されています。

VRRP : Virtual Router Redundancy Protocol。スタティックにデフォルトでルーティングされる環境に内在する単一障害点をなくします。VRRP は、LAN 上のいずれかの VRRP ルータに、仮想ルータとしての役割を動的に割り当てる選択プロトコルを指定します。仮想ルータに関連付けされた IP アドレスを制御し、これらの IP アドレスに送信されたパケットを転送する VRRP ルータは、「マスター」と呼ばれます。マスターが使用できなくなったとき、選択プロセスにより、転送処理のダイナミック フェールオーバーが行われます。この場合、エンド ホストにより、LAN 上のいずれかの仮想ルータ IP アドレスがデフォルトのファーストホップ ルータとして使用可能となります。

IP サービスの設定

ここでは、オプションの IP サービスを設定する手順について説明します。この章で説明する IP サービス コマンドの詳細については、『*Cisco IOS IP Application Services Command Reference*』を参照してください。この章で説明するその他のコマンドについて詳細が記載されている資料を探すには、コマンド リファレンス マスター インデックス、またはオンライン検索を使用してください。

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、「IP サービスの機能情報」（P.22）を参照してください。

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

この章の構成

IP サービスの概要

IP ソース ルーティング

Cisco IOS ソフトウェアは、すべてのパケットの IP ヘッダー オプションを検査します。RFC 791 に定義されている IP ヘッダー オプションである Strict Source Route、Loose Source Route、Record Route、および Time Stamp をサポートします。これらのオプションのいずれかがイネーブルにされているパケットを検出すると、適切なアクションを実行します。無効なオプションが設定されたパケットを検出すると、Internet Control Message Protocol（ICMP; インターネット制御メッセージ プロトコル）パラメータの問題に関するメッセージをパケットの送信元に送信し、該当のパケットを破棄します。

IP は、送信元 IP ホストが IP ネットワーク上のルートを指定できるプロビジョニング（「ソース ルーティング」と呼ばれます）を提供します。ソース ルーティングは、IP ヘッダーのオプションとして指定されます。ソース ルーティングが指定されると、ソフトウェアは指定されたソース ルートに従ってパケットを転送します。IP ソース ルーティングは、ネットワーク上の特定のルートを通るようにパケットに強制したい場合に採用されます。デフォルトでは、ソース ルーティングが実行されます。IP ソース ルーティングがネットワークでの正規の目的に使用されることはめったにありません。古い IP 実装では、ソース-ルート パケットが適切に処理されないことがあり、ソース ルーティング オプションを指定してデータグラムに送信することで、これらの実装を実行するデバイスがクラッシュすることがあります。可能である限り、IP ソース ルーティングをディセーブルにします。IP ソース ルーティングをディセーブルにすると、Cisco ルータは、ソース ルーティング オプションを送受信する IP パケットの転送を行いません。

ICMP の概要

Internet Control Message Protocol（ICMP; インターネット制御メッセージ プロトコル）は、元来、RFC 792 で TCP/IP スイート用に作成されたもので、少数のエラー状態を報告するように設計されました。ICMP は、さまざまなエラー状態を報告し、フィードバック機能やテスト機能を提供することもできます。各メッセージでは、共通のフォーマットが使用され、同じプロトコル ルールを使用して送受信されます。

ICMP により、カプセル化されたメッセージの IP デバイス間での送受信を許可することで、IP はアドレッシング、データグラム パッケージング、およびルーティングを実行できるようになります。これらのメッセージは、他の IP メッセージのように、IP データグラムにカプセル化されます。メッセージが生成されると、元の IP ヘッダーは ICMP メッセージにカプセル化され、これらの 2 つの情報は新しい IP ヘッダー内にカプセル化されて、エラー報告として送信元デバイスに返されます。

ICMP メッセージはさまざまな状況で送信されます。たとえば、データグラムが宛先に到達できない場合、ゲートウェイにデータグラムを転送するためのバッファリング機能がない場合、ゲートウェイが短いルート上でトラフィックを送信するホストを指定できる場合、などが挙げられます。メッセージに関するメッセージの無限後退を避けるため、ICMP メッセージに関する ICMP メッセージが送信されることはありません。

ICMP によって、IP の信頼性が高められることや、データグラム配信や制御メッセージが戻されることが確実になることはありません。一部のデータグラムは、データ損失が報告されることなく、ドロップされることがあります。IP を使用する上位レベルのプロトコルは、信頼性の高い通信が求められる場合、信頼性を高めるための独自の手順を実装する必要があります。

IPv6 および ICMP の詳細については、次の URL に掲載されている『*Cisco IOS IPv6 Configuration Guide*』の「Implementing IPv6 Addressing and Basic Connectivity」を参照してください。

http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-addrg_bsc_con.html

ICMP 到達不能エラー メッセージ

宛先ホストのアプリケーションに対してメッセージを完全に配信できない場合は、タイプ 3 のエラー メッセージが送信されます。ICMP ヘッダーに含まれる 6 つのコードに、次のような到達不能条件が示されます。

- 0：ネットワーク到達不能
- 1：ホスト到達不能
- 2：プロトコル到達不能
- 3：ポート到達不能
- 4：フラグメンテーションが必要であるのに「Don't Fragment」（DF）ビットが設定されている
- 5：ソース ルート機能停止

Cisco IOS ソフトウェアは、ICMP 到達不能宛先エラー メッセージの生成を抑止できます。これは「レート制限」と呼ばれます。デフォルトでは、0.5 秒の間に 2 つ以上の到達不能メッセージが生成されないようにします。コード 4 やその他の到達不能宛先エラー メッセージがあるため、このように間隔を空けて設定できます。ただし、送信されていない ICMP メッセージの数を表示する方法はありません。

送信されていないタイプ 3 メッセージをカウントして表示する方法は、ICMP 到達不能宛先カウンタ機能によって提供されます。ルータに対する Denial of Service（DoS; サービス拒否）攻撃を示す過剰なレート制限が見られる期間が発生すると、この機能によりコンソール ロギングにもエラー メッセージが表示されます。

不明なプロトコルを使用した、自身に宛てた非ブロードキャスト パケットを受け取ると、Cisco IOS ソフトウェアは送信元に ICMP プロトコル 到達不能メッセージを送り返します。同様に、宛先アドレスへのルートがないことが明らかで最終的な宛先に配信できないパケットを受け取ったときも、Cisco IOS ソフトウェアは送信元に ICMP プロトコル到達不能メッセージを送り返します。この機能はデフォルトでイネーブルになっています。

可能である限り、Internet Message Control Protocol（ICMP; インターネット制御メッセージ プロトコル）ホスト到達不能メッセージをディセーブルにします。ICMP は、パス、ルート、ネットワーク状態に関する情報をリレーする方法で、IP トラフィックをサポートします。これらのメッセージは、ネットワーク マッピング情報を取得することを目的に攻撃者によって利用されることがあります。

空のインターフェイスはパケット シンクであるため、ここで転送されたパケットは必ず破棄され、（機能がディセーブルになっていない限り）ホスト到達不能メッセージが生成されます。この場合、空のインターフェイスを使用して DoS 攻撃をブロックしていると、ローカル ネットワークではこれらのメッセージのフラッディングが発生します。このような状況に陥らないようにするためには、これらのメッセージをディセーブルにします。また、ブロックされたすべてのパケットは空のインターフェイスに転送されるため、ホスト到達不能メッセージを受信する攻撃者がそれらのメッセージを使用して Access Control

List（ACL; アクセス コントロール リスト）設定を利用できるようになることがあります。ルータに「null 0」インターフェイスを設定している場合は、廃棄されたパケットや空のインターフェイスにルーティングされたパケットの ICMP ホスト到達不能メッセージをディセーブルにしてください。

ICMP マスク応答メッセージ

ネットワーク デバイスでは、インターネットワーク内の特定のサブネットワークのサブネット マスクを認識することが必要になる場合があります。このような場合、この情報を取得するため、デバイスは ICMP マスク要求メッセージを送信することができます。必要な情報を保有するデバイスからの応答として、ICMP マスク応答メッセージが送信されます。Cisco IOS ソフトウェアは、ICMP マスク要求メッセージに応答できます（この機能がイネーブルになっている場合）。

これらのメッセージは、ネットワーク マッピング情報を取得することを目的に攻撃者によって利用されることがあります。

ICMP リダイレクト メッセージ

ルートは、最善ではないことがあります。たとえば、ルータは、パケットを受信したインターフェイスを通してパケットを再送信するように強制されることがあります。ルータが、パケットを受信したのと同じインターフェイスを通してパケットを再送信すると、Cisco IOS ソフトウェアはパケットの発信元に対して ICMP リダイレクト メッセージを送信し、ルータがサブネット上で受信デバイスに直接接続されていることと、パケットは同じサブネット上の別のシステムに転送する必要があることを知らせます。ソフトウェアがパケットの発信元に ICMP リダイレクト メッセージを送信するのは、送信元ホストは、このデバイスをまったく関与させることなく、パケットをネクストホップに送信できるからです。リダイレクト メッセージは、送信者に対し、ルートから受信デバイスを削除し、より具体的にパスを示すデバイスに置き換えるように指示します。この機能はデフォルトでイネーブルになっています。

適切に機能している IP ネットワークでは、ルータは独自のローカル サブネット上にあるホストにしかリダイレクトを送信しません。エンド ノードがリダイレクトを送信することはなく、またリダイレクトが複数のネットワーク ホップを通過することもありません。ただし、攻撃者がこれらのルールに違反することがあり、これに基づいた攻撃も見られます。ICMP リダイレクトをディセーブルにすると、ネットワークに運用上の影響を及ぼすことなく、この方法で攻撃される可能性を排除できます。

サービス拒否攻撃

サービス拒否は次第に懸念が高まってきている問題です。特に、このような攻撃に関連するコストには大きな関心が寄せられています。DoS 攻撃は、ネットワーク デバイスのパフォーマンス低下、デバイスのネットワークからの切断、システム クラッシュの発生、などの原因となります。ネットワーク サービスを利用できないと、企業やサービス プロバイダーは生産性低下や売上損失の損害を被ることになります。

DoS 攻撃の目的は、ユーザや組織がサービスまたはリソースにアクセスできないようにすることです。Web サイトが DoS 攻撃の危険にさらされると、数百万のユーザのそのサイトへのアクセスが拒否されます。通常、DoS 攻撃によって情報が不正に盗み取られることはありません。DoS 攻撃では、不正なユーザがアクセスできるようにするのではなく、許可されたユーザのアクセスを妨害することで、苛立たせたり、コストを発生させたりします。Distributed DoS（DDoS; 分散型 DoS）攻撃は、危険にさらされたシステムで攻撃パケットのフラッディングを発生させるように DoS 攻撃を増幅させたもので、これにより、対象システムのユーザのサービス拒否が生じます。

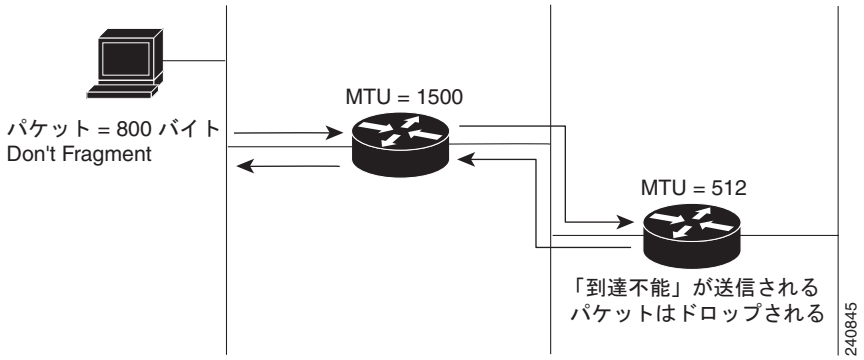
DoS 攻撃は、ICMP エコー要求（ping）のストリームが宛先サブネットにブロードキャストされるときに発生します。これらの要求の送信元アドレスは、ターゲットの送信元アドレスに改ざんされます。攻撃者が要求を送信すると、その都度、サブネット上のホストはターゲット上でフラッディングを発生さ

せ、帯域幅を浪費させます。大部分の DoS 攻撃は「Smurf」攻撃と呼ばれます。これは実行可能プログラムにちなんで名付けられたものです。ホストに対するネットワーク レベル攻撃のカテゴリに該当します。ICMP 到達不能宛先カウンタ機能の error-message ロギングがイネーブルになっていると、DoS 攻撃を簡単に検出できます。

PMTUD

Cisco IOS ソフトウェアは、RFC 1191 に定義されたとおりに、IP PMTUD メカニズムをサポートします。IP PMTUD を使用すると、ホストは経路上のさまざまなリンクで許容される Maximum Transmission Unit（MTU; 最大伝送ユニット）サイズの差異をダイナミックに検出し、対処できます。（パケットが、**ip mtu** インターフェイス コンフィギュレーション コマンドでインターフェイスに設定した MTU よりも大きい場合など）フラグメンテーションが必要であるのに「Don't Fragment」（DF）ビットが設定されているため、ルータがデータグラムを転送できない場合もあります。Cisco IOS ソフトウェアは送信元ホストにメッセージを送信し、この問題を警告します。ホストは、パス沿いにあるすべてのリンクでの最小パケット サイズに合わせて、宛先に送信するパケットをフラグメンテーションすることが必要になります。この技術を図 1 に示します。

図 1　　IP PMTUD



IP PMTUD は、ネットワーク内のリンクが機能停止して別のリンクを使用しなければならないときに、MTU サイズのリンクが異なる場合（そしてルータが異なる場合）に役立ちます。図 1 に示すように、ルータはネットワーク上で IP パケットを送信していますが、1 台目のルータの MTU は 1500 バイトに設定され、2 台目のルータの MTU は 512 バイトに設定されています。データグラムの「Don't Fragment」ビットが設定されていると、512 バイトのルータはデータグラムを転送できないため、このデータグラムはドロップされます。この場合、512 バイトより大きいパケットはすべてドロップされます。2 台目のルータは、「フラグメンテーションが必要であるのに「Don't Fragment」（DF）ビットが設定されている」ことを示す Code フィールドとともに、ICMP 宛先到達不能メッセージをデータグラムの送信元に返します。IP PMTUD をサポートするため、未使用のヘッダー フィールドの下位ビットにはネクストホップ ネットワーク リンクの MTU が含まれます。

IP PMTUD は、接続が確立されているものの、送信者が介在するリンクに関する情報をまったく有していない場合にも役立ちます。リンクで生じる最大 MTU を使用できるようにすることが推奨されます。MTU が大きいほど、ホストが送信しなければならないパケット数が少なくなります。

（注） IP PMTUD は、エンド ホストによって開始されるプロセスです。エンド ホストが IP PMTUD をサポートしない場合、受信デバイスは、エンド ホストでのデータグラムのフラグメンテーションを回避するメカニズムを持たないことになります。

発信インターフェイス上で小さい MTU が設定されているルータが、大きい MTU が設定されているホストからパケットを受信すると（たとえば、トークン リング インターフェイスからパケットを受信し、発信イーサネット インターフェイスに転送する場合など）、このルータは、受信したパケットを、発信インターフェイスの MTU よりも大きいサイズにフラグメンテーションします。パケットをフラグメンテーションすると、ルータのパフォーマンスは低下します。ネットワーク内のルータで受信パケットのフラグメンテーションを行わないようにするには、ネットワーク内のすべてのホストおよびルータで IP PMTUD を実行し、常に各ルータ インターフェイス タイプの MTU をできる限り大きく設定するようにします。

IP MAC アカウンティングと優先順位アカウンティング

Cisco IP アカウンティング サポートは、基本的な IP アカウンティング機能を提供します。IP アカウンティングをイネーブルにすると、ユーザが、送信元と宛先の IP アドレスに基づいて Cisco IOS ソフトウェアを介してスイッチングされたバイト数およびパケット数を参照できるようになります。中継 IP トラフィックだけが、発信ベースで測定されます。ソフトウェアが生成したトラフィックや、ソフトウェアで終了したトラフィックは、アカウンティング統計情報に含まれません。正確なアカウンティングの合計を得られるように、ソフトウェアは 2 つのアカウンティング データベース（アクティブ データベースとチェックポイント データベース）を維持します。

Cisco IP アカウンティング サポートは、IP アクセス リストに一致しなかった IP トラフィックを特定するための情報も提供します。IP アクセス リストに一致しなかった IP 送信元アドレスが特定されると、セキュリティ違反の可能性が警告されます。データでは、IP アクセス リスト コンフィギュレーションを確認する必要があることも通知されます。この機能をユーザが使用できるようにするには、**ip accounting access-violations** インターフェイス コンフィギュレーション コマンドを使用して、アクセス リストに一致しなかった IP アカウンティングをイネーブルにする必要があります。イネーブルにすると、ユーザは、送信元と宛先のペアのアクセス リストに対してセキュリティ違反を試みた送信元からのバイト数およびパケット数を表示できるようになります。デフォルトでは、IP アカウンティングは、アクセス リストに一致してルーティングされたパケット数を表示します。

MAC アドレス アカウンティング機能は、LAN インターフェイス上の送信元と宛先の MAC アドレスに基づいて IP トラフィックのアカウンティング情報を提供します。MAC アカウンティングは、一意の MAC アドレスとの間で IP パケットを送受信した、LAN インターフェイスの合計のパケット数とバイト数を計算します。また、最後に送受信したパケットのタイムスタンプも記録します。たとえば、IP MAC アカウンティングを使用して、Network Access Profile（NAPS; ネットワーク アクセス プロファイル）/ ピアリング ポイントでさまざまなピアとの間で送受信したトラフィック数を確認できます。IP MAC アカウンティングはイーサネット、ファスト イーサネット、FDDI インターフェイス上でサポートされ、Cisco Express Forwarding（CEF; シスコ エクスプレス フォワーディング）、distributed CEF（dCEF）、フロー、および最適なスイッチングをサポートします。

優先順位アカウンティング機能は、任意のインターフェイスの優先順位に基づいて、IP トラフィックのアカウンティング情報を提供します。この機能は、IP パケットを送受信したインターフェイスの合計のパケット数とバイト数を計算し、IP 優先順位に基づいて結果をソートします。この機能はすべてのインターフェイスおよびサブインターフェイスでサポートされ、CEF、dCEF、フロー、および最適なスイッチングをサポートします。

Show and Clear Commands for IOS Sockets

Show and Clear Commands for IOS Sockets 機能には、**show udp**、**show sockets**、および **clear sockets** コマンドが導入されました。これらの新しいコマンドは、Cisco IOS ソケット ライブラリのモニタリングや管理に役立ちます。

Cisco IOS ソフトウェアでは、ソケットはプロセス単位のエンティティです。これは、ソケットの最大数がプロセス単位であり、すべてのソケットはプロセスベースに管理されることを意味します。たとえば、各 Cisco IOS プロセスには、ファイル記述子番号が 1 のソケットを持たせることができます。これは、システム単位にファイル記述子を割り当てる UNIX やその他のオペレーティング システムとは異なります。

show コマンドと **clear** コマンドは、現在の機能と一致するようにプロセス単位に動作します。このため、コマンドによるアクションは、CLI で入力したプロセス ID で指定された特定のプロセスにのみ適用されます。

多くのアプリケーションでは、主にデバッグ目的で **show** コマンドと **clear** コマンドが必要になります。次に、これらのコマンドが役に立つシナリオの例を示します。

- アプリケーション H.323 は、音声呼にソケットを使用しています。現在の呼数から考えると、より多くのソケットに対応できるスペースが残っているはずです。ただし、これ以上、ソケットを開くことができません。このような場合、**show sockets** コマンドを使用して、すべてのソケット スペースを実際に使用しているか、または（利用可能な）未使用のソケットがあるかどうかを調べることができます。
- アプリケーションは特定のソケット イベントが発生するのを待機しています。UDP セグメントが見つかりましたが、アプリケーションはアクティブになりません。このような場合、**show udp** コマンドを使用して、モニタされているイベントのリストを表示し、UDP ソケット イベントがモニタされているか、またはソケット ライブラリがアプリケーションのアクティブ化に失敗していないかを判断することができます。
- アプリケーションは、特定のプロセスに関するすべてのソケットを閉じようとしています。このような場合、**clear sockets** コマンドを使用して、ソケットと、その下位にある TCP/UDP 接続または Stream Control Transmission Protocol（SCTP）アソシエーションの両方を閉じることができます。

IP サービスの設定方法

ネットワークの DoS 攻撃からの保護

ICMP は、パス、ルート、ネットワーク状態に関する情報をリレーする方法で、IP トラフィックをサポートします。ICMP メッセージは、ネットワーク マッピング情報を取得することを目的に攻撃者によって利用されることがあります。IP ソース ルーティングを使用して、送信元 IP ホストは IP ネットワーク上のルートを指定することができます。IP ソース ルーティングがネットワークでの正規の目的に使用されることはめったにありません。古い IP 実装では、ソース - ルート パケットが適切に処理されないことがあり、ソース ルーティング オプションを指定してデータグラムに送信することで、これらの実装を実行するデバイスがクラッシュすることがあります。

可能である限り、ICMP メッセージと IP ソース ルーティングはディセーブルにしてください。

手順の概要

1. **enable**
2. **configure terminal**
3. **no ip source-route**
4. **interface** *type/number*
5. **no ip unreachables**
6. **no ip redirects**
7. **no ip mask-reply**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**no ip source-route** **例：** `Router(config)# no ip source-route`	IP ソース ルーティングをディセーブルにします。
ステップ 4	**interface** *type/number* **例：** `Router(config)# interface null 0`	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 5	**no ip unreachables** **例：** `Router(config-if)# no ip unreachables`	到達不能な ICMP プロトコルとホスト到達不能メッセージの送信をディセーブルにします。このコマンドは、デフォルトでイネーブルになっています。 **（注）** 到達不能メッセージをディセーブルにすると、IP PMTUD もディセーブルになります。パス ディスカバリが Cisco IOS ソフトウェアにより到達不能メッセージを送信するためです。
ステップ 6	**no ip redirects** **例：** `Router(config-if)# no ip redirects`	ルートを学習するため、ICMP リダイレクト メッセージの送信をディセーブルにします。このコマンドは、デフォルトでイネーブルになっています。
ステップ 7	**no ip mask-reply** **例：** `Router(config-if)# no ip mask-reply`	ICMP マスク応答メッセージの送信をディセーブルにします。

ICMP Unreachable Rate Limiting User Feedback の設定

このタスクは、到達不能宛先パケットの統計情報をすべてクリアし、到達不能宛先メッセージの間隔を指定するために実行します。このタスクでは、パケット カウンタ（しきい値）と、コンソールへのロギング メッセージをトリガーする間隔も設定します。このタスクは、しきい値を設定した後に新しくロギングを開始する場合に有用です。

手順の概要

1. **enable**
2. **clear ip icmp rate-limit** [*interface-type interface-number*]
3. **configure terminal**
4. **ip icmp rate-limit unreachable** [**df**] [*ms*] [**log** [*packets*] [*interval-ms*]]
5. **exit**
6. **show ip icmp rate-limit** [*interface-type interface-number*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**clear ip icmp rate-limit** [*interface-type interface-number*] 例： `Router# clear ip icmp rate-limit ethernet 2/3`	設定されたすべてのインターフェイスに関する、現在の ICMP 到達不能統計情報をすべてクリアします。オプションの *interface-type* 引数と *interface-number* 引数を使用すると、1 つのインターフェイスに関する統計情報のみがクリアされます。
ステップ 3	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	**ip icmp rate-limit unreachable** [**df**] [*ms*] [**log** [*packets*] [*interval-ms*]] **例：** `Router(config)# ip icmp rate-limit unreachable df log 1100 12000`	メッセージ生成について、ICMP 到達不能宛先メッセージのレート制限と、エラー メッセージ ログのしきい値を指定します。デフォルトでは、0.5 秒の間に 2 つ以上の到達不能メッセージが送信されないようにします。 引数およびキーワードは次のとおりです。 • **df**：（任意）ICMP ヘッダーに「Don't Fragment」（DF）ビットが設定されていると、データグラムのフラグメンテーションは行われません。**df** キーワードを指定しないと、その他のすべてのタイプの宛先到達不能メッセージが送信されます。 • *ms*：（任意）到達不能メッセージが生成される間隔。有効範囲は 1 ～ 4294967295 です。 • **log**：（任意）エラー メッセージのリスト。具体的な引数は次のとおりです。 – *packets*：（任意）ログ生成のしきい値を決定するパケット数。デフォルト値は 1000 です。 – *interval-ms*：（任意）ロギング メッセージがトリガーされる間隔の時間制限。デフォルトは 60000（1 分）です。 **（注）** コマンドを設定するとすぐにカウントが開始します。
ステップ 5	**exit** **例：** `Router# exit`	特権 EXEC モードに戻ります。
ステップ 6	**show ip icmp rate-limit** [*interface-type interface-number*] **例：** `Router# show ip icmp rate-limit ethernet 2/3`	（任意）設定されたすべてのインターフェイスに関する、現在の ICMP 到達不能統計情報をすべて表示します。オプションの *interface-type* 引数と *interface-number* 引数を使用すると、1 つのインターフェイスに関する統計情報のみが表示されます。

例

次に、インターフェイスに到達不能な宛先を表示する **show ip icmp rate-limit** コマンドの出力例を示します。

```
Router# show ip icmp rate-limit

                           DF bit unreachables       All other unreachables
Interval (millisecond)     500                       500

Interface                  # DF bit unreachables     # All other unreachables
---------                  ---------------------     ------------------------
Ethernet0/0                0                         0
Ethernet0/2                0                         0
Serial3/0/3                0                         19

The greatest number of unreachables is on serial interface 3/0/3.
```

MTU パケット サイズの設定

すべてのインターフェイスには、デフォルト MTU パケット サイズが設定されています。Cisco IOS ソフトウェアがインターフェイスに設定されている MTU サイズを超える IP パケットのフラグメンテーションを行うように、IP MTU サイズを調整することができます。

MTU 値を変更すると（**mtu** インターフェイス コンフィギュレーション コマンドを使用）、IP MTU 値に影響を及ぼします。現在の IP MTU 値が MTU 値と同じである場合に MTU 値を変更すると、IP MTU 値は新しい MTU に一致するように自動的に変更されます。ただし、その逆は当てはまりません。つまり、IP MTU 値を変更しても、**mtu** インターフェイス コンフィギュレーション コマンドの値には影響しません。

物理メディア上にあるデバイスでは、正常に動作させるためには同じプロトコル MTU を使用する必要があります。

このタスクは、指定インターフェイスの MTU パケット サイズを設定するために実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type/number*
4. **ip mtu** *bytes*
5. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type*/*number* 例： `Router(config)# interface ethernet1/1`	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ip mtu** *bytes* 例： `Router(config-if)# ip mtu 300`	インターフェイスの IP MTU パケット サイズを設定します。
ステップ 5	**exit** 例： `Router(config-if)# exit`	特権 EXEC モードに戻ります。

IP アカウンティングの設定

IP アカウンティングをイネーブルにするため、このタスクはインターフェイスごとに実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip accounting-threshold** *threshold*
4. **ip accounting-list** *ip-address wildcard*
5. **ip accounting-transits** *count*
6. **interface** *type/number*
7. **ip accounting** [**access-violations**] [**output-packets**]
8. **ip accounting mac-address** {**input** | **output**}
   または
   ip accounting precedence {**input** | **output**}

手順の詳細

	コマンド	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip accounting-threshold** *threshold* 例： `Router(config)# ip accounting-threshold 500`	（任意）作成するアカウンティング エントリの最大数を設定します。
ステップ 4	**ip accounting-list** *ip-address wildcard* 例： `Router(config)# ip accounting-list 192.31.0.0 0.0.255.255`	（任意）ホストのアカウンティング情報をフィルタリングします。
ステップ 5	**ip accounting-transits** *count* 例： `Router(config)# ip accounting-transits 100`	（任意）IP アカウンティング データベースに格納される中継レコードの数を制御します。
ステップ 6	**interface** *type*/*number* 例： `Router(config)# interface ethernet1/1`	インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 7	**ip accounting** [**access-violations**] [**output-packets**] 例： `Router(config-if)# ip accounting access-violations`	基本的な IP アカウンティングをイネーブルにします。 • オプションの **access-violations** キーワードを使用して、IP アクセス リストに一致しなかった IP トラフィックを特定するため、IP アカウンティング機能をイネーブルにします。 • オプションの **output-packets** キーワードを使用して、インターフェイス上の IP パケット出力に基づいて IP アカウンティングをイネーブルにします。
ステップ 8	**ip accounting mac-address** {**input** | **output**} または **ip accounting precedence** {**input** | **output**} 例： `Router(config-if)# ip accounting mac-address output` または 例： `Router(config-if)# ip accounting precedence output`	（任意）受信（入力）または送信（出力）パケットの MAC アドレスに基づいて IP アカウンティングを設定します。 または （任意）受信（入力）または送信（出力）パケットの優先順位に基づいて IP アカウンティングを設定します。

IP ネットワークのモニタリングとメンテナンス

IP ルーティング テーブル、キャッシュ、データベース、ソケット プロセスの内容など、特定の統計情報を表示できます。結果の情報を使用して、リソースの活用法を判断したり、ネットワーク問題を解決したりできます。

手順の概要

1. **clear ip traffic**
2. **clear ip accounting** [**checkpoint**]
3. **clear sockets** *process-id*
4. **show ip accounting** [**checkpoint**] [**output-packets** | **access-violations**]
5. **show interface** [*type number*] **mac**
6. **show interface** [*type number*] **precedence**
7. **show ip redirects**
8. **show ip sockets**
9. **show sockets** *process-id* [**detail**] [**events**]
10. **show udp** [**detail**]
11. **show ip traffic**

（注） Cisco IOS Release 12.4(11)T および以降のリリースでは、**show ip sockets** コマンドは **show udp**、**show sockets**、および **show ip sctp** コマンドに置き換えられました。**show ip sctp** コマンドの詳細については、『*Cisco IOS Voice Command Reference*』を参照してください。

ステップ 1　**clear ip traffic**

すべてのインターフェイス上にあるすべての IP トラフィック統計カウンタをクリアするには、次のコマンドを使用します。

```
Router# clear ip traffic
```

ステップ 2　**clear ip accounting** [**checkpoint**]

特定のキャッシュ、テーブル、データベースのすべての内容を削除できます。キャッシュ、テーブル、またはデータベースは、特定の構造が無効になったり、無効になるおそれのあるときにクリアすることが必要になります。IP アカウンティングがイネーブルであるときにアクティブな IP アカウンティング データベースをクリアするには、次のコマンドを使用します。

```
Router# clear ip accounting
```

IP アカウンティングがイネーブルであるときにチェックポイントが作成された IP アカウンティング データベースをクリアするには、次のコマンドを使用します。

```
Router# clear ip accounting checkpoint
```

ステップ 3　**clear sockets** *process-id*

すべての IP ソケットを閉じ、その下位にあるトランスポート接続と特定のプロセスのデータ構造をクリアするには、次のコマンドを使用します。

```
Router# clear sockets 35
```

```
All sockets (TCP, UDP and SCTP) for this process will be cleared.
Do you want to proceed? [yes/no]: y
Cleared sockets for PID 35
```

ステップ 4 **show ip accounting** [**checkpoint**] [**output-packets** | **access-violations**]

アクセス リストの不一致を表示するには、**show ip accounting** コマンドを使用します。このコマンドを使用するには、まず、インターフェイス ベースで IP アカウンティングをイネーブルにする必要があります。

チェックポイント データベースを表示するには、**checkpoint** キーワードを使用します。アクセス コントロールと一致し、ルーティングを表示する必要のあるパケットに関する情報を指定するには、**output-packets** キーワードを使用します。送信元と宛先のペアの最後のパケットで一致しなかったアクセス リストの数を表示するには、**access-violations** キーワードを使用します。パケット数により、特定の宛先に対する攻撃の状況（攻撃の強さなど）が明らかになります。**access-violations** キーワードを指定しないと、このコマンドでは、デフォルトで、アクセス リストに一致してルーティングされたパケット数が表示されます。

output-packets キーワードと **access-violations** キーワードのどちらも指定しない場合は、デフォルトで output-packets が使用されます。

次に、**show ip accounting** コマンドの出力例を示します。

```
Router# show ip accounting

   Source           Destination              Packets               Bytes
 172.16.19.40    192.168.67.20                  7                 306
 172.16.13.55    192.168.67.20                 67                2749
 172.16.2.50     192.168.33.51                 17                1111
 172.16.2.50     172.31.2.1                    5                 319
 172.16.2.50     172.31.1.2                    463               30991
 172.16.19.40    172.16.2.1                     4                 262
 172.16.19.40    172.16.1.2                    28                2552
 172.16.20.2     172.16.6.100                  39                2184
 172.16.13.55    172.16.1.2                    35                3020
 172.16.19.40    192.168.33.51                1986               95091
 172.16.2.50     192.168.67.20                 233               14908
 172.16.13.28    192.168.67.53                 390               24817
 172.16.13.55    192.168.33.51               214669             9806659
 172.16.13.111   172.16.6.23                 27739             1126607
 172.16.13.44    192.168.33.51                35412             1523980
 192.168.7.21    172.163.1.2                     11                824
 172.16.13.28    192.168.33.2                    21               1762
 172.16.2.166    192.168.7.130                  797              141054
 172.16.3.11     192.168.67.53                    4                 246
 192.168.7.21    192.168.33.51                15696              695635
 192.168.7.24    192.168.67.20                   21                916
 172.16.13.111   172.16.10.1                     16               1137
 accounting threshold exceeded for 7 packets and 433 bytes
```

次に、**show ip accounting access-violations** コマンドの出力例を示します。アクセス リストに一致せず、ルーティングされなかったパケットが出力されます。

```
Router# show ip accounting access-violations

   Source           Destination      Packets        Bytes        ACL
172.16.19.40    192.168.67.20              7          306         77
172.16.13.55    192.168.67.20             67         2749        185
172.16.2.50     192.168.33.51             17         1111        140
172.16.2.50     172.16.2.1                5          319        140
172.16.19.40    172.16.2.1                4          262         77
Accounting data age is 41
```

ステップ 5　show interface [*type number*] **mac**

MAC アカウンティング用に設定されたインターフェイスの情報を表示するには、**show interface mac** コマンドを使用します。次に、**show interface mac** コマンドの出力例を示します。

```
Router# show interface ethernet 0/1 mac

Ethernet0/1
Input  (511 free)
0007.f618.4449(228):  4 packets, 456 bytes, last: 2684ms ago
Total:  4 packets, 456 bytes
Output  (511 free)
0007.f618.4449(228):  4 packets, 456 bytes, last: 2692ms ago
Total:  4 packets, 456 bytes
```

ステップ 6　show interface [*type number*] **precedence**

優先順位アカウンティング用に設定されたインターフェイスの情報を表示するには、**show interface precedence** コマンドを使用します。

次に、**show interface precedence** コマンドの出力例を示します。この例では、合計のパケット数とバイト数は IP パケットを受信（入力）または送信（出力）するインターフェイスについて算出され、結果は IP 優先順位に基づいてソートされます。

```
Router# show interface ethernet 0/1 precedence

Ethernet0/1
Input
Precedence 0:  4 packets, 456 bytes
Output
Precedence 0:  4 packets, 456 bytes
```

ステップ 7　show ip redirects

デフォルト ルータのアドレスおよび ICMP リダイレクト メッセージを受信するホストのアドレスを表示するには、**show ip redirects** コマンドを使用します。

次に、**show ip redirects** コマンドの出力例を示します。

```
Router# show ip redirects

Default gateway is 172.16.80.29

Host               Gateway           Last Use    Total Uses  Interface
172.16.1.111      172.16.80.240        0:00             9  Ethernet0
172.16.1.4        172.16.80.240        0:00             4  Ethernet0
```

ステップ 8　show ip sockets

IP ソケット情報を表示し、使用しているソケットが正しく開いていることを確認するには、**show ip sockets** コマンドを使用します。ローカルとリモートのエンドポイントがある場合は、特定されたポートを使用して接続が確立されます。

次に、**show ip sockets** コマンドの出力例を示します。

```
Router# show ip sockets

Proto    Remote          Port      Local           Port  In Out Stat TTY OutputIF
 17      10.0.0.0          0       172.16.186.193  67    0   0    1   0
 17      172.16.191.135   514      172.16.191.129  1811  0   0    0   0
 17      172.16.135.20    514      172.16.191.1    4125  0   0    0   0
 17      172.16.207.163   49       172.16.186.193  49    0   0    9   0
 17      10.0.0.0         123      172.16.186.193  123   0   0    1   0
 88      10.0.0.0         0        172.16.186.193  202   0   0    0   0
 17      172.16.96.59     32856    172.16.191.1    161   0   0    1   0
 17     --listen--              --any--        496  0    0   1    0
```

ステップ 9 **show sockets** *process-id* [**detail**] [**events**]

現在開いているソケットの数を表示し、*process-id* 引数を指定してトランスポート プロトコル プロセスに関する配信状況を表示するには、**show sockets** コマンドを使用します。次に、指定したプロセスで開いているソケットの総数を示す **show sockets** コマンドの出力例を示します。

```
Router# show sockets 35

Total open sockets - TCP:7, UDP:0, SCTP:0
```

次に、開いている同じプロセスについて、**detail** キーワードを使用して情報を表示した場合の出力例を示します。

```
Router# show sockets 35 detail

   FD LPort FPort Proto Type    TransID

   0  5000  0     TCP   STREAM  0x6654DEBC
State: SS_ISBOUND
Options: SO_ACCEPTCONN

   1  5001  0     TCP   STREAM  0x6654E494
State: SS_ISBOUND
Options: SO_ACCEPTCONN

   2  5002  0     TCP   STREAM  0x656710B0
State: SS_ISBOUND
Options: SO_ACCEPTCONN

   3  5003  0     TCP   STREAM  0x65671688
State: SS_ISBOUND
Options: SO_ACCEPTCONN

   4  5004  0     TCP   STREAM  0x65671C60
State: SS_ISBOUND
Options: SO_ACCEPTCONN

   5  5005  0     TCP   STREAM  0x65672238
State: SS_ISBOUND
Options: SO_ACCEPTCONN

   6  5006  0     TCP   STREAM  0x64C7840C
State: SS_ISBOUND
Options: SO_ACCEPTCONN

Total open sockets - TCP:7, UDP:0, SCTP:0
```

次に、IP ソケット イベント情報を表示する例を示します。

```
Router# show sockets 35 events

Events watched for this process: READ
FD Watched Present Select Present

0 --- --- R-- R--
```

ステップ 10　show udp [detail]

UDP プロセスに関する IP ソケット情報を表示するには、**show udp** コマンドを使用します。次に、UDP ソケットに関する詳細情報を表示する例を示します。

```
Router# show udp detail

 Proto    Remote      Port      Local       Port  In Out Stat TTY OutputIF
 17       10.0.0.0    0         10.0.21.70  67    0  0   2211 0
 Queues: output 0
         input  0 (drops 0, max 50, highwater 0)
 Proto    Remote      Port      Local       Port  In Out Stat TTY OutputIF
 17       10.0.0.0    0         10.0.21.70  2517  0   0  11   0
 Queues: output 0
         input  0 (drops 0, max 50, highwater 0)
 Proto    Remote      Port      Local       Port  In Out Stat TTY OutputIF
 17       10.0.0.0    0         10.0.21.70  5000  0  0   211  0
 Queues: output 0
         input  0 (drops 0, max 50, highwater 0)
 Proto    Remote      Port      Local       Port  In Out Stat TTY OutputIF
 17       10.0.0.0    0         10.0.21.70  5001  0  0   211  0
 Queues: output 0
         input  0 (drops 0, max 50, highwater 0)
 Proto    Remote      Port      Local       Port  In Out Stat TTY OutputIF
 17       10.0.0.0    0         10.0.21.70  5002  0  0   211  0
 Queues: output 0
         input  0 (drops 0, max 50, highwater 0)
 Proto    Remote      Port      Local       Port  In Out Stat TTY OutputIF
 17       10.0.0.0    0         10.0.21.70  5003  0  0   211  0
 Queues: output 0
         input  0 (drops 0, max 50, highwater 0)
 Proto    Remote      Port      Local       Port  In Out Stat TTY OutputIF
 17       10.0.0.0    0         10.0.21.70  5004  0  0   211  0
 Queues: output 0
         input  0 (drops 0, max 50, highwater 0)
```

（注）　Cisco IOS Release 12.4(11)T および以降のリリースでは、**show ip sockets** コマンドは **show udp**、**show sockets**、および **show ip sctp** コマンドに置き換えられました。**show ip sctp** コマンドの詳細については、『*Cisco IOS Voice Command Reference*』を参照してください。

ステップ 11　show ip traffic

IP プロトコル統計情報を表示するには、**show ip traffic** コマンドを使用します。次に、**clear ip traffic** コマンドでクリアされた IP トラフィック統計情報の例を示します。

```
Router# clear ip traffic
Router# show ip traffic

IP statistics:
 Rcvd:  0 total, 0 local destination
        0 format errors, 0 checksum errors, 0 bad hop count
        0 unknown protocol, 0 not a gateway
        0 security failures, 0 bad options, 0 with options
 Opts:  0 end, 0 nop, 0 basic security, 0 loose source route
        0 timestamp, 0 extended security, 0 record route
        0 stream ID, 0 strict source route, 0 alert, 0 cipso
        0 other
 Frags: 0 reassembled, 0 timeouts, 0 couldn't reassemble
        0 fragmented, 0 couldn't fragment
 Bcast: 0 received, 0 sent
 Mcast: 0 received, 0 sent
 Sent: 0 generated, 0 forwarded
```

```
 Drop: 0 encapsulation failed, 0 unresolved, 0 no adjacency
       0 no route, 0 unicast RPF, 0 forced drop

ICMP statistics:
 Rcvd: 0 format errors, 0 checksum errors, 0 redirects, 0 unreachable
       0 echo, 0 echo reply, 0 mask requests, 0 mask replies, 0 quench
       0 parameter, 0 timestamp, 0 info request, 0 other
       0 irdp solicitations, 0 irdp advertisements
 Sent: 0 redirects, 0 unreachable, 0 echo, 0 echo reply
       0 mask requests, 0 mask replies, 0 quench, 0 timestamp
       0 info reply, 0 time exceeded, 0 parameter problem
       0 irdp solicitations, 0 irdp advertisements

UDP statistics:
 Rcvd: 0 total, 0 checksum errors, 0 no port
 Sent: 0 total, 0 forwarded broadcasts

TCP statistics:
 Rcvd: 0 total, 0 checksum errors, 0 no port
 Sent: 0 total

Probe statistics:
 Rcvd: 0 address requests, 0 address replies
       0 proxy name requests, 0 where-is requests, 0 other
 Sent: 0 address requests, 0 address replies (0 proxy)
       0 proxy name replies, 0 where-is replies

EGP statistics:
 Rcvd: 0 total, 0 format errors, 0 checksum errors, 0 no listener
 Sent: 0 total

IGRP statistics:
 Rcvd: 0 total, 0 checksum errors
 Sent: 0 total

OSPF statistics:
 Rcvd: 0 total, 0 checksum errors
       0 hello, 0 database desc, 0 link state req
       0 link state updates, 0 link state acks

 Sent: 0 total

IP-IGRP2 statistics:
 Rcvd: 0 total
 Sent: 0 total

PIMv2 statistics: Sent/Received
 Total: 0/0, 0 checksum errors, 0 format errors
 Registers: 0/0, Register Stops: 0/0, Hellos: 0/0
 Join/Prunes: 0/0, Asserts: 0/0, grafts: 0/0
 Bootstraps: 0/0, Candidate_RP_Advertisements: 0/0

IGMP statistics: Sent/Received
 Total: 0/0, Format errors: 0/0, Checksum errors: 0/0
 Host Queries: 0/0, Host Reports: 0/0, Host Leaves: 0/0
 DVMRP: 0/0, PIM: 0/0
```

IP サービスの設定例

例：DoS 攻撃からのネットワークの保護

次に、ICMP がパス、ルート、およびネットワーク状態に関する情報をリレーしないように、イーサネット 0/0 の一部の ICMP デフォルトを変更する例を示します。このような情報は、攻撃者がネットワーク マッピング情報を入手するために使用される可能性があります。

到達不能メッセージをディセーブルにすると、IP PMTUD もディセーブルになるという副次的効果があります。これは、Cisco IOS ソフトウェアに到達不能メッセージを送信するように指示することによってパス ディスカバリが機能するためです。ネットワーク セグメント内にデバイスの台数が少なく、確実に信頼できるトラフィック パターン（ほとんど使用されないユーザ デバイスの台数が少ないセグメントでよく発生する）が見られる場合は、デバイスであまり使用されないオプションをディセーブルにすることを推奨します。

```
Router# configure terminal
Router(config)# no ip source-route
Router(config)#interface ethernet 0/0
Router(config-if)# no ip unreachables
Router(config-if)# no ip redirects
Router(config-if)# no ip mask-reply
```

例：ICMP 到達不能宛先カウンタの設定

次に、到達不能宛先パケット統計情報をすべてクリアし、到達不能宛先メッセージの間隔を指定する場合の例を示します。この例では、パケット カウンタのしきい値と、コンソールへのロギング メッセージをトリガーする間隔も設定します。

```
Router# clear ip icmp rate-limit ethernet 0/0
Router# configure terminal
Router(config)# ip icmp rate-limit unreachable df log 1100 12000
```

例：MTU パケット サイズの設定

次に、イーサネット インターフェイス 0/0 のデフォルトの MTU パケット サイズを設定する例を示します。

```
Router# configure terminal
Router(config)# interface ethernet 0/0
Router(config-if)# ip mtu 300
```

例：IP アカウンティングの設定

次に、送信元と宛先の MAC アドレス、および送受信するパケットの IP 優先順位に基づいて IP アカウンティングをイネーブルにする例を示します。

```
Router# configure terminal
Router(config)# interface ethernet0/5
Router(config-if)# ip accounting mac-address input
Router(config-if)# ip accounting mac-address output
Router(config-if)# ip accounting precedence input
Router(config-if)# ip accounting precedence output
```

次に、アクセス リストに一致しない IP トラフィックを特定する機能を使用し、また IP アカウンティング データベースに格納される中継レコードの数を 100 に指定して、アカウンティングをイネーブルにする例を示します。

```
Router# configure terminal
Router(config)# ip accounting-transits 100
Router(config)# interface ethernet0/5
Router(config-if)# ip accounting output-packets
Router(config-if)# ip accounting access-violations
```

その他の参考資料

関連資料

内容	参照先
IP アドレッシングとサービス設定作業	『*Cisco IOS IP Addressing Services Configuration Guide*』
IP アクセス リスト	『*Cisco IOS Security Configuration Guide: Securing the Data Plane*』の「Access Control Lists (ACLs)」
IP アプリケーション サービス コマンド：コマンド構文、コマンド モード、コマンド履歴、デフォルト設定、使用に関する注意事項、および例	『*Cisco IOS IP Application Services Command Reference*』

RFC

RFC	タイトル
RFC 791	「*Internet Protocol*」
RFC 792	「*Internet Control Message Protocol*」
RFC 1191	「*Path MTU discovery*」

シスコのテクニカル サポート

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

IP サービスの機能情報

表 1 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。

プラットフォーム サポートとソフトウェア イメージ サポートに関する情報を入手するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator を使用すると、特定のソフトウェア リリース、フィーチャ セット、またはプラットフォームをサポートするソフトウェア イメージを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 表 1 に、特定のソフトウェア リリース トレイン内の機能に対するサポートが導入されたソフトウェア リリースだけを示します。特に断りのないかぎり、そのソフトウェア リリース トレイン以降のリリースでもその機能がサポートされます。

表 1　IP サービスの機能情報

機能名	リリース	機能情報
Clear IP Traffic CLI	12.4(2)T 12.2(31)SB2	Clear IP Traffic CLI 機能で、**clear ip traffic** コマンドが導入されました。これにより、ルータをリロードするのではなく、ルータ上のすべての IP トラフィック統計情報がクリアされるようになりました。安全性を高めるため、このコマンドを入力すると、ユーザに確認プロンプトが表示されます。 この機能は、Cisco IOS Release 12.4(2)T で導入されました。 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。 • 「IP ネットワークのモニタリングとメンテナンス」（P.14） コマンド **clear ip traffic** がこの機能により導入されました。

表 1　IP サービスの機能情報 （続き）

機能名	リリース	機能情報
ICMP Unreachable Rate Limiting User Feedback	12.4(2)T 12.2(31)SB2	ICMP Unreachable Rate Limiting User Feedback 機能により、到達不能な宛先であるために破棄されたパケットをクリアして表示することができます。エラー メッセージをトリガーするしきい値の間隔を設定できます。メッセージ ロギングが生成されると、コンソールに表示されます。 この機能は、Cisco IOS Release 12.4(2)T で導入されました。 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。 • 「ICMP の概要」（P.2） • 「サービス拒否攻撃」（P.4） • 「ICMP Unreachable Rate Limiting User Feedback の設定」（P.9） • 「例：DoS 攻撃からのネットワークの保護」（P.20） **clear ip icmp rate-limit**、**ip icmp rate-limit unreachable**、**show ip icmp rate-limit** の各コマンドがこの機能により導入または変更されました。
IP Precedence Accounting	12.2(21) 12.1(27b)E1 12.1(5)T15 12.2(25)S 12.2(33)SRA 12.2(18)SXF13 12.2(33) SXH1 15.0(1)S	IP Precedence Accounting 機能により、インターフェイス上の優先順位に基づいて IP トラフィックのアカウンティング情報が提供されます。この機能は、IP パケットを送受信したインターフェイスごとにパケット数の合計とバイト数の合計を計算し、IP 優先順位に基づいて結果をソートします。この機能はすべてのインターフェイスおよびサブインターフェイスでサポートされ、CEF、dCEF、フロー、および最適なスイッチングをサポートします。 この機能に関する詳細については、次の各項を参照してください。 • 「IP MAC アカウンティングと優先順位アカウンティング」（P.6） • 「例：IP アカウンティングの設定」（P.21） **show interface precedence** および **ip accounting precedence** の各コマンドがこの機能により導入されました。

表 1　IP サービスの機能情報 （続き）

機能名	リリース	機能情報
Show and Clear Commands for IOS Sockets	12.4(11)T	Show and Clear Commands for IOS Sockets 機能には、**show udp**、**show sockets**、および **clear sockets** コマンドが導入されました。これらの新しいコマンドは、Cisco IOS ソケットライブラリのモニタリングや管理に役立ちます。 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。 • 「Show and Clear Commands for IOS Sockets」（P.6） • 「IP ネットワークのモニタリングとメンテナンス」（P.14） **clear sockets**、**show sockets**、**show udp** の各コマンドがこの機能により導入または変更されました。 コマンド **show ip sockets** がこの機能により置換されました。

TCP の設定

TCP は、データ転送で使用される、データと確認応答のフォーマットを規定したプロトコルです。TCP は、通信の参加者がデータ転送の前に接続を確立する必要があるため、コネクション型のプロトコルです。フロー制御やエラー訂正を行うことで、TCP では順序通りにパケットが配送される信頼性が保証されます。IP パケット が損失する場合や順序通りに到達しない場合、TCP は正しいパケットを受信するまで再送を要求するので、信頼性があると見なされます。この章では、TCP に関する概念と、ネットワーク上での TCP の設定方法について説明します。

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、「TCP の機能情報」（P.22）を参照してください。

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

この章の構成

TCP の前提条件

TCP タイムスタンプ、TCP 選択的確認応答、および TCP ヘッダー圧縮

TCP タイムスタンプは送信と応答の双方で常に送られ、ヘッダーのタイムスタンプ値は常に変化するので、TCP ヘッダー圧縮では発信パケットを圧縮しません。シリアル リンクでの TCP ヘッダー圧縮を許可すると、TCP タイムスタンプ オプションはディセーブルにされます。シリアル ラインで TCP ヘッダー圧縮を使用する場合、TCP タイムスタンプと TCP 選択的確認応答はディセーブルにする必要があります。どちらの機能もデフォルトではディセーブルです。TCP 選択的確認応答がイネーブルの場合、ディセーブルにするには、**no ip tcp selective-ack** コマンドを使用します。

TCP の概要

TCP サービス

TCP は IP 環境で信頼性のあるデータ転送を提供します。TCP は Open Systems Interconnection（OSI）参照モデルのトランスポート層（レイヤ 4）に対応します。サービスの中で、TCP が提供するものとして、ストリーム データ転送、信頼性、能率的なフロー制御、全二重通信、およびデータ多重化があります。

ストリーム データ転送では、TCP はシーケンス番号で識別される構造化されないバイト ストリームを配送します。このサービスの利点は、アプリケーションがデータを TCP に渡す前にブロックに分ける必要がないことです。TCP は、バイト列をセグメント単位にグループ化し、IP に渡して配送させます。

TCP は、インターネットワークを介したエンドツーエンドの確実なパケット配送というコネクション型動作で信頼性を実現します。これは、受信側への確認応答で、発信側が次に受信を予期するバイト位置をその確認応答の番号として示し、バイト列を順序づけすることによって行います。指定された期間

に確認応答がないバイト列は再送されます。TCP の信頼性メカニズムを使用すれば、デバイスで、消失、遅延、重複、または破損したパケットを処理できます。タイムアウト メカニズムを使用すれば、デバイスで、消失パケットを検出して、再送信を要求できます。

TCP は効率的にフローを制御します。これは、受信 TCP プロセスが、送信元に確認応答を返すときに、内部バッファをオーバーフローさせずに受信可能な最も高いシーケンス番号を指定することを意味します。

TCP には全二重通信が備わっており、同時に送信と受信を処理できます。

TCP データ多重化では、同時に存在する多数の上位層の通信を、単一接続の上で多重化することができます。

TCP 接続の確立

信頼できる転送サービスを使用するには、TCP ホストは相手側とコネクション型のセッションを確立する必要があります。接続の確立は、「スリーウェイ ハンドシェイク」メカニズムを使用して実行されます。

スリーウェイ ハンドシェイクでは、接続の端点からの初期シーケンス値を両側で合意することで双方を同期します。また、このメカニズムでは、両側でデータ転送が可能になっていることと、お互いに相手側も転送が可能だと認識されることが保証されます。スリーウェイ ハンドシェイクは、セッションが確立されている間か終了した後で、パケットを転送しないため、または再送するために必要です。

各ホストは、送信しているストリーム内のバイト位置を追跡するために使われるシーケンス番号をランダムに選択します。その後、スリーウェイ ハンドシェイクは次のように進行します。

- 最初のホスト（ホスト A）が、初期シーケンス番号（X）と接続の要求を示すために同期開始（SYN）ビットを設定したパケットを送信して、接続を開始します。
- 2 番目のホスト（ホスト B）が SYN を受信し、シーケンス番号 X を記録し、SYN 確認応答（ACK = X + 1）によって応答します。ホスト B は自分自身の初期シーケンス番号（SEQ = Y）を含めます。ACK = 20 は、そのホストがバイト 0 ～ 19 を受信済みで、次はバイト 20 を予期していることを示します。このテクニックは前方確認応答と呼ばれます。
- ホスト A は、ホスト B が送信したすべてのバイトを受け取ったことに対し、ホスト A が次に予期する受信バイト位置（ACK = Y + 1）を示す前方確認応答でこれに応答します。次にデータ転送が始まります。

TCP 接続試行時間

Cisco IOS ソフトウェアが TCP 接続の確立に試行する待ち時間を設定できます。接続試行時間はホスト パラメータなので、デバイスを通過するトラフィックについてではなく、デバイスを起源とするトラフィックについてだけ関連するものです。TCP 接続試行時間を設定するには、グローバル コンフィギュレーション モードで **ip tcp synwait-time** コマンドを使用します。デフォルトは 30 秒です。

TCP 選択的確認応答

TCP 選択的確認応答機能は、1 つの TCP データ ウィンドウから複数のパケットが損失する場合のパフォーマンスを改善します。

この機能ができる前は、累積する確認応答から使用できる限られた情報で、TCP 送信者はラウンドトリップ時間に関する 1 つの損失パケットについてだけ知ることができました。積極的な送信者は、早い段階でパケットを再送信できますが、そのような再送信セグメントがすでに正常受信されている可能性があります。

TCP 選択的確認応答機能はパフォーマンスの改善に役立ちます。受信側の TCP ホストは送信側に選択的確認応答パケットを返し、送信側に受信済みのデータを知らせることができます。言い換えると、受信側はパケットを順序通りに受け取らなかったということを通知できます。送信側は、それで（最初の損失パケット以降すべてではなく）欠けているデータ セグメントだけを再送できます。

選択的確認応答の前に、TCP が 8 パケット ウィンドウのうちパケット 4 と 7 を損失すると、TCP はパケット 1、2、および 3 の確認応答だけ受信します。パケット 4 ～ 8 を再送信する必要があります。選択的確認応答を使うと、TCP はパケット 1、2、3、5、6、および 8 の確認応答を受け取ります。パケット 4 と 7 だけを再送信する必要があります。

TCP 選択的確認応答は 1 つの TCP ウィンドウ内で複数のパケットが損失したときだけ使われます。この機能がイネーブルでも使用しない場合、パフォーマンスに影響はありません。TCP 選択的確認応答をイネーブルにするには、グローバル コンフィギュレーション モードで **ip tcp selective-ack** コマンドを使用します。

TCP 選択的確認応答の詳細については、RFC 2018 を参照してください。

TCP タイムスタンプ

TCP タイムスタンプ オプションによって、TCP ラウンドトリップ時間の計測精度が向上します。タイムスタンプは送信と応答の双方で常に送信され、ヘッダーのタイムスタンプ値はいつも変化するため、TCP ヘッダー圧縮では発信パケットを圧縮しません。シリアル リンクでの TCP ヘッダー圧縮を許可すると、TCP タイムスタンプ オプションはディセーブルにされます。TCP タイムスタンプ オプションをイネーブルにするには、**ip tcp timestamp** コマンドを使用します。

TCP タイムスタンプの詳細については、RFC 1323 を参照してください。TCP ヘッダー圧縮の詳細については、『*Cisco IOS Quality of Service Solutions Configuration Guide*』の「Configuring TCP Header Compression」の章を参照してください。

TCP 最大リード サイズ

Telnet や rlogin で、TCP が入力キューから一度に読み込むことのできる最大の文字数は、デフォルトで非常に大きな値（32 ビット整数で正の最大値）です。TCP 最大リード サイズ値を変更するには、グローバル コンフィギュレーション モードで **ip tcp chunk-size** コマンドを使用します。

この値を変更することは推奨しません。

TCP PMTUD

PMTUD は TCP 接続 エンドポイント間のネットワーク帯域幅利用効率を最大化する方式で、RFC 1191 で説明されています。IP PMTUD を使用すると、ホストは経路上のさまざまなリンクで許容される Maximum Transmission Unit（MTU; 最大伝送ユニット）サイズの差異をダイナミックに検出し、対処できます。フラグメンテーションが必要（パケットが **interface** コンフィギュレーション コマンドを使用してインターフェイスに対して設定した MTU よりも大きい場合）なのに、「don't fragment」（DF）ビットがセットされているため、ルータがデータグラムを転送できない場合があります。中間ゲートウェイが、「Fragmentation needed and DF bit set」Internet Control Message Protocol（ICMP）メッセージを送信ホストに送信して、問題を警告します。この ICMP メッセージを受信すると、ホストは仮定のパス MTU を減らし、その結果として経路上の全リンクの最小パケットサイズに適した、より小さなパケットを送信します。

デフォルトでは、TCP PMTUD はディセーブルです。この機能がイネーブルかディセーブルかに関わらず、既存の接続は影響を受けません。

異なるサブネット上のシステム間でバルク データを移動するために TCP 接続を使用する場合、この機能をイネーブルにすることを推奨します。Remote Source-Route Bridging（RSRB; リモート ソース ルート ブリッジング）を TCP カプセル化、Serial Tunnel（STUN; シリアル トンネル）、X.25 Remote Switching（XOT; X.25 リモート スイッチング、X.25 over TCP とも呼ばれます）、および何らかのプロトコル変換構成で使用している場合も、この機能をイネーブルにすることを推奨します。

ホストとして動作するルータが開設した接続への PMTUD をイネーブルにするには、**ip tcp path-mtu-discovery** グローバル コンフィギュレーション コマンドを使用します。

PMTUD の詳細については、『*Cisco IOS IP Application Services Configuration Guide*』の「Configuring IP Services」の章を参照してください。

TCP ウィンドウ スケーリング

TCP ウィンドウ スケーリング機能は、RFC 1323「*TCP Extensions for High Performance*」内のウィンドウ スケーリング オプションに対するサポートを追加します。Long Fat Network（LFN; 広帯域高遅延ネットワーク）と呼ばれる大きな帯域遅延積の特性を持つネットワーク経路での TCP のパフォーマンスを改善するため、より大きなウィンドウ サイズが推奨されます。TCP ウィンドウ スケーリングの強化で、そのサポートを提供します。

Cisco IOS ソフトウェアでのウィンドウ スケーリング拡張は TCP ウィンドウの定義を 32 ビットに拡大し、この 32 ビット値を TCP ヘッダーの 16 ビットウィンドウ フィールドに適合させるため、スケール係数を使用します。ウィンドウ サイズはスケール係数 14 まで大きくすることができます。典型的なアプリケーションは、広帯域高遅延ネットワークで動作するときにスケール係数 3 を使います。

TCP ウィンドウ スケーリング機能は RFC 1323 に準拠しています。最大ウィンドウ サイズは、1,073,741,823 バイトに増加しています。より大きなスケーラブル ウィンドウ サイズによって、広帯域高遅延ネットワーク上での TCP のパフォーマンスを向上できます。TCP ウィンドウ サイズを設定するには、グローバル コンフィギュレーション モードで **ip tcp window-size** コマンドを使用します。

TCP スライディング ウィンドウ

TCP スライディング ウィンドウにより、ホストは確認応答を待つ前に複数のバイト列やパケットを送信できるため、ネットワークの帯域幅をより効率的に使用できます。

TCP では、受信側は現在のウィンドウ サイズをすべてのパケットに設定します。TCP はバイト ストリーム 接続を提供しているため、ウィンドウ サイズはバイト単位で表現されます。ウィンドウは、送信者が確認応答を待機する前に送信できるデータ バイト数です。初期ウィンドウ サイズは接続確立時に示されますが、フロー制御によってデータ転送の間に変わる可能性があります。ウィンドウ サイズが 0 のときは「データ送信禁止」を意味します。デフォルトの TCP ウィンドウ サイズは 4128 バイトです。ルーターが大きなパケット（536 バイトよりも大きい）を送信していると確認できない限り、デフォルト値をそのまま使用することを推奨します。デフォルトのウィンドウ サイズを変更するには、**ip tcp window-size** コマンドを使用します。

たとえば、TCP スライディング ウィンドウの動作で、ウィンドウ サイズが 5 バイトの受信側に送るバイト シーケンス（1 ～ 10 の番号が付いた）があるとします。送信側は、最初の 5 バイトを取り囲むようにウィンドウを配置して、それをまとめて送信します。送信側はその後、確認応答を待ちます。

受信側は、ACK = 6 で応答します。これは 1 ～ 5 バイトを受け取り、次に 6 バイト目を予期していることを示します。同じパケットの中では、ウィンドウ サイズが 5 だと示します。送信側はスライディング ウィンドウを右に 5 バイト分ずらし、6 ～ 10 バイトを転送します。受信側は、ACK = 11 で応答します。これは、次に 11 バイト目を予期していることを示します。このパケットで、受信側はウィンドウ サイズが 0 であると示すことができます（例えば、内部バッファがいっぱいになったため）。この時点では、受信側からウィンドウ サイズが 1 以上の別パケットが送信されるまで、送信側はこれ以上のバイト列を送信できません。

TCP 発信キューサイズ

接続に TTY が関連付けられている場合（たとえば Telnet 接続など）、接続ごとの TCP 発信キューサイズはデフォルトで 5 セグメントです。接続に関連付けられている TTY がない場合、デフォルトのキューサイズは 20 セグメントです。デフォルト値を 5 セグメントから変更するには、**ip tcp queuemax** コマンドを使用します。

TCP 輻輳回避

TCP 輻輳回避機能を使用すると、単一のウィンドウ内で複数パケットが損失しているとき、TCP 送信側に対する確認応答パケットをモニタできます。以前は、送信側は高速リカバリ モードを終了するか、3 以上の重複確認応答パケットを待ってから次の未応答パケットを再送信するか、または再送タイマーのスロー スタートを待ちました。これは、パフォーマンスの問題になることがありました。

RFC 2581 および RFC 3782 の実装では、高速リカバリの期間に受信する部分確認応答への応答を組み込む高速リカバリ アルゴリズムの改良に対応し、単一のウィンドウ内で複数パケットが損失している状況でのパフォーマンスを改善します。

この機能は、既存の高速リカバリ アルゴリズムの強化です。この機能をイネーブルまたはディセーブルにするコマンドはありません。

debug ip tcp transactions コマンドの出力は、次の状態を表示することによって、確認応答パケットをモニタするように拡張されています。

- 高速リカバリ モードに移行した TCP。
- 高速リカバリ モードの間に受信した重複する確認応答。
- 受信した部分確認応答。

TCP 明示的輻輳通知

Explicit Congestion Notification（ECN; TCP 明示的輻輳通知）機能では、中間のルータが端点のホストにネットワーク輻輳が差し迫っていることを通知できるようになります。また、Telnet、Web 閲覧、音声や映像データの転送を含む、遅延やパケット損失の影響を受けるアプリケーションに関連付けられた TCP セッションのサポートも強化されています。この機能の利点は、データ転送時の遅延やパケット損失の軽減です。TCP 明示的輻輳通知をイネーブルにするには、グローバル コンフィギュレーション モードで **ip tcp ecn** コマンドを使用します。

TCP MSS 調整

TCP MSS 調整機能では、ルータを通過する一時的なパケット（特に SYN ビットが設定された TCP セグメント）の Maximum Segment Size（MSS; 最大セグメント サイズ）を設定することができるようになります。中間のルータで SYN パケットが切り捨てられないように最大セグメント サイズ値を指定するには、インターフェイス コンフィギュレーション モードで **ip tcp adjust-mss** コマンドを使用します。

ホスト（通常は PC）がサーバと TCP セッションを開始するときは、TCP SYN パケットの MSS オプション フィールドを使って IP セグメント サイズをネゴシエートします。MSS フィールドの値は、ホスト上の MTU 設定によって決まります。PC のデフォルト MSS 値は 1500 バイトです。

PPP over Ethernet（PPPoE）標準は、1,492 バイトのみの MTU をサポートします。ホストと PPPoE での MTU サイズの不一致は、ホストとサーバの間にあるルータで 1500 バイトのパケットが損失し、PPPoE を介した TCP セッションが終了する原因となる場合があります。たとえホストでパス MTU

（パス全体から正しい MTU を検出します）がイネーブルでも、パス MTU が機能するためにホストからリレーする必要がある ICMP エラー メッセージをシステム管理者がディセーブルにすることがあり、セッションが損失する場合があります。

ip tcp adjust-mss コマンドで TCP SYN パケットの MSS 値を調整すると、TCP セッション損失防止の役に立ちます。

ip tcp adjust-mss コマンドは、ルータを通過する TCP 接続に対してのみ有効です。

ほとんどの場合、**ip tcp adjust-mss** コマンドの *max-segment-size* 引数の最適値は 1,452 バイトです。この値に IP ヘッダーの 20 バイト、TCP ヘッダーの 20 バイト、および PPPoE ヘッダーの 8 バイトを足すと、イーサネット リンクの MTU サイズに適合する 1500 バイトのパケットになります。

設定手順については、「一時的な TCP SYN パケットに対する MSS 値、および MTU の設定」（P.10）を参照してください。

TCP アプリケーション フラグ拡張

TCP アプリケーション フラグ拡張機能によって、TCP アプリケーションに関する追加のフラグが表示可能になります。フラグには、ステータスやオプションという 2 種類のタイプがあります。ステータス フラグは、再送タイムアウト、アプリケーション クローズ、リスンの同期（SYNC）ハンドシェイクなど、TCP 接続のステータスを示します。追加のフラグは、VPN Routing and Forwarding（VRF; VPN ルーティングおよび転送）インスタンスが設定されているかどうか、ユーザが待機中かどうか、キープアライブ タイマーが動作中かどうかなどの設定オプションのステートを示します。TCP アプリケーション フラグを表示するには、**show tcp** コマンドを使用します。

TCP Show 拡張

TCP Show 拡張機能では、ホスト名形式ではなく、IP 形式でアドレスを表示したり、接続に関連付けられた VRF テーブルを表示したりする機能が導入されています。全エンドポイントのステータスを IP 形式のアドレス付きで表示するには、**show tcp brief numeric** コマンドを使用します。

ゼロフィールドと TCP パケット

Cisco IOS Release 15.0(1)M、12.2(33)XNE、12.2(33)SXI1、および 12.2(33)SRE と Cisco IOS XE Release 2.5 よりも前のリリースでは、ルータ上でゼロフィールド TCP パケットが受信されると、TCP パケット カウンタがインクリメントされました。

Cisco IOS Release 15.0(01)M、12.2(33)XNE、12.2(33)SXI1、および 12.2(33)SRE と Cisco IOS XE Release 2.5 以降のリリースでは、ルータ上でゼロフィールド TCP パケットが受信されると、TCP パケット カウンタがインクリメントされません。

show ip traffic コマンドが設定されているときに、ゼロフィールド TCP パケットが受信されると、それが TCP 統計情報フィールドの下に 0 として表示されます。**debug ip tcp packet** コマンドが設定されており、ゼロフィールド TCP パケットが受信された場合は、次のようなデバッグ メッセージが表示されます。

```
Jan 19 21:57:28.487: TCP: Alert! Received a segment with cleared flags 10.4.14.49
```

TCP MIB for RFC 4022 サポート

TCP MIB for RFC 4022 サポート機能で、RFC 4022「*Management Information Base for the Transmission Control Protocol (TCP)*」に対するサポートが導入されました。RFC 4022 は、TCP の管理容易性を向上させるための TCP MIB の増分変更です。

選択されたプラットフォーム、Cisco IOS リリース、およびフィーチャ セットの MIB を検索してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。

http://www.cisco.com/go/mibs

TCP の設定方法

- 「TCP パフォーマンス パラメータの設定」（P.8）（任意）
- 「一時的な TCP SYN パケットに対する MSS 値、および MTU の設定」（P.10）（任意）
- 「TCP パフォーマンス パラメータの確認」（P.11）（任意）

TCP パフォーマンス パラメータの設定

前提条件

- ウィンドウ スケーリングをサポートするには、リンクの両側を設定する必要があります。設定しないと、最大ウィンドウ サイズとしてデフォルトの 65,535 バイトが適用されます。
- リモートピアとのスリーウェイ ハンドシェイク中に ECN の機能がネゴシエートされるため、ECN をサポートするには、リモート ピアが ECN 対応である必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip tcp synwait-time** *seconds*
4. **ip tcp path-mtu-discovery** [**age-timer** {*minutes* | **infinite**}]
5. **ip tcp selective-ack**
6. **ip tcp timestamp**
7. **ip tcp chunk-size** *characters*
8. **ip tcp window-size** *bytes*
9. **ip tcp ecn**
10. **ip tcp queuemax** *packets*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip tcp synwait-time** *seconds* 例： `Router(config)# ip tcp synwait-time 60`	（任意）Cisco IOS ソフトウェアが TCP 接続の確立を試行する待ち時間を設定します。 • デフォルトは 30 秒です。
ステップ 4	**ip tcp path-mtu-discovery** [**age-timer** {*minutes* | **infinite**}] 例： `Router(config)# ip tcp path-mtu-discovery age-timer 11`	（任意）PMTUD をイネーブルにします。 • **age-timer**：TCP がより大きな MSS でパス MTU を再評価する分単位の時間間隔です。デフォルト値は 10 分です。最大で 30 分です。 • **infinite**：age timer をディセーブルにします。
ステップ 5	**ip tcp selective-ack** 例： `Router(config)# ip tcp selective-ack`	（任意）TCP 選択的確認応答をイネーブルにします。
ステップ 6	**ip tcp timestamp** 例： `Router(config)# ip tcp timestamp`	（任意）TCP タイムスタンプをイネーブルにします。

	コマンドまたはアクション	目的
ステップ 7	**ip tcp chunk-size** *characters* 例： `Router(config)# ip tcp chunk-size 64000`	（任意）Telnet や rlogin に対する TCP 最大リード サイズを設定します。 **（注）** この値を変更することは推奨しません。
ステップ 8	**ip tcp window-size** *bytes* 例： `Router(config)# ip tcp window-size 75000`	（任意）TCP ウィンドウ サイズを設定します。 • *bytes* 引数には 0 ～ 1073741823 の整数を設定できます。ウィンドウ スケーリングが LFN をサポートできるようにするには、TCP ウィンドウ サイズを 65535 より大きくする必要があります。ウィンドウ スケーリングが設定されていない場合、デフォルトのウィンドウ サイズは 4128 です。 **（注）** Cisco IOS Release 15.0(1)M 以降では、*bytes* 引数を 68 ～ 1073741823 の整数に設定できます。
ステップ 9	**ip tcp ecn** 例： `Router(config)# ip tcp ecn`	（任意）TCP の ECN をイネーブルにします。
ステップ 10	**ip tcp queuemax** *packets* 例： `Router(config)# ip tcp queuemax 10`	（任意）TCP 発信キュー サイズを設定します。

一時的な TCP SYN パケットに対する MSS 値、および MTU の設定

ルータを通過する一時的なパケット（特に SYN ビットが設定された TCP セグメント）の MSS を設定し、IP パケットの MTU サイズを設定するには、この作業を実行します。

ip tcp adjust-mss コマンドと同じインターフェイス上で **ip mtu** コマンドを設定する場合は、次のコマンドと値を使用することを推奨します。

- **ip tcp adjust-mss 1452**
- **ip mtu 1492**

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip tcp adjust-mss** *max-segment-size*
5. **ip mtu** *bytes*
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* 例： `Router(config)# interface ethernet 0/1`	インターフェイス タイプを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ip tcp adjust-mss** *max-segment-size* 例： `Router(config-if)# ip tcp adjust-mss 1452`	ルータを通過する TCP SYN パケットの MSS 値を調整します。 • *max-segment-size* 引数には、MSS をバイト単位で指定します。指定できる値の範囲は 500 ～ 1460 です。
ステップ 5	**ip mtu** *bytes* 例： `Router(config-if)# ip mtu 1492`	各インターフェイスにおいて送信される IP パケットの MTU サイズをバイト単位で設定します。
ステップ 6	**end** 例： `Router(config-if)# end`	グローバル コンフィギュレーション モードに戻ります。

TCP パフォーマンス パラメータの確認

手順の概要

1. **show tcp** [*line-number*] [**tcb** *address*]
2. **show tcp brief** [**all** | **numeric**]
3. **debug ip tcp transactions**
4. **debug ip tcp congestion**

手順の詳細

ステップ 1 **show tcp** [*line-number*] [**tcb** *address*]

TCP 接続のステータスを表示します。引数およびキーワードは次のとおりです。

- *line-number*：（任意）Telnet 接続ステータスの絶対行番号。
- **tcb**：（任意）ECN 対応の接続の Transmission Control Block（TCB; 転送制御ブロック）。
- *address*：（任意）TCB アドレス（16 進数）。有効な範囲は、0x0 ～ 0xFFFFFFFF です。

次に、ECN が利用可能な接続に関する詳細情報を 16 進数アドレスで表示する **show tcp tcb** コマンドの出力例を示します。

```
Router# show tcp tcb 0x62CD2BB8

Connection state is LISTEN, I/O status: 1, unread input bytes: 0
Connection is ECN enabled
Local host: 10.10.10.1, Local port: 179
Foreign host: 10.10.10.2, Foreign port: 12000

Enqueued packets for retransmit: 0, input: 0 mis-ordered: 0 (0 bytes)

Event Timers (current time is 0x4F31940):
Timer          Starts    Wakeups            Next
Retrans             0          0             0x0
TimeWait            0          0             0x0
AckHold             0          0             0x0
SendWnd             0          0             0x0
KeepAlive           0          0             0x0
GiveUp              0          0             0x0
PmtuAger            0          0             0x0
DeadWait            0          0             0x0

iss:          0 snduna:          0 sndnxt:          0     sndwnd:      0
irs:          0 rcvnxt:          0 rcvwnd:       4128  delrcvwnd:      0

SRTT: 0 ms, RTTO: 2000 ms, RTV: 2000 ms, KRTT: 0 ms
minRTT: 60000 ms, maxRTT: 0 ms, ACK hold: 200 ms
Flags: passive open, higher precedence, retransmission timeout

TCB is waiting for TCP Process (67)

Datagrams (max data segment is 516 bytes):
Rcvd: 6 (out of order: 0), with data: 0, total data bytes: 0
Sent: 0 (retransmit: 0, fastretransmit: 0), with data: 0, total data
bytes: 0
```

Cisco IOS ソフトウェア モジュラリティ

次に、ソフトウェア モジュラリティ イメージから **show tcp tcb** コマンドの出力例を示します。

```
Router# show tcp tcb 0x1059C10

Connection state is ESTAB, I/O status: 0, unread input bytes: 0
Local host: 10.4.2.32, Local port: 23
Foreign host: 10.4.2.39, Foreign port: 11000
VRF table id is: 0

Current send queue size: 0 (max 65536)
Current receive queue size: 0 (max 32768)  mis-ordered: 0 bytes

Event Timers (current time is 0xB9ACB9):
Timer          Starts    Wakeups            Next(msec)
```

```
Retrans             6          0               0
SendWnd             0          0               0
TimeWait            0          0               0
AckHold             8          4               0
KeepAlive          11          0         7199992
PmtuAger            0          0               0
GiveUp              0          0               0
Throttle            0          0               0

irs:    1633857851  rcvnxt: 1633857890  rcvadv: 1633890620  rcvwnd:  32730
iss:    4231531315  snduna: 4231531392  sndnxt: 4231531392  sndwnd:   4052
sndmax: 4231531392  sndcwnd:     10220

SRTT: 84 ms,  RTTO: 650 ms,  RTV: 69 ms,  KRTT: 0 ms
minRTT: 0 ms,  maxRTT: 200 ms, ACK hold: 200 ms

Keepalive time: 7200 sec, SYN wait time: 75 sec
Giveup time: 0 ms, Retransmission retries: 0, Retransmit forever: FALSE

State flags: none

Feature flags: Nagle

Request flags: none
Window scales: rcv 0, snd 0, request rcv 0, request snd 0
Timestamp option: recent 0, recent age 0, last ACK sent          0

Datagrams (in bytes): MSS 1460, peer MSS 1460, min MSS 1460, max MSS 1460
Rcvd: 14 (out of order: 0), with data: 10, total data bytes: 38
Sent: 10 (retransmit: 0, fastretransmit: 0), with data: 5, total data bytes: 76

Header prediction hit rate: 72 %

Socket states: SS_ISCONNECTED, SS_PRIV

Read buffer flags: SB_WAIT, SB_SEL, SB_DEL_WAKEUP
Read notifications: 4

Write buffer flags: SB_DEL_WAKEUP
Write notifications: 0
Socket status: 0
```

ステップ 2 **show tcp brief** [**all** | **numeric**]

（任意）アドレスを IP 形式で表示します。

TCP 接続のエンドポイントに関する簡潔な説明を表示するには、**show tcp brief** コマンドを使用します。Domain Name System（DNS; ドメイン ネーム システム）ホスト名形式のアドレスですべてのエンドポイントに関するステータスを表示するには、オプションの **all** キーワードを使用します。このキーワードを使用していない場合は、LISTEN ステートのエンドポイントは表示されません。IP 形式のアドレスですべてのエンドポイントに関するステータスを表示するには、オプションの **numeric** キーワードを使用します。

（注） ルータで **ip domain-lookup** コマンドがイネーブルになっていて **show tcp brief** コマンドが実行された場合、出力表示のためのルータ応答時間は非常に遅くなります。応答時間を早くするには、**ip domain-lookup** コマンドをディセーブルにします。

次に、ユーザが Telnet でシステムに接続している間の **show tcp brief** コマンドでの出力例を示します。

```
Router# show tcp brief

TCB       Local Address           Foreign Address        (state)
609789AC  Router.cisco.com.23     cider.cisco.com.3733   ESTAB
```

次の例は、**numeric** キーワードを使用して IP 形式のアドレスが表示された後の IP アクティビティを示しています。

```
Router# show tcp brief numeric

TCB           Local Address          Foreign Address     (state)
6523A4FC      10.1.25.3.11000        10.1.25.3.23         ESTAB
65239A84      10.1.25.3.23           10.1.25.3.11000      ESTAB
653FCBBC      *.1723 *.* LISTEN
```

ステップ 3　debug ip tcp transactions

状態変化、再送、重複パケットのように重要な TCP トランザクションに関する情報を表示するには、**debug ip tcp transactions** コマンドを使用します。このコマンドは、データリンク レイヤ上層に分離される TCP/IP ネットワークでのパフォーマンス上の問題をデバッグするときに特に有用です。

次に、**debug ip tcp transactions** コマンドの出力例を示します。

```
Router# debug ip tcp transactions

TCP: sending SYN, seq 168108, ack 88655553
TCP0: Connection to 10.9.0.13:22530, advertising MSS 966
TCP0: state was LISTEN -> SYNRCVD [23 -> 10.9.0.13(22530)]
TCP0: state was SYNSENT -> SYNRCVD [23 -> 10.9.0.13(22530)]
TCP0: Connection to 10.9.0.13:22530, received MSS 956
TCP0: restart retransmission in 5996
TCP0: state was SYNRCVD -> ESTAB [23 -> 10.9.0.13(22530)]
TCP2: restart retransmission in 10689
TCP2: restart retransmission in 10641
TCP2: restart retransmission in 10633
TCP2: restart retransmission in 13384 -> 10.0.0.13(16151)]
TCP0: restart retransmission in 5996 [23 -> 10.0.0.13(16151)]
```

debug ip tcp transactions コマンド出力の次の行は、TCP が高速リカバリモードに移行したことを示しています。

```
fast re-transmit - sndcwnd - 512, snd_last - 33884268765
```

debug ip tcp transactions コマンド出力の次の行は、TCP が高速リカバリ モードのときに重複確認応答が受信されたこと（1 行目）と、部分確認応答が受信されていたこと（2 行目）を示しています。

```
TCP0:ignoring second congestion in same window sndcwn - 512, snd_1st - 33884268765
TCP0:partial ACK received sndcwnd:338842495
```

ステップ 4　debug ip tcp congestion

debug ip tcp congestion コマンドは、TCP 輻輳イベントに関する情報を表示するために使用します。また、**debug ip tcp congestion** コマンドは、データリンク層上で切り分けた、TCP/IP ネットワーク上の性能上の問題をデバッグするために使用できます。さらに、このコマンドは、TCP の送信ウィンドウ、輻輳ウィンドウ、および輻輳しきい値ウィンドウ内のばらつきに関する情報も表示します。

次に、**debug ip tcp congestion** コマンドの出力例を示します。

```
Router# debug ip tcp congestion

*May 20 22:49:49.091: Setting New Reno as congestion control algorithm
*May 22 05:21:47.281: Advance cwnd by 12
*May 22 05:21:47.281: TCP85FD0C10: sndcwnd: 1472
```

```
*May 22 05:21:47.285: Advance cwnd by 3
*May 22 05:21:47.285: TCP85FD0C10: sndcwnd: 1475
*May 22 05:21:47.285: Advance cwnd by 3
*May 22 05:21:47.285: TCP85FD0C10: sndcwnd: 1478
*May 22 05:21:47.285: Advance cwnd by 9
*May 22 05:21:47.285: TCP85FD0C10: sndcwnd: 1487
.
.
.
*May 20 22:50:32.559: [New Reno] sndcwnd: 8388480 ssthresh: 65535 snd_mark: 232322
*May 20 22:50:32.559: 10.168.10.10:42416 <---> 10.168.30.11:49100 congestion window
changes
*May 20 22:50:32.559: cwnd from 8388480 to 2514841, ssthresh from 65535 to 2514841
```

Cisco IOS TCP では、New Reno がデフォルト輻輳制御アルゴリズムです。ただし、アプリケーションで Binary Increase Congestion Control（BIC）を輻輳制御アルゴリズムとして使用することもできます。次に、BIC 輻輳制御アルゴリズムを使用した **debug ip tcp congestion** コマンドからの出力例を示します。

```
Router# debug ip tcp congestion

*May 22 05:21:42.281: Setting BIC as congestion control algorithm
*May 22 05:21:47.281: Advance cwnd by 12
*May 22 05:21:47.281: TCP85FD0C10: sndcwnd: 1472
*May 22 05:21:47.285: Advance cwnd by 3
*May 22 05:21:47.285: TCP85FD0C10: sndcwnd: 1475
*May 22 05:21:47.285: Advance cwnd by 3
*May 22 05:21:47.285: TCP85FD0C10: sndcwnd: 1478
*May 22 05:21:47.285: Advance cwnd by 9
*May 22 05:21:47.285: TCP85FD0C10: sndcwnd: 1487
.
.
.
.
.
.
*May 20 22:50:32.559: [BIC] sndcwnd: 8388480 ssthresh: 65535 bic_last_max_cwnd: 0
last_cwnd: 8388480
*May 20 22:50:32.559: 10.168.10.10:42416 <---> 10.168.30.11:49100 congestion window
changes
*May 20 22:50:32.559: cwnd from 8388480 to 2514841, ssthresh from 65535 to 2514841
*May 20 22:50:32.559: bic_last_max_cwnd changes from 0 to 8388480
```

TCP の設定例

例：TCP ECN の設定の確認

次の例では、TCP ECN が設定されていることを確認する方法を示します。

```
Router# show running-config

Building configuration...
.
.
.
ip tcp ecn ! ECN is configured.
.
.
.
```

次の例では、指定された接続（ローカル ホスト）上で、TCP が ECN 対応かどうかの確認方法を示します。

```
Router# show tcp tcb 123456A

!Local host
!
Connection state is ESTAB, I/O status: 1, unread input bytes: 0
Connection is ECN Enabled
Local host: 10.1.25.31, Local port: 11002
Foreign host: 10.1.25.34, Foreign port: 23
```

次の例では、1 つのアドレスについて簡易情報を表示させる方法を示しています。

```
Router# show tcp brief
!
TCB          Local address            Foreign Address        (state)
609789C      Router.cisco.com.23      cider.cisco.com.3733    ESTAB
```

次の例では、IP TCP ECN デバッグをイネーブルにする方法を示します。

```
Router# debug ip tcp ecn
!
TCP ECN debugging is on
!
Router# telnet 10.1.25.31

Trying 10.1.25.31 ...
!
01:43:19: 10.1.25.35:11000 <---> 10.1.25.31:23   out ECN-setup SYN
01:43:21: 10.1.25.35:11000 <---> 10.1.25.31:23   congestion window changes
01:43:21: cwnd from 1460 to 1460, ssthresh from 65535 to 2920
01:43:21: 10.1.25.35:11000 <---> 10.1.25.31:23   in non-ECN-setup SYN-ACK
```

TCP 接続が ECN を利用するときは、それ以前にホストは、Echo Congestion Experience（ECE; エコー輻輳経験）および Congestion Window Reduced（CWR; 輻輳ウィンドウ減少）ビットがヘッダーに設定されている ECN-setup SYN（synchronization）パケットをリモートの端点に送ります。ECE および CWR ビットを設定すると、輻輳のことではなく、送信中の TCP が ECN 対応であることをリモートの端点に示します。リモートの端点は、ECN-setup SYN-ACK（確認応答）パケットを送信側ホストに送ります。

この例の「out ECN-setup SYN」テキストは、ECE ビットと CWR ビットが設定された SYN パケットがリモート エンドに送信されたことを意味します。「in non-ECN-setup SYN-ACK」行は、リモートの端点は ECN 要求を承認する確認応答をしなかったため、このセッションでは ECN を利用できないことを示します。

次のデバッグ出力は、双方の端点で ECN 機能がイネーブルであることを示します。ECN-setup SYN に対し、相手側の端点が ECN-setup SYN-ACK メッセージを使用して承認の確認応答を返しました。この接続の以後のセッションでは、ECN を使用できます。

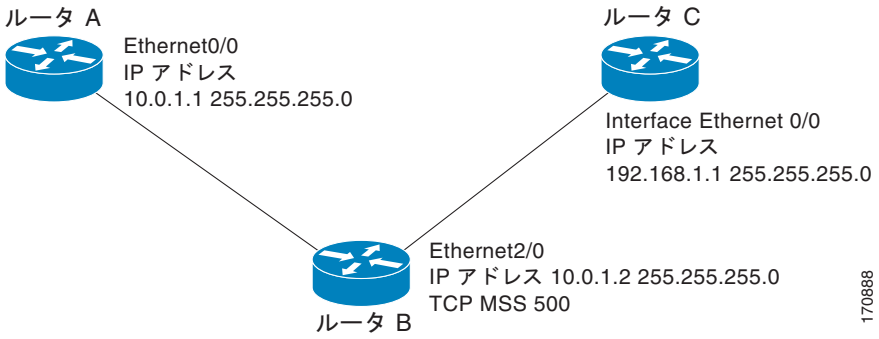
```
Router# telnet 10.10.10.10

Trying 10.10.10.10 ... Open
Password required, but none set
!
1d20h: 10.1.25.34:11003 <---> 10.1.25.35:23   out ECN-setup SYN
1d20h: 10.1.25.34:11003 <---> 10.1.25.35:23   in ECN-setup SYN-ACK
```

次は、ホストが接続されていることを確認する方法を示します。

```
Router# show debugging
!
TCP:
  TCP Packet debugging is on
  TCP ECN debugging is on
!
Router# telnet 10.1.25.234
!
Trying 10.1.25.234 ...
!
00:02:48: 10.1.25.31:11001 <---> 10.1.25.234:23   out ECN-setup SYN
00:02:48: tcp0: O CLOSED 10.1.25.234:11001 10.1.25.31:23 seq 1922220018
        OPTS 4 ECE CWR SYN  WIN 4128
00:02:50: 10.1.25.31:11001 <---> 10.1.25.234:23   congestion window changes
00:02:50: cwnd from 1460 to 1460, ssthresh from 65535 to 2920
00:02:50: tcp0: R SYNSENT 10.1.25.234:11001 10.1.25.31:23 seq 1922220018
        OPTS 4 ECE CWR SYN  WIN 4128
00:02:54: 10.1.25.31:11001 <---> 10.1.25.234:23   congestion window changes
00:02:54: cwnd from 1460 to 1460, ssthresh from 2920 to 2920
00:02:54: tcp0: R SYNSENT 10.1.25.234:11001 10.1.25.31:23 seq 1922220018
        OPTS 4 ECE CWR SYN  WIN 4128
00:03:02: 10.1.25.31:11001 <---> 10.1.25.234:23   congestion window changes
00:03:02: cwnd from 1460 to 1460, ssthresh from 2920 to 2920
00:03:02: tcp0: R SYNSENT 10.1.25.234:11001 10.1.25.31:23 seq 1922220018
        OPTS 4 ECE CWR SYN  WIN 4128
00:03:18: 10.1.25.31:11001 <---> 10.1.25.234:23   SYN with ECN disabled
00:03:18: 10.1.25.31:11001 <---> 10.1.25.234:23   congestion window changes
00:03:18: cwnd from 1460 to 1460, ssthresh from 2920 to 2920
00:03:18: tcp0: O SYNSENT 10.1.25.234:11001 10.1.25.31:23 seq 1922220018
        OPTS 4 SYN  WIN 4128
00:03:20: 10.1.25.31:11001 <---> 10.1.25.234:23   congestion window changes
00:03:20: cwnd from 1460 to 1460, ssthresh from 2920 to 2920
00:03:20: tcp0: R SYNSENT 10.1.25.234:11001 10.1.25.31:23 seq 1922220018
        OPTS 4 SYN  WIN 4128
00:03:24: 10.1.25.31:11001 <---> 10.1.25.234:23   congestion window changes
00:03:24: cwnd from 1460 to 1460, ssthresh from 2920 to 2920
00:03:24: tcp0: R SYNSENT 10.1.25.234:11001 10.1.25.31:23 seq 1922220018
        OPTS 4 SYN  WIN 4128
00:03:32: 10.1.25.31:11001 <---> 10.1.25.234:23   congestion window changes
00:03:32: cwnd from 1460 to 1460, ssthresh from 2920 to 2920
00:03:32: tcp0: R SYNSENT 10.1.25.234:11001 10.1.25.31:23 seq 1922220018
        OPTS 4 SYN  WIN 4128
    !Connection timed out; remote host not responding
```

例：TCP MSS 調整の設定

図 1　TCP MSS 調整のトポロジ例



次の例では、図 1 に示すトポロジ例のインターフェイス調整値を設定して確認する方法を示します。ルータ B で、インターフェイスの調整値を設定します。

```
Router_B(config)# interface ethernet2/0
Router_B(config-if)# ip tcp adjust-mss 500
```

MSS 調整が設定されたルータ B を使用して、ルータ A からルータ C に Telnet します。

```
Router_A# telnet 192.168.1.1
Trying 192.168.1.1... Open
```

ルータ C からデバッグ出力を監視します。

```
Router_C# debug ip tcp transactions

Sep 5 18:42:46.247: TCP0: state was LISTEN -> SYNRCVD [23 -> 10.0.1.1(38437)]
Sep 5 18:42:46.247: TCP: tcb 32290C0 connection to 10.0.1.1:38437, peer MSS 500, MSS is
500
Sep 5 18:42:46.247: TCP: sending SYN, seq 580539401, ack 6015751
Sep 5 18:42:46.247: TCP0: Connection to 10.0.1.1:38437, advertising MSS 500
Sep 5 18:42:46.251: TCP0: state was SYNRCVD -> ESTAB [23 -> 10.0.1.1(38437)]
```

ルータ B で設定されたとおりに MSS が 500 に調整されます。

次の例は、MSS 値を 1452 にした PPPoE クライアントの設定を示します。

```
Router(config)# vpdn enable
Router(config)# no vpdn logging
Router(config)# vpdn-group 1
Router(config-vpdn)# request-dialin
Router(config-vpdn-req-in)# protocol pppoe
Router(config-vpdn-req-in)# exit
Router(config-vpdn)# exit
Router(config)# interface Ethernet0
Router(config-if)# ip address 192.168.100.1.255.255.255.0
Router(config-if)# ip tcp adjust-mss 1452
Router(config-if)# ip nat inside
Router(config-if)# exit
Router(config)# interface ATM0
Router(config-if)# no ip address
Router(config-if)# exit
Router(config-if)# no atm ilmi-keepalive
Router(config-if)# pvc 8/35
Router(config-if)# pppoe client dial-pool-number 1
Router(config-if)# dsl equipment-type CPE
Router(config-if)# dsl operating-mode GSHDSL symmetric annex B
```

```
Router(config-if)# dsl linerate AUTO
Router(config-if)# exit
Router(config)# interface Dialer1
Router(config-if)# ip address negotiated
Router(config-if)# ip mtu 1492
Router(config-if)# ip nat outside
Router(config-if)# encapsulation ppp
Router(config-if)# dialer pool 1
Router(config-if)# dialer-group 1
Router(config-if)# ppp authentication pap callin
Router(config-if)# ppp pap sent-username sohodyn password 7 141B1309000528
Router(config-if)# ip nat inside source list 101 Dialer1 overload
Router(config-if)# exit
Router(config)# ip route 0.0.0.0.0.0.0.0 Dialer1
Router(config)# access-list permit ip 192.168.100.0.0.0.255 any
```

例：TCP アプリケーション フラグ拡張の設定

次の出力は、**show tcp** コマンドを使用して表示されたフラグ（ステータスとオプション）を示しています。

```
Router# show tcp
.
.
.
Status Flags: passive open, active open, retransmission timeout
 App closed

Option Flags: vrf id set
IP Precedence value: 6
.
.
.
SRTT: 273 ms, RTTO: 490 ms, RTV: 217 ms, KRTT: 0 ms
minRTT: 0 ms, maxRTT: 300 ms, ACK hold: 200 ms
```

例：IP 形式でのアドレスの表示

次の例は、**numeric** キーワードを使用して IP 形式のアドレスを表示する IP アクティビティを示しています。

```
Router# show tcp brief numeric

TCB           Local Address          Foreign Address     (state)
6523A4FC      10.1.25.3.11000        10.1.25.3.23         ESTAB
65239A84      10.1.25.3.23           10.1.25.3.11000      ESTAB
653FCBBC      *.1723 *.* LISTEN
```

その他の参考資料

関連資料

内容	参照先
IP アドレッシングとサービス設定作業	『*Cisco IOS IP Addressing Services Configuration Guide*』
IP アプリケーション サービス コマンド：コマンド構文、コマンド モード、コマンド履歴、デフォルト設定、使用に関する注意事項、および例	『*Cisco IOS IP Application Services Command Reference*』
PMTUD	『*Configuring IP Services*』
TCP セキュリティ機能	• 『*TCP Out-of-Order Packet Support for Cisco IOS Firewall and Cisco IOS IPS*』 • 『*Configuring TCP Intercept (Preventing Denial-of-Service Attacks)*』
TCP ヘッダー圧縮、 クラスベースの TCP ヘッダー圧縮	• 『*Configuring Class-Based RTP and TCP Header Compression*』 • 『*Configuring TCP Header Compression*』
トラブルシューティング TCP	『*Internetwork Troubleshooting Handbook* 』の「*Troubleshooting TCP/IP*」の部分

規格

規格	タイトル
新しい規格または変更された規格はサポートされていません。また、既存の規格に対するサポートに変更はありません。	—

MIB

MIB	MIB リンク
CISCO-TCP-MIB	選択されたプラットフォーム、シスコ ソフトウェア リリース、およびフィーチャ セットの MIB を検索してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
RFC 793	「*Transmission Control Protocol*」
RFC 1191	「*Path MTU discovery*」
RFC 1323	「*TCP Extensions for High Performance*」
RFC 2018	「*TCP Selective Acknowledgment Options*」
RFC 2581	「*TCP Congestion Control*」
RFC 3168	「*The Addition of Explicit Congestion Notification (ECN) to IP*」
RFC 3782	「*The NewReno Modification to TCP's Fast Recovery Algorithm*」
RFC 4022	「*Management Information Base for the Transmission Control Protocol (TCP)*」

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 ・テクニカル サポートを受ける ・ソフトウェアをダウンロードする ・セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける ・ツールおよびリソースへアクセスする - Product Alert の受信登録 - Field Notice の受信登録 - Bug Toolkit を使用した既知の問題の検索 ・Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する ・トレーニング リソースへアクセスする ・TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

TCP の機能情報

表 1 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。

プラットフォーム サポートとソフトウェア イメージ サポートに関する情報を入手するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator を使用すると、特定のソフトウェア リリース、フィーチャ セット、またはプラットフォームをサポートするソフトウェア イメージを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 表 1 に、特定のソフトウェア リリース トレイン内の機能に対するサポートが導入されたソフトウェア リリースだけを示します。特に断りのないかぎり、そのソフトウェア リリース トレイン以降のリリースでもその機能がサポートされます。

表 1　TCP の機能情報

機能名	リリース	機能情報
TCP アプリケーション フラグ 拡張	12.4(2)T 12.2(31)SB2	TCP アプリケーション フラグ拡張機能によって、TCP アプリケーションに関する追加のフラグが表示可能になります。フラグには、ステータスやオプションという 2 種類のタイプがあります。ステータス フラグは、再送タイムアウト、アプリケーション クローズ、リスンの同期（SYNC）ハンドシェイクなど、TCP 接続のステータスを示します。追加のフラグは、VRF 識別が設定されているかどうか、ユーザが待機中かどうか、キープアライブ タイマーが動作中かどうかなどの設定オプションのステートを示します。 次の項では、この機能に関する情報について説明します。 • 「TCP アプリケーション フラグ拡張」（P.7） • 「TCP パフォーマンス パラメータの確認」（P.11） • 「例：TCP アプリケーション フラグ拡張の設定」（P.19） コマンド **show tcp** がこの機能により変更されました。

表 1　TCP の機能情報 （続き）

機能名	リリース	機能情報
TCP 輻輳回避	12.3(7)T	TCP 輻輳回避機能を使用すると、単一のウィンドウ内で複数パケットが損失しているとき、TCP 送信側に対する確認応答パケットをモニタできます。以前は、送信側は高速リカバリ モードを終了するか、3 以上の重複確認応答パケットを待ってから次の未応答パケットを再送信するか、または再送タイマーのスロー スタートを待ちました。これは、パフォーマンスの問題になることがありました。 RFC 2581 および RFC 3782 の実装では、高速リカバリの期間に受信する部分確認応答への応答を組み込む高速リカバリ アルゴリズムの改良に対応し、単一のウィンドウ内で複数パケットが損失している状況でのパフォーマンスを改善します。 この機能は、既存の高速リカバリ アルゴリズムの強化です。この機能をイネーブルまたはディセーブルにするコマンドはありません。 **debug ip tcp transactions** コマンドの出力は、次の状態を表示することによって、確認応答パケットをモニタするように拡張されています。 • 高速リカバリ モードに移行した TCP。 • 高速リカバリ モードの間に受信した重複する確認応答。 • 受信した部分確認応答。 この機能に関する詳細については、次の各項を参照してください。 • 「TCP 輻輳回避」（P.6） • 「TCP パフォーマンス パラメータの確認」（P.11） コマンド **debug ip tcp transactions** がこの機能により変更されました。

表 1　TCP の機能情報 （続き）

機能名	リリース	機能情報
TCP 明示的輻輳通知	12.3(7)T	Explicit Congestion Notification（ECN; TCP 明示的輻輳通知）機能では、中間のルータが端点のホストにネットワーク輻輳が差し迫っていることを通知できるようになります。また、Telnet、Web 閲覧、音声や映像データの転送を含む、遅延やパケット損失の影響を受けるアプリケーションに関連付けられた TCP セッションのサポートも強化されています。この機能の利点は、データ転送時の遅延やパケット損失の軽減です。 この機能に関する詳細については、次の各項を参照してください。 • 「TCP 明示的輻輳通知」（P.6） • 「TCP パフォーマンス パラメータの設定」（P.8） • 「TCP パフォーマンス パラメータの確認」（P.11） • 「例：TCP ECN の設定の確認」（P.16） **debug ip tcp ecn**、**ip tcp ecn**、**show debugging**、**show tcp** の各コマンドがこの機能により導入または変更されました。
TCP MIB for RFC 4022 サポート	Cisco IOS XE 3.1.0 SG 12.2(33)XN	TCP MIB for RFC 4022 サポート機能で、RFC 4022「*Management Information Base for the Transmission Control Protocol (TCP)*」に対するサポートが導入されました。RFC 4022 は、TCP の管理容易性を向上させるための TCP MIB の増分変更です。 この機能により、新規追加または変更されたコマンドはありません。
TCP MSS 調整	12.2(4)T 12.2(8)T 12.2(18)ZU2 12.2(28)SB 12.2(33)SRA 12.2(33)SXH 15.0(1)S	TCP MSS 調整機能では、ルータを通過する一時的なパケット（特に SYN ビットが設定された TCP セグメント）の Maximum Segment Size（MSS; 最大セグメント サイズ）を設定することができるようになります。 この機能は、12.2(4)T で初めて導入されました。 この機能により導入されたコマンドが、12.2(8)T で **ip adjust-mss** から **ip tcp adjust-mss** に変更されました。 12.2(28)SB および 12.2(33)SRA で、この機能がサブ インターフェイスで設定できるように強化されました。 この機能に関する詳細については、次の各項を参照してください。 • 「TCP MSS 調整」（P.6） • 「一時的な TCP SYN パケットに対する MSS 値、および MTU の設定」（P.10） • 「例：TCP MSS 調整の設定」（P.18） コマンド **ip tcp adjust-mss** がこの機能により導入されました。

表 1　TCP の機能情報 （続き）

機能名	リリース	機能情報
TCP Show 拡張	Cisco IOS XE 3.1.0 SG 12.4(2)T 12.2(31)SB2	TCP Show 拡張機能では、ホスト名形式ではなく、IP 形式でアドレスを表示したり、接続に関連付けられた VRF テーブルを表示したりする機能が導入されています。 次の項では、この機能に関する情報について説明します。 • 「TCP Show 拡張」（P.7） • 「TCP パフォーマンス パラメータの確認」（P.11） • 「例：IP 形式でのアドレスの表示」（P.19） コマンド **show tcp brief** がこの機能により変更されました。
TCP ウィンドウ スケーリング	12.2(8)T 12.2(31)SB2	TCP ウィンドウ スケーリング機能は、RFC 1323 のウィンドウ スケーリング オプションのサポートを追加しました。Long Fat Network（LFN; 広帯域高遅延ネットワーク）と呼ばれる広帯域で高遅延の特性を持つネットワーク経路での TCP のパフォーマンスを改善するため、より大きなウィンドウ サイズが推奨されます。TCP ウィンドウ スケーリングの強化で、そのサポートを提供します。 この機能に関する詳細については、次の各項を参照してください。 • 「TCP ウィンドウ スケーリング」（P.5） • 「TCP パフォーマンス パラメータの設定」（P.8） • 「TCP パフォーマンス パラメータの確認」（P.11） **ip broadcast-address** コマンドがこの機能で導入または変更されました。

用語集

LFN：Long Fat Network（広帯域高遅延ネットワーク）。高スループットで伝送距離が長い場合のネットワークで、帯域が広く遅延が大きいもの。衛星中継のネットワークは LFN の一例です。衛星リンクは伝播遅延が大きく、通常広い帯域幅を持ちます。

TCP：Transmission Control Protocol（伝送制御プロトコル）。信頼性のある全二重方式データ転送を提供するコネクション型のトランスポート レイヤ プロトコル。TCP は TCP/IP プロトコル スタックの一部です。

WCCP の設定

Web Cache Communication Protocol（WCCP）はシスコが開発したコンテンツルーティング テクノロジーです。IP パケットを代行受信し、IP パケットに指定されている宛先とは別の宛先にそのパケットをリダイレクトします。パケットは、インターネット上にある宛先の Web サーバから、クライアントのローカルのコンテンツ エンジンにリダイレクトされるのが一般的です。WCCP の展開シナリオによっては、Web サーバからクライアント方向でもトラフィックをリダイレクトする必要があります。WCCP を使用すると、コンテンツ エンジンをネットワーク インフラストラクチャに統合できます。

Cisco IOS Release 12.1 以降では、WCCP version 1（WCCPv1）または version 2（WCCPv2）を使用できます。

このマニュアルの作業では、ネットワークにコンテンツ エンジンが設定済みであることを前提にしています。Cisco Content Engine および WCCP に関連するハードウェアおよびネットワークの計画の詳細については、次の URL にある Cisco Content Engine のマニュアルを参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/webscale/content/index.htm

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、「WCCP の機能情報」（P.29）を参照してください。

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

この章の構成

WCCP の前提条件

- WCCP を使用するには、インターネットに接続しているインターフェイスに IP を設定し、別のインターフェイスをコンテンツ エンジンに接続する必要があります。
- コンテンツ エンジンに接続するインターフェイスは、ファスト イーサネット インターフェイスまたはギガビット イーサネット インターフェイスにする必要があります。

WCCP に関する制約事項

一般

次の制約事項が WCCPv1 および WCCPv2 に適用されます。

- WCCP は、IPv4 ネットワークの場合だけ機能します。

WCCPv1

次の制約事項が WCCPv1 に適用されます。

- WCCPv1 は HTTP（TCP ポート 80）トラフィックのリダイレクションだけをサポートします。
- WCCPv1 では、複数のルータをコンテンツ エンジンのクラスタに接続できません。

WCCPv2

次の制約事項が WCCPv2 に適用されます。

- WCCP は、IPv4 ネットワークの場合だけ機能します。
- マルチキャスト クラスタにサービスを提供するルータの場合、Time To Live（TTL; 存続可能時間）値を 15 以下に設定する必要があります。
- サービス グループは、最大 32 個のコンテンツ エンジンおよび 32 個のルータで構成できます。
- クラスタのすべてのコンテンツ エンジンは、クラスタにサービスを提供するすべてのルータと通信できるように設定する必要があります。
- マルチキャスト アドレスは 224.0.0.0 ～ 239.255.255.255 の範囲にする必要があります。

WCCP VRF のサポート

Cisco IOS Release 12.2(33)SRE では、この機能が Cisco 7200 NPE-G2 ルータと Cisco 7304-NPE-G100 ルータ上でのみサポートされます。

レイヤ 2 フォワーディングおよび返送

次の制約事項が WCCP および WCCP レイヤ 2 フォワーディングおよび返送に適用されます。

- レイヤ 2 リダイレクションの場合、各 WCCP ルータ上のインターフェイスにコンテンツ エンジンを直接接続する必要があります。マルチキャスト IP アドレスを使用しない場合、コンテンツ エンジンの WCCP 設定は、WCCP ルータの直接接続されているインターフェイスの IP アドレスを常に参照します。WCCP ルータに設定されているループバック IP アドレスまたは他の IP アドレスは参照されません。

Cisco ASR 1000 シリーズ集約サービス ルータ

- Cisco ASR 1000 シリーズ集約サービス ルータは、WCCPv1 をサポートしません。
- 通過パケットは、6-Rack-Unit（6RU）と 13RU シャーシ上で Forwarding Processor（FP）フェールオーバーが発生したときに失われます。
- クラスタのすべてのコンテンツ エンジンは、クラスタにサービスを提供するすべてのルータと通信できるように設定する必要があります。
- WCCP サービスのロード バランシング方式としてのハッシュ割り当ては、サポートされません。Cisco IOS XE Release 3.1S 以降では、HASH 割り当てを送信するクライアントがルータによってオンラインになることはできません。Cisco ASR 1000 ルータ上で **show ip wccp 61 detail** コマンドを発行すると、Hash が互換性のない割り当て手段であることが表示されます。
- **show ip wccp** コマンドを使用すると、ソフトウェアベース（プロセス、ファスト、およびシスコ エクスプレス フォワーディング（CEF））の WCCP パケットの転送に関する情報が表示されます。Cisco ASR 1000 は、CEF またはプロセススイッチング パスではなく、ハードウェア内に WCCP が実装されています。そのため、**show ip wccp** コマンドを入力すると、パケット カウントは 0 になります。**show platform software wccp interface counters** コマンドまたは **show platform software wccp counters** コマンドを使用して、Cisco ASR 1000 上の WCCP に関するグローバル統計情報を表示します。

  Cisco IOS-XE Release 3.1S で **show ip wccp** コマンドを発行すると、リダイレクトされた WCCP パケットが表示されます。
- 発信インターフェイス上での WCCP パケットのリダイレクトは、XE Release 3.1S よりも前の XE リリースでサポートされていません。

Cisco Catalyst 4500 シリーズ スイッチ

次の制約事項が Cisco Catalyst 4500 シリーズ スイッチに適用されます。

- Catalyst 4500 シリーズ スイッチは WCCPv1 をサポートしません。
- 同じクライアント インターフェイスで同時に最大 8 個のサービス グループがサポートされます。
- レイヤ 2（L2）のリライト フォワーディング方式はサポートされますが、Generic Route Encapsulation（GRE）はサポートされません。
- コンテンツ エンジンにレイヤ 2（L2）を直接接続する必要があります。1 つまたは複数ホップ離れたレイヤ 3（L3）接続はサポートされません。
- Ternary Content Addressable Memory（TCAM; Ternary CAM）フレンドリ マスクベースの割り当てはサポートされますが、ハッシュ バケットベースの方式はサポートされません。
- クライアント インターフェイス上の WCCP に関するリダイレクト Access Control List（ACL; アクセス コントロール リスト）はサポートされません。
- インターフェイス上の受信トラフィックのリダイレクションはサポートされますが、発信トラフィックのリダイレクションはサポートされません。
- TCAM の空きがなくなると、トラフィックはリダイレクトされず、通常どおりに転送されます。
- WCCP バージョン 2 規格では、最大 256 個のマスクをサポートします。ただし、Catalyst 4500 シリーズ スイッチは、単一のマスクへのマスク割り当てテーブルだけをサポートします。

Cisco Catalyst 6500 シリーズ スイッチ

次の制約事項が Cisco Catalyst 6500 シリーズ スイッチに適用されます。

- Policy Feature Card 2（PFC2; ポリシー フィーチャ カード 2）が搭載されているため、リリース 12.2(17d)SXB 以降のリリースは WCCP をサポートします。
- PFC3 が搭載されているため、リリース 12.2(18)SXD1 以降のリリースは WCCP をサポートします。

- WCCP レイヤ 2 PFC リダイレクション機能を使用するには、この章の説明に従って Catalyst 6500 シリーズ スイッチ で WCCP を設定します。また、次の URL で参照できる「*Transparent Caching*」に従って、キャッシュ エンジンで加速 WCCP を設定します。

  http://www.cisco.com/en/US/docs/app_ntwk_services/waas/acns/v42/configuration/guide/transprt.html

- Cisco Application and Content Networking System（ACNS）ソフトウェア リリース 4.2.2 よりも後のリリースは、WCCP レイヤ 2 ポリシー フィーチャ カード（PFC）のリダイレクション ハードウェア アクセラレーションをサポートします。
- マスク割り当てに設定されているコンテンツ エンジンが、割り当て方式としてハッシュが選択されているファームに参加しようとする場合、キャッシュ エンジンの割り当て方式が既存のファームの方式と一致しない限り、ファームに参加できません。
- サービス グループのフォワーディング方式として WCCP レイヤ 2 PFC リダイレクションを使用する場合、**show ip wccp** *service-number* コマンド出力のパケット カウンタには、パケット カウントではなく、フロー カウントが表示されます。

Catalyst 6500 シリーズ スイッチおよび Cisco 7600 シリーズ ルータのアクセス コントロール リスト

WCCP がマスク割り当てを使用している場合、リダイレクト リストはアプライアンスのマスク情報に結合され、結果の結合されたアクセス コントロール リスト（ACL）は、Catalyst 6500 シリーズ スイッチまたは Cisco 7600 シリーズ ルータ ハードウェアに渡されます。

次の制約事項がリダイレクト リスト ACL に適用されます。

- ACL は IPV4 簡易または拡張 ACL にする必要があります。
- プロトコルは、IP、UDP、または TCP にする必要があります。
- 個々の発信元または宛先のポート番号だけを指定できます。ポート範囲は指定できません。
- 個々の発信元または宛先のポート番号のほかに、唯一の有効なマッチング条件は、**dscp** または **tos** です。
- **fragments**、**time-range**、**options**、または TCP フラグは使用できません。

リダイレクト ACL が上記の制約事項を満たさない場合、次のエラー メッセージがログに記録されます。

```
WCCP-3-BADACE: Service <service group>, invalid access-list entry (seq:<sequence>,
reason:<reason>)
```

WCCP はパケットのリダイレクトを継続しますが、アクセス リストが調整されるまで、ソフトウェアでリダイレクションが実行されます（NetFlow スイッチング）。

WCCP の概要

WCCP の概要

WCCP は、Cisco Content Engine（または WCCP を実行する他のコンテンツ エンジン）を使用して、ネットワークの Web トラフィック パターンをローカライズします。それによって、ローカルでコンテンツ要求を実行できます。トラフィックのローカライズによって、送信コストとダウンロード時間が削減されます。

WCCP によって、Cisco IOS ルーティング プラットフォームは、透過的にコンテンツ要求をリダイレクトできるようになります。透過的リダイレクションの主な利点は、Web プロキシを使用するためにユーザがブラウザを設定する必要がないことです。ユーザはターゲット URL を使用してコンテンツを要求できます。また、ユーザの要求はコンテンツ エンジンに自動的にリダイレクトされます。この場合の「透過的」とは、エンド ユーザが要求したファイル（Web ページなど）が、元々指定していたサーバからではなく、コンテンツ エンジンから送信されることをそのユーザが意識しないという意味です。

コンテンツ エンジンでは、要求の受信時に、独自のローカル キャッシュからサービスを提供しようとします。要求した情報が存在しない場合、コンテンツ エンジンから独自の要求が元のターゲット サーバに発行され、必要な情報が取得されます。コンテンツ エンジンは、要求された情報を取得すると、要求クライアントに転送し、以降の要求に対応するためにキャッシュします。そのため、ダウンロードのパフォーマンスが大きく向上し、送信コストが大幅に削減されます。

WCCP によって、コンテンツ エンジン クラスタと呼ばれる一連のコンテンツ エンジンは、1 つまたは複数のルータにコンテンツを提供できるようになります。ネットワーク管理者は、このようなクラスタ処理機能によって容易にコンテンツ エンジンを拡張し、高いトラフィック負荷を管理できます。シスコ クラスタ処理テクノロジーを使用すると、各クラスタ メンバを同時に実行できるため、リニア スケーラビリティが実現します。クラスタ処理コンテンツ エンジンによって、キャッシュ ソリューションのスケーラビリティ、冗長性、および可用性が大幅に改善されます。最大 32 個のコンテンツ エンジンをクラスタ処理し、目的の容量まで拡張できます。

レイヤ 2 フォワーディング、リダイレクション、および返送

WCCP は、Generic Routing Encapsulation（GRE）またはレイヤ 2（L2）を使用して、IP トラフィックをリダイレクトまたは返送します。WCCP が GRE を介してトラフィックを転送すると、リダイレクトされたパケットは GRE ヘッダー内でカプセル化されます。また、このパケットには WCCP リダイレクト ヘッダーも含まれます。WCCP が L2 を使用してトラフィックを転送すると、IP パケットの元の MAC ヘッダーは上書きされ、WCCP クライアントの MAC ヘッダーで置換されます。

フォワーディング方式として L2 を使用すると、以降の検索を行わずに、コンテンツ エンジンに直接転送できます。レイヤ 2 リダイレクションには、ルータおよびコンテンツ エンジンが直接接続されている（つまり同じ IP サブネット上にある）必要があります。

WCCP が GRE を介してトラフィックを返送すると、返送されたパケットは GRE ヘッダー内でカプセル化されます。宛先 IP アドレスはルータのアドレスで、発信元アドレスは WCCP クライアントのアドレスです。WCCP が L2 を介してトラフィックを返送すると、元の IP パケットは、ヘッダー情報を追加せずに返送されます。パケットの返送先ルータは、パケットの発信元を認識し、リダイレクションを回避します。

WCCP リダイレクション方式は、返送方式と一致する必要はありません。

L2 フォワーディング、返送、またはリダイレクションは、一般的にハードウェア アクセラレーション プラットフォームに使用します。Cisco IOS Release 12.4(20)T 以降のリリースでは、L2 フォワーディング、返送、およびリダイレクトをソフトウェア スイッチング プラットフォームにも使用できます。

Cisco ASR 1000 シリーズ集約サービス ルータでは、GRE および L2 両方のフォワーディング / 返送方式にハードウェアが使用されるため、大幅なパフォーマンスの低下はありません。

Application and Content Networking System（ACNS）ソフトウェアを実行するコンテンツ エンジンの場合、**l2-redirect** キーワードを指定した **wccp custom-web-cache** コマンドを使用して、L2 リダイレクションを設定します。Cisco Wide Area Application Services（WAAS）ソフトウェアを実行するコンテンツ エンジンの場合、**l2-redirect** キーワードを指定した **wccp tcp-promiscuous** コマンドを使用して、L2 リダイレクションを設定します。

Cisco Content Engine の設定に使用する Cisco ACNS コマンドの詳細については、次の URL の『*Cisco ACNS Software Command Reference*, Release 5.5.13』を参照してください。

http://www.cisco.com/en/US/docs/app_ntwk_services/waas/acns/v55_13/command/reference/5513cref.html

Cisco Content Engine の設定に使用する WAAS コマンドの詳細については、次の URL の『*Cisco Wide Area Application Services Command Reference (Software Versions 4.2.1)*』を参照してください。

http://www.cisco.com/en/US/docs/app_ntwk_services/waas/waas/v421/command/reference/cmdref.html

WCCP マスク割り当て

WCCP マスク割り当て機能によって、（デフォルトのハッシュ割り当て方式ではなく）WCCP サービスのロード バランシング方式としてマスク割り当てを使用できます。

Application and Content Networking System（ACNS）ソフトウェアを実行するコンテンツ エンジンの場合、**mask-assign** キーワードを指定した **wccp custom-web-cache** コマンドを使用して、マスク割り当てを設定します。Cisco Wide Area Application Services（WAAS）ソフトウェアを実行するコンテンツ エンジンの場合、**mask-assign** キーワードを指定した **wccp tcp-promiscuous** コマンドを使用して、マスク割り当てを設定します。

Cisco Content Engine の設定に使用する Cisco ACNS コマンドの詳細については、次の URL の『*Cisco ACNS Software Command Reference*, Release 5.5.13』を参照してください。

http://www.cisco.com/en/US/docs/app_ntwk_services/waas/acns/v55_13/command/reference/5513cref.html

Cisco Content Engine の設定に使用する WAAS コマンドの詳細については、次の URL の『*Cisco Wide Area Application Services Command Reference (Software Versions 4.2.1)*』を参照してください。

http://www.cisco.com/en/US/docs/app_ntwk_services/waas/waas/v421/command/reference/cmdref.html

ハードウェア アクセラレーション

Catalyst 4500 シリーズ スイッチには、直接接続された Cisco Content Engine 用にハードウェア アクセラレーション機能があります。

Catalyst 6500 シリーズ スイッチおよび Cisco 7600 シリーズ ルータには、WCCP レイヤ 2 ポリシー フィーチャ カード（PFC）リダイレクション ハードウェア アクセラレーション機能があります。互換性のあるスイッチまたはルータに直接接続する場合、ハードウェア アクセラレーションを使用すると、Cisco Content Engine では L2 MAC アドレスのリライト リダイレクション方式を実行できます。

スイッチングまたはルーティング ハードウェアの場合、リダイレクション プロセスは加速されます。これは、Generic Routing Encapsulation（GRE）を使用した L3 リダイレクションよりも効率的です。L2 リダイレクションはスイッチまたはルータで実行され、マルチレイヤ スイッチ フィーチャ カード（MSFC）からは不可視です。WCCP L2 PFC リダイレクション機能には、MSFC での設定は必要ありません。**show ip wccp** {*service-number* | **web-cache**} **detail** コマンドを使用すると、各コンテンツ エンジンで現在使用されているリダイレクション方式が表示されます。

ルータまたはスイッチでハードウェア リダイレクションを最大限に活用するためには、「レイヤ 2 フォワーディング、リダイレクション、および返送」（P.5）を参照して、L2 リダイレクションおよびマスク割り当てを使用してコンテンツ エンジンを設定する必要があります。

L2 リダイレクションおよびマスク割り当てを強制するには、ハードウェアベースのプラットフォームで **ip wccp web-cache accelerated** コマンドを使用します。このコマンドを使用すると、アプライアンスが L2 およびマスク割り当て用に設定されている場合にだけ、サービス グループを構成し、パケットをリダイレクトするようにルータが設定されます。

次の注意事項が WCCP レイヤ 2 PFC リダイレクションに適用されます。

- WCCP レイヤ 2 PFC リダイレクション機能によって、IP フロー マスクは full-flow モードに設定されます。
- Cisco Cache Engine ソフトウェア リリース 2.2 以降のリリースを設定して、WCCP レイヤ 2 PFC リダイレクション機能を使用できます。
- L2 リダイレクションは PFC で実行され、MSFC からは不可視です。MSFC で **show ip wccp** {*service-number* | **web-cache**} **detail** コマンドを使用すると、L2 リダイレクト フローの最初のパケットだけに関する統計情報が表示されます。この情報から、L2 リダイレクションを使用しているフロー数（パケット数ではない）がわかります。**show mls entries** コマンドを入力すると、L2 リダイレクト フローの他のパケットが表示されます。PFC3 には、GRE 用のハードウェア アクセラレーション機能があります。GRE とともに WCCP レイヤ 3 リダイレクションを使用する場合、カプセル化にはハードウェア サポートがありますが、PFC3 での、WCCP GRE トラフィックの非カプセル化にはハードウェア サポートがありません。

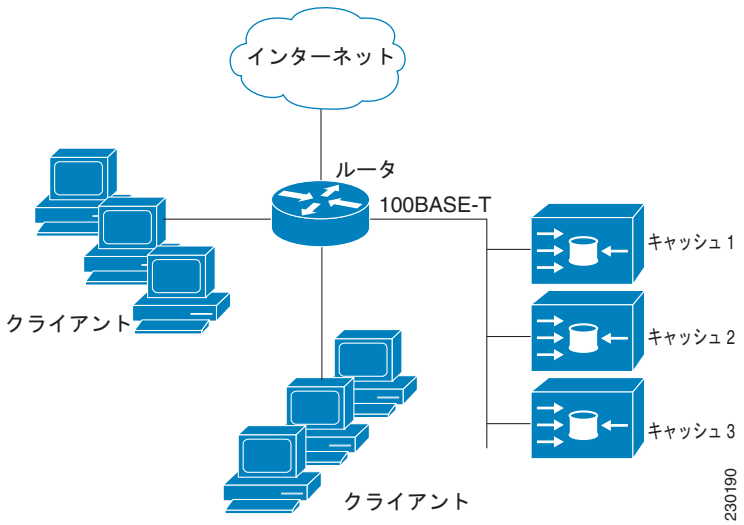
Cisco ASR 1000 シリーズ集約サービス ルータ

Cisco ASR 1000 シリーズ集約サービス ルータの WCCP 実装は、デフォルトでハードウェア アクセラレーションです。ハードウェア アクセラレーションをイネーブルにするために、Cisco ASR ルータで **ip wccp web-cache accelerated** コマンドを設定する必要はありません。

WCCPv1 の設定

WCCPv1 の場合、1 つのクラスタにサービスを提供できるのは 1 つのルータだけです。このシナリオでは、このルータがすべての IP パケット リダイレクションを実行するデバイスです。図 1 に、WCCPv1 の設定を示します。

図 1　　WCCPv1 の設定



コンテンツ エンジンで、コンテンツは重複しません。コンテンツ エンジンを複数使用する利点は、複数の物理コンテンツ エンジンをクラスタ処理して 1 つの論理キャッシュのように見せることで、キャッシング ソリューションを拡張できることです。

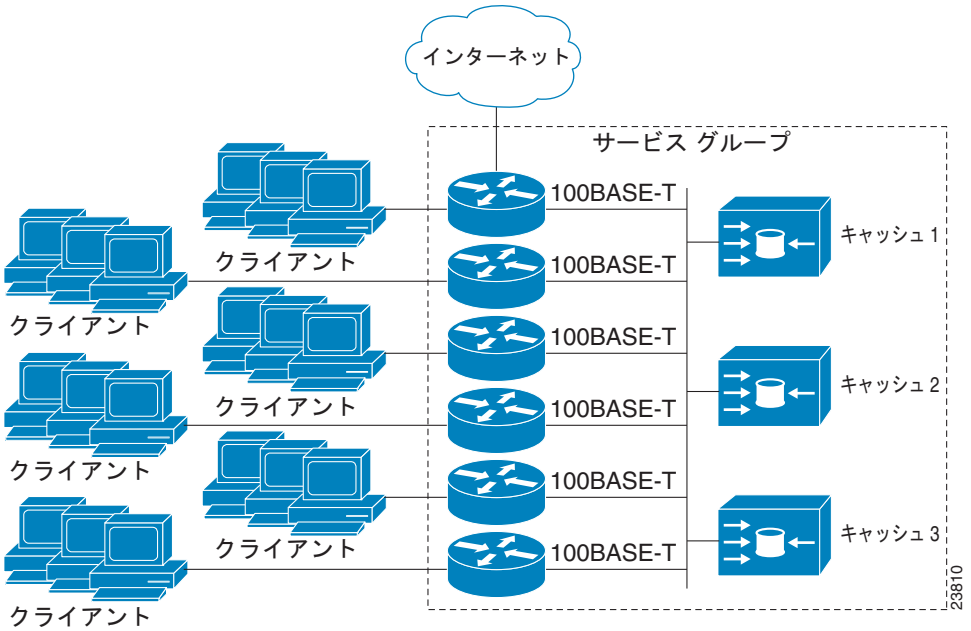
次の一連のイベントで、WCCPv1 設定の動作の詳細について説明します。

1. 各コンテンツ エンジンは、制御ルータの IP アドレスを使用してシステム管理者が設定します。最大 32 個のコンテンツ エンジンを単一の制御ルータに接続できます。
2. コンテンツ エンジンは、WCCP を使用して自身の IP アドレスを制御ルータに送信して、プレゼンスを示します。ルータおよびコンテンツ エンジンは、制御チャネルを介して相互に通信します。このチャネルは、UDP ポート 2048 に基づいています。
3. この情報は、制御ルータがクラスタ ビュー（クラスタ内のキャッシュ リスト）を作成するときに使用されます。このビューはクラスタ内の各コンテンツ エンジンに送信され、基本的にすべてのコンテンツ エンジンが相互を認識するようになります。クラスタのメンバシップが変化せずに一定の時間が経過すると、安定したビューが確立します。
4. 安定したビューが確立すると、リード コンテンツ エンジンとして 1 つのコンテンツ エンジンが選択されます（リードとは、IP アドレスが最も低いクラスタですべてのコンテンツ エンジンから見えるコンテンツ エンジンのことです）。このリード コンテンツ エンジンでは、WCCP を使用して、IP パケット リダイレクションの実行方法を制御ルータに示します。具体的には、リード コンテンツ エンジンは、リダイレクトされるトラフィックをクラスタのコンテンツ エンジン全体に分散する方法を指定します。

WCCPv2 の設定

複数のルータが WCCPv2 を使用して 1 つのコンテンツ エンジン クラスタにサービスを提供できます。この設定は WCCPv1 と対照的です。WCCPv1 では、1 つのルータだけがコンテンツ要求をクラスタにリダイレクトできます。図 2 に、複数のルータを使用する設定例を示します。

図 2　　WCCPv2 を使用する Cisco Cache Engine のネットワーク設定



クラスタ、および同じサービスを実行しているクラスタに接続するルータ内のコンテンツ エンジンのサブセットは、*サービス グループ*と呼ばれます。使用できるサービスには、TCP および User Datagram Protocol（UDP; ユーザ データグラム プロトコル）リダイレクションなどがあります。

WCCPv1 では、単一ルータのアドレスを使用して、コンテンツ エンジンが設定されました。WCCPv2 の場合、各コンテンツ エンジンがサービス グループ内のすべてのルータを認識する必要があります。サービス グループ内のすべてのルータのアドレスを指定するには、次のいずれかの方式を選択できます。

- ユニキャスト：グループ内の各ルータのルータ アドレス リストを、各コンテンツ エンジンで設定します。この場合、グループ内の各ルータのアドレスは、設定時に各コンテンツ エンジンについて明示的に指定する必要があります。
- マルチキャスト：単一のマルチキャスト アドレスを各コンテンツ エンジンで設定します。マルチキャスト アドレス方式の場合、コンテンツ エンジンは、サービス グループのすべてのルータに提供するシングル アドレス通知を送信します。たとえば、コンテンツ エンジンは、パケットを常にマルチキャスト アドレス 224.0.0.100 に送信するように示すことができます。それによって、マルチキャスト パケットは、WCCP を使用してリスンしているグループ用に設定されたサービス グループ内のすべてのルータに送信されます（詳細については、**ip wccp group-listen** インターフェイス コンフィギュレーション コマンドを参照してください）。

マルチキャスト オプションの場合に必要な操作は、各コンテンツ エンジンで単一のアドレスを指定することだけなので、設定が容易です。このオプションを使用して、サービス グループからルータを動的に追加および削除できます。毎回、異なるアドレス リストを使用してコンテンツ エンジンを再設定する必要はありません。

次の一連のイベントで、WCCPv2 設定の動作の詳細について説明します。

1. 各コンテンツ エンジンは、ルータ リストを使用して設定します。
2. 各コンテンツ エンジンはプレゼンスと、通信の確立に使用されたすべてのルータ リストをアナウンスします。ルータは、グループ内のコンテンツ エンジンのビュー（リスト）で応答します。
3. そのビューがクラスタ内のすべてのコンテンツ エンジンで一貫している場合、1 つのコンテンツ エンジンをリードとして指定し、ルータがパケットのリダイレクト時に展開する必要があるポリシーを設定します。

HTTP 以外のサービスのサポート

WCCPv2 では、多様な UDP および TCP トラフィックなど、HTTP（TCP ポート 80 トラフィック）以外のトラフィックをリダイレクトできます。WCCPv1 は HTTP（TCP ポート 80）トラフィックのリダイレクションだけをサポートしていました。WCCPv2 では他のポート宛てのパケットをリダイレクトできます。たとえば、プロキシ Web キャッシュ処理、File Transfer Protocol（FTP; ファイル転送プロトコル）キャッシング、FTP プロキシの処理、80 以外のポートの Web キャッシング、Real Audio、ビデオ アプリケーション、およびテレフォニー アプリケーションに使用されるポートなどです。

使用可能な多様な種類のサービスに対応するために、WCCPv2 は複数の *サービス グループ*という概念を導入しました。サービス情報は、ダイナミック サービス識別番号（98 など）または事前定義したサービス キーワード（**web-cache** など）を使用して、WCCP コンフィギュレーション コマンドで指定します。この情報は、サービス グループ メンバがすべて同じサービスを使用または提供していることを確認するために使用されます。

サービス グループのコンテンツ エンジンは、プロトコル（TCP または UDP）によってリダイレクトされるトラフィックと、最大 8 個の発信元ポートまたは宛先ポートを指定します。各サービス グループには、プライオリティ ステータスが割り当てられています。ダイナミック サービスのプライオリティは、コンテンツ エンジンによって割り当てられます。プライオリティ値の範囲は、0 ～ 255 です（0 が最も低いプライオリティ）。事前定義した Web キャッシュ サービスには、240 のプライオリティが割り当てられています。

複数ルータのサポート

WCCPv2 では、複数のルータをキャッシュ エンジンのクラスタに接続できます。1 つのサービス グループでルータを複数使用すると、冗長化、インターフェイスの集約、リダイレクション負荷の分散ができます。WCCPv2 は、サービス グループごとに最大 32 個のルータをサポートします。各サービス グループの確立および保守は独立して行われます。

MD5 セキュリティ

WCCPv2 には、パスワードと HMAC MD5 規格を使用して、サービス グループの一部になるルータとコンテンツ エンジンを制御できる、オプションの認証機能があります。共有シークレット MD5 ワンタイム認証（**ip wccp** [**password** [**0** | **7**] *password*] グローバル コンフィギュレーション コマンドを使用して設定）を使用すれば、傍受、検査、およびリプレイからメッセージを保護することができます。

Web キャッシュ パケット返送

コンテンツ エンジンが、エラーまたは過負荷のために、キャッシュした要求オブジェクトを提供できない場合、コンテンツ エンジンは、元々指定されていた宛先サーバに前方転送するように、要求をルータに返送します。WCCPv2 には、機能していないコンテンツ エンジンから返送された要求を判断できるパケットのチェック機能があります。ルータはこの情報を使用して、（要求をコンテンツ エンジン クラスタに再送信しようとするのではなく）要求を元の宛先サーバに転送できます。このプロセスのエラー処理はクライアントに意識されません。

コンテンツ エンジンがパケットを拒否し、パケット返送機能を開始する場合、一般的に次のような理由があります。

- コンテンツ エンジンが過負荷になり、パケットを処理する余裕がなくなった場合
- コンテンツ エンジンが、パケットのキャッシング機能が低下する特定の条件についてフィルタリングしている場合（たとえば、IP 認証が有効になった場合）

負荷分散

WCCPv2 を使用すると、個々のコンテンツ エンジンに割り当てる負荷を調整して、空きリソースを効率的に使用できるようになります。さらに、クライアントに対して高い Quality Of Service（QoS）を確保できます。WCCPv2 を使用すると、指定したコンテンツ エンジンが特定のコンテンツ エンジン上の負荷を調整し、クラスタ内のコンテンツ エンジン全体で負荷を分散できます。WCCPv2 では、負荷分散を実行するために次の 3 つの技術を使用しています。

- ホット スポット処理：個々のハッシュ バケットをすべてのコンテンツ エンジンに分散できます。WCCPv2 よりも前のリリースでは、1 つのハッシュ バケットの情報を転送できるのは、1 つのコンテンツ エンジンに対してだけでした。
- ロード バランシング：過負荷のコンテンツ エンジンから、空き容量がある他のメンバに負荷を移行するように、コンテンツ エンジンに割り当てるハッシュ バケット セットを調整できます。
- 負荷制限：コンテンツ エンジンの容量を超えないように、ルータが負荷を選択してリダイレクトできるようにします。

これらのハッシュ処理パラメータを使用すると、コンテンツ エンジンの過負荷を防ぎ、障害が発生する可能性を軽減します。

WCCP VRF のサポート

WCCP VRF サポート機能は、Virtual Routing and Forwarding（VRF）のサポートを実装することで、既存の WCCPv2 プロトコルを強化します。

WCCP VRF サポート機能を使用すると、グローバル定義に加え、VRF ベースでサービス グループを設定できます。

サービス ID の他に、ルータに到着する WCCP プロトコル パケットの VRF が、設定されたサービス グループにキャッシュ エンジンを関連付けるために使用されます。

リダイレクトが適用されたインターフェイス、キャッシュ エンジンに接続されたインターフェイス、およびリダイレクトされなかったパケットが残されるインターフェイスを 1 つの VRF に含める必要があります。

Cisco IOS Release 12.2(33)SRE では、この機能が Cisco 7200 NPE-G2 ルータと Cisco 7304-NPE-G100 ルータ上でのみサポートされます。

WCCP バイパス パケット

WCCP は IP パケットを代行受信し、IP ヘッダーに指定されている宛先以外の宛先に、そのパケットをリダイレクトします。パケットは、インターネット上にある Web サーバから、宛先のローカルの Web キャッシュにリダイレクトされるのが一般的です。

場合によっては、Web キャッシュでリダイレクトされたパケットを適切に管理できず、パケットを変更せずに元のルータに返送することがあります。このようなパケットはバイパス パケットと呼ばれ、カプセル化なしのレイヤ 2 フォワーディング（L2）を使用して、または Generic Routing Encapsulation（GRE）でカプセル化して、発信元のルータに返送されます。ルータはカプセル化を解除し、通常どおり、パケットを転送します。入力インターフェイスと関連付けられている VRF（関連付けられている VRF がない場合はグローバル テーブル）は、パケットを宛先にルーティングするときに使用されます。

GRE はシスコが開発したトンネリング プロトコルで、IP トンネル内部でさまざまなプロトコルから派生したパケット タイプをカプセル化して、IP ネットワーク上に仮想ポイントツーポイント リンクを構築します。

WCCP クローズド サービスおよびオープン サービス

パケット フローを代行受信し、Cisco IOS ルータによって外部 WCCP クライアント デバイスにリダイレクトするアプリケーションの場合、WCCP クライアント デバイスを使用できないと、状況によってはアプリケーションのパケット フローをブロックする必要があります。このブロックを実行するには、WCCP クローズド サービスを設定します。WCCP サービスをクローズドに設定すると、WCCP では登録されている WCCP クライアントがないパケットが破棄され、リダイレクトされたトラフィックが受信されます。

デフォルトでは、WCCP はオープン サービスとして動作します。この場合、中間デバイスがなくても、クライアントとサーバ間の通信は正常に進行します。

ip wccp service-list コマンドを使用できるのは、クローズド モード サービスの場合だけです。アプリケーション プロトコルの種類またはポート番号を登録するには、**service-list** キーワードおよび *service-access-list* 引数を使用します。

サービスリスト ACL と、キャッシュ エンジンから受信された定義が一致しなかった場合は、サービスを開始できません。

WCCP 発信 ACL チェック

WCCP は IP パケットを代行受信し、IP ヘッダーに指定されている宛先以外の宛先に、そのパケットをリダイレクトします。パケットは、インターネット上にある Web サーバから、リダイレクト ルータのローカルの Web キャッシュにリダイレクトされるのが一般的です。

アクセス コントロール リスト（ACL）は、ルーティング処理したパケットを転送するか、ルータ インターフェイスでブロックするかを制御して、ネットワーク トラフィックをフィルタ処理します。各パケットは確認され、ACL に指定されている基準に従って、転送するかドロップするかが判断されます。ACL の条件には、トラフィックの発信元アドレス、トラフィックの宛先アドレス、または上位レイヤのプロトコルを指定できます。IP ACL は、IP アドレスに適用する許可条件と拒否条件の一連のコレクションです。ルータは、同時に 1 つずつ、ACL の条件に対してアドレスをテストします。最初の一致によって、そのアドレスを受け入れるか拒否するかが決まります。最初の一致後に Cisco IOS ソフトウェアは条件のテストを停止するため、条件の順序が重要です。一致する条件がない場合、暗黙的な「deny all」句によって、ルータはそのアドレスを拒否します。

リダイレクションが実行されるインターフェイスに、発信 ACL が設定されている場合、状況によっては、トラフィックのリダイレクト先ホストが宛先へのアクセス権を取得します（アクセス権がなければブロックされる宛先です）。

WCCP 発信 ACL チェック機能によって、発信 ACL チェック処理は元のインターフェイスで実行されるため、チェック処理はセキュアであり、すべてのプラットフォームおよび Cisco IOS スイッチング パスで一貫しています。

WCCP サービス グループ

WCCP は、定義済みの特徴を使用して、元の宛先から代替の宛先へとトラフィックをリダイレクトする Cisco IOS ソフトウェアのコンポーネントです。一般的な WCCP アプリケーションには、リモート Web サーバ宛ての発信トラフィックをローカル Web キャッシュにリダイレクトして、応答時間を改善し、ネットワーク リソースの使用状況を最適化する機能があります。

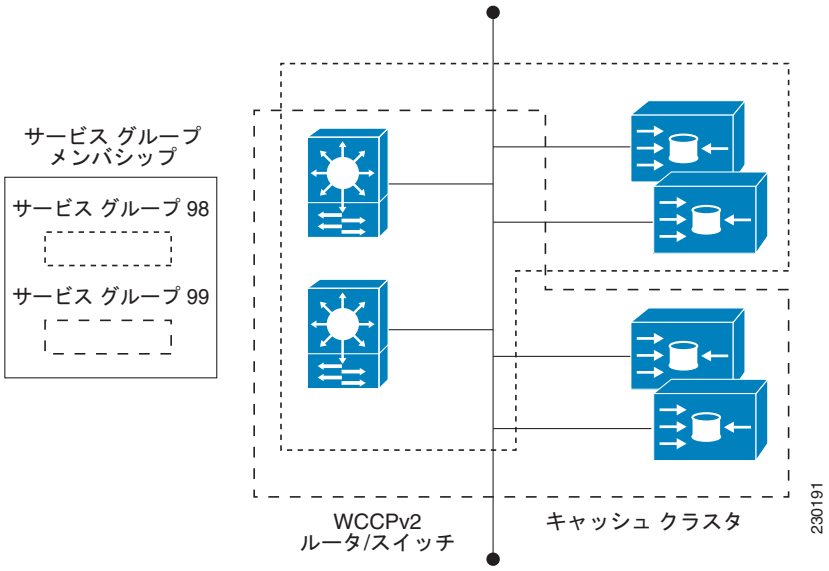
リダイレクションに選択されるトラフィックの性質は、コンテンツ エンジンで指定されるサービス グループによって定義され、WCCP を使用してルータに通信されます。Cisco IOS Release 12.3(14)T よりも前の Cisco IOS リリースに実装されている最新の WCCP では、最大 8 個のサービス グループを定義できました。この最大値によって、キャッシングの展開が制限されていました。Cisco IOS Release 12.3(14)T 以降のリリースで、すべての VRF で使用できるサービス グループの最大数が 256 に増えました。

WCCPv2 は、サービス グループごとに最大 32 個のルータをサポートします。各サービス グループの確立および保守は独立して行われます。

トラフィックの代行受信およびリダイレクトのために展開されている論理リダイレクション サービスに基づいて、WCCPv2 はサービス グループを使用します。標準のサービスは Web キャッシュです。Web キャッシュは TCP ポート 80（HTTP）トラフィックを代行受信し、そのトラフィックをコンテンツ エンジンにリダイレクトします。このサービスは、Web キャッシュ サービスの特徴はルータとコンテンツ エンジンの両方から認識されているため、*既知のサービス*と呼ばれます。サービスの識別よりも詳細な既知のサービスの説明は必要ありません。標準の Web キャッシュ サービスを指定するには、**web-cache** キーワードを指定して **ip wccp** コマンドを使用します。

（注） 1 つのルータで同時に複数のサービスを実行できます。また、ルータおよびコンテンツ エンジンは、同時に複数のサービス グループに参加できます。

図 3　　WCCP サービス グループ



ダイナミック サービスは、コンテンツ エンジンによって定義されます。コンテンツ エンジンは、代行受信するプロトコルまたはポート、およびトラフィックの分散方法をルータに指示します。ダイナミック サービス グループのトラフィックの特徴に関する情報は、ルータ自体にはありません。この情報は、グループに参加する最初のコンテンツ エンジンから提供されるためです。ダイナミック サービスでは、単一のプロトコルに最大 8 個のポートを指定できます。

たとえば、Cisco Content Engine ではダイナミック サービス 99 を使用して、リバース プロキシ サービスを指定します。ただし、他のコンテンツ エンジン デバイスでは、その他のサービスにこのサービス番号を使用する可能性があります。このマニュアルの構成情報では、Cisco ルータで一般的なサービスをイネーブルにする方法について説明しています。

WCCP：Check Services All

インターフェイスは、WCCP サービスを複数使用して設定できます。1 つのインターフェイスに複数の WCCP サービスを設定する場合、サービスの優先順位は、他の設定済みサービスのプライオリティと比較した、そのサービスの相対的なプライオリティによって変わります。各 WCCP サービスには、定義の一部にプライオリティ値があります。複数の WCCP サービスを使用してインターフェイスを設定する場合、パケットの優先順位は、プライオリティ順でサービス グループに対して対応付けられます。

（注）　WCCP サービス グループのプライオリティは、Cisco IOS ソフトウェアで設定できません。

ip wccp check services all コマンドを使用すると、一致についてすべての設定済みサービスをチェックし、必要に応じてそのサービスについてリダイレクションを実行するように WCCP を設定できます。パケットのリダイレクト先キャッシュは、リダイレクト ACL およびサービスのプライオリティによって制御できます。

WCCP サービスをリダイレクト ACL を使用して設定する場合、IP パケットに一致するサービスが見つかるまで、プライオリティ順にサービスがチェックされます。パケットに一致するサービスがない場合、パケットはリダイレクトされません。サービスがパケットに一致し、サービスにリダイレクト ACL が設定されている場合、IP パケットは ACL に対してチェックされます。ACL によってパケットが拒否される場合、**ip wccp check services all** コマンドを設定していない限り、低いプライオリティのサービスにパケットは渡されません。**ip wccp check services all** コマンドを設定すると、インターフェイスに設定されている残りの低いプライオリティのサービスに対して、引き続きパケットのマッチングが試行されます。

WCCP の設定方法

次の設定作業では、ネットワークで使用するコンテンツ エンジンのインストールと設定が完了していることを前提としています。クラスタでコンテンツ エンジンを設定してから、ルータまたはスイッチの WCCP 機能を設定する必要があります。コンテンツ エンジンの設定とセットアップ作業については、『*Cisco Cache Engine User Guide*』を参照してください。

- 「WCCP の設定」（P.14）（必須）
- 「クローズド サービスの設定」（P.16）（任意）
- 「マルチキャスト アドレスへのルータの登録」（P.17）（任意）
- 「WCCP サービス グループでのアクセス リストの使用」（P.19）（任意）
- 「WCCP 発信 ACL チェックのイネーブル化」（P.20）（任意）
- 「WCCP コンフィギュレーション設定の確認とモニタリング」（P.21）（任意）

WCCP の設定

WCCP を設定するには、次の作業を実行します。

ip wccp {**web-cache** | *service-number*} グローバル コンフィギュレーション コマンドを使用して WCCP サービスを設定するまで、ルータの WCCP はディセーブルです。**ip wccp** 形式のコマンドを初めて使用すると、WCCP がイネーブルになります。デフォルトで、WCCPv2 がサービスに使用されますが、WCCPv1 の機能を使用することもできます。WCCP の実行バージョンをバージョン 2 からバージョン 1 に変更するには、または最初の変更後に WCCPv2 に戻すには、グローバル コンフィギュレーション モードで **ip wccp version** コマンドを使用します。

WCCPv1 で使用できない機能の場合、エラー プロンプトが画面に出力されます。たとえば、WCCPv1 がルータ上で実行され、ダイナミック サービスを設定しようとしている場合、「WCCP V1 only supports the web-cache service」というメッセージが表示されます。**show ip wccp** EXEC コマンドを使用すると、ルータで現在実行されている WCCP プロトコル バージョン番号が表示されます。

ip wccp web-cache password コマンドを使用すると、サービス グループのルータおよびコンテンツ エンジンのパスワードを設定できます。MD5 パスワード セキュリティの場合、サービス グループのパスワードを使用して、サービス グループに参加させる各ルータおよびコンテンツ エンジンを設定する必要があります。パスワードは最大 8 文字で構成できます。サービス グループの各コンテンツ エンジンまたはルータは、WCCP メッセージ ヘッダーの検証後すぐに、受信した WCCP パケットのセキュリティ コンポーネントを認証します。認証に失敗したパケットは破棄されます。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip wccp version** {**1** | **2**}
4. **ip wccp** [**vrf** *vrf-name*] {**web-cache** | *service-number*} [**group-address** *group-address*] [**redirect-list** *access-list*] [**group-list** *access-list*] [**password** *password*]
5. **interface** *type number*
6. **ip wccp** [**vrf** *vrf-name*] {**web-cache** | *service-number*} **redirect** {**out** | **in**}
7. **exit**
8. **interface** *type number*
9. **ip wccp redirect exclude in**

手順の詳細

	コマンド	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip wccp version** {**1** | **2**} 例： `Router(config)# ip wccp version 2`	ルータで設定する WCCP のバージョンを指定します。WCCPv2 がデフォルトの実行バージョンです。
ステップ 4	**ip wccp** [**vrf** *vrf-name*] {**web-cache** | *service-number*} [**group-address** *group-address*] [**redirect-list** *access-list*] [**group-list** *access-list*] [**password** *password* [**0** | **7**]] 例： `Router(config)# ip wccp web-cache password password1`	ルータでイネーブルにする Web キャッシュまたはダイナミック サービスを指定し、サービス グループに関連付ける VRF 名を指定し、サービス グループに使用される IP マルチキャスト アドレスを指定し、使用するアクセス リストを指定し、MD5 認証を使用するかどうかを指定し、WCCP サービスをイネーブルにします。
ステップ 5	**interface** *type number* 例： `Router(config)# interface ethernet0/0`	Web キャッシュ サービスが実行するインターフェイス番号をターゲットにし、インターフェイス コンフィギュレーション モードを開始します。
ステップ 6	**ip wccp** [**vrf** *vrf-name*] {**web-cache** | *service-number*} **redirect** {**out** | **in**} 例： `Router(config-if)# ip wccp web-cache redirect in`	WCCP を使用して、発信インターフェイスまたは受信インターフェイスでパケットのリダイレクションをイネーブルにします。 **out** および **in** キーワード オプションの指定に従って、発信インターフェイスまたは受信インターフェイスのリダイレクションを指定できます。
ステップ 7	**exit** 例： `Router(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了します。
ステップ 8	**interface** *type number* 例： `Router(config)# interface GigabitEthernet0/2/0`	リダイレクトからトラフィックを除外するインターフェイス番号を対象として、インターフェイス コンフィギュレーション モードを開始します。
ステップ 9	**ip wccp redirect exclude in** 例： `Router(config-if)# ip wccp redirect exclude in`	（任意）指定したインターフェイスのトラフィックをリダイレクションから除外します。

クローズド サービスの設定

WCCP 用のサービス グループの数を指定し、クローズド サービスまたはオープン サービスとしてサービス グループを設定し、オプションで全サーバのチェックを指定するには、この作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip wccp** [**vrf** *vrf-name*] *service-number* **service-list** *service-access-list* **mode** {**open** | **closed**}

   または

   ip wccp [**vrf** *vrf-name*] **web-cache mode** {**open** | **closed**}
4. **ip wccp check services all**
5. **ip wccp** [**vrf** *vrf-name*] {**web-cache** | *service-number*}
6. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip wccp** [**vrf** *vrf-name*] *service-number* **service-list** *service-access-list* **mode** {**open**	**closed**} または **ip wccp** [**vrf** *vrf-name*] **web-cache mode** {**open**	**closed**} 例： `Router(config)# ip wccp 90 service-list 120 mode closed` または 例： `Router(config)# ip wccp web-cache mode closed`	ダイナミック WCCP サービスをクローズドまたはオープンとして設定します。 または Web キャッシュ サービスをクローズドまたはオープンとして設定します。 **（注）** Web キャッシュ サービスをクローズド サービスとして設定する場合、サービス アクセス リストを指定できません。 **（注）** ダイナミック WCCP サービスをクローズド サービスとして設定する場合、サービス アクセス リストを指定する必要があります。

	コマンドまたはアクション	目的
ステップ 4	**ip wccp check services all** 例： `Router(config)# ip wccp check services all`	（任意）WCCP サービスのチェックをイネーブルにします。 **ip wccp check services all** コマンドを使用すると、一致について他の設定済みサービスをチェックし、必要に応じてそのサービスについてリダイレクションを実行するように WCCP を設定できます。パケットのリダイレクト先キャッシュは、サービス記述だけでなく、リダイレクト ACL によって制御できます。 （注） **ip wccp check services all** コマンドは、すべてのサービスに適用され、単一のサービスには関連付けられないグローバル WCCP コマンドです。
ステップ 5	**ip wccp** [**vrf** *vrf-name*] {**web-cache** | *service-number*} 例： `Router(config)# ip wccp 201`	WCCP サービス ID を指定します。標準の Web キャッシュ サービスまたはダイナミック サービス番号（0 ～ 255）を指定できます。 指定できるサービスの最大数は 256 です。
ステップ 6	**exit** 例： `Router(config)# exit`	特権 EXEC モードに戻ります。

マルチキャスト アドレスへのルータの登録

サービス グループにマルチキャスト アドレス オプションを使用する場合、インターフェイスでマルチキャスト ブロードキャストをリスンできるようにルータを設定する必要があります。

リダイレクトされるトラフィックが仲介ルータを通過する必要があるネットワーク構成の場合、通過するルータを設定して、IP マルチキャスト ルーティングを実行するようにします。次の 2 つのコンポーネントを設定して、仲介ルータを通過できるようにします。

- **ip multicast-routing** グローバル コンフィギュレーション コマンドを使用して、IP マルチキャスト ルーティングをイネーブルにします。
- **ip wccp group-listen** インターフェイス コンフィギュレーション コマンドを使用して、キャッシュ エンジンの接続先のインターフェイスが、マルチキャストの送信を受信できるようにします。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip multicast-routing** [**vrf** *vrf-name*] [**distributed**]
4. **ip wccp** [**vrf** *vrf-name*] {**web-cache** | *service-number*} **group-address** *multicast-address*
5. **interface** *type number*
6. **ip pim** {**sparse-mode** | **sparse-dense-mode** | **dense-mode** [**proxy-register** {**list** *access-list* | **route-map** *map-name*}]}
7. **ip wccp** [**vrf** *vrf-name*] {**web-cache** | **service-number**} **group-listen**

手順の詳細

	コマンド	目的
ステップ 1	**enable** 例： Router> enable	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： Router# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip multicast-routing** [**vrf** *vrf-name*] [**distributed**] 例： Router(config)# ip multicast-routing	IP マルチキャスト ルーティングをイネーブルにします。
ステップ 4	**ip wccp** [**vrf** *vrf-name*] {**web-cache** | *service-number*} **group-address** *multicast-address* 例： Router(config)# ip wccp 99 group-address 239.1.1.1	サービス グループのマルチキャスト アドレスを指定します。
ステップ 5	**interface** *type number* 例： Router(config)# interface ethernet0/0	コンテンツ エンジンの接続先インターフェイスが、Web キャッシュ サービスが実行するマルチキャスト送信を受信できるようにし、インターフェイス コンフィギュレーション モードを開始します。
ステップ 6	**ip pim** {**sparse-mode** | **sparse-dense-mode** | **dense-mode** [**proxy-register** {**list** *access-list* | **route-map** *map-name*}]} 例： Router(config-if)# ip pim dense-mode	（任意）インターフェイスで Protocol Independent Multicast（PIM）をイネーブルにします。 **（注）** Catalyst 6500 シリーズ スイッチおよび Cisco 7600 シリーズ ルータで **ip wccp group-listen** コマンドが適切に動作するために、**ip wccp group-listen** コマンドに加えて、**ip pim** コマンドを入力する必要があります。
ステップ 7	**ip wccp** [**vrf** *vrf-name*] {**web-cache** | *service-number*} **group-listen** 例： Router(config-if)# ip wccp 99 group-listen	インターフェイスを設定して、WCCP の IP マルチキャスト パケットの受信をイネーブルまたはディセーブルにします。

WCCP サービス グループでのアクセス リストの使用

どのトラフィックをどのコンテンツ エンジンに送信するかを決定するために、アクセス リストを使用するようにルータの設定作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **access-list** *access-list-number* **remark** *remark*
4. **access-list** *access-list-number* **permit** {*source* [*source-wildcard*] | **any**} [**log**]
5. **access-list** *access-list-number* **remark** *remark*
6. **access-list** *access-list-number* **deny** {*source* [*source-wildcard*] | **any**} [**log**]
7. アクセス リストの基礎とする発信元を指定し終わるまで、ステップ 3 ～ 6 の組み合わせを繰り返します。
8. **ip wccp web-cache group-list** *access-list*
9. **ip wccp web-cache redirect-list** *access-list*

手順の詳細

	コマンド	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**access-list** *access-list-number* **remark** *remark* 例： `Router(config)# access-list 1 remark Give access to user1`	(任意) アクセス リスト エントリについて、ユーザにわかりやすいコメントを追加します。 • 最大 100 文字の注記を、アクセス リスト エントリの前または後に指定できます。
ステップ 4	**access-list** *access-list-number* **permit** {*source* [*source-wildcard*] | **any**} [**log**] 例： `Router(config)# access-list 1 permit 172.16.5.22 0.0.0.0`	キャッシュ エンジンへのトラフィックのリダイレクションをイネーブルまたはディセーブルにするアクセス リストを作成します。 発信元アドレスおよびワイルドカード マスクに基づいて、指定した発信元を許可します。 • すべてのアクセス リストには、1 つ以上の許可文が必要です。許可文は、最初のエントリである必要はありません。 • 標準の IP アクセス リストは、1 ～ 99 または 1300 ～ 1999 の番号が付けられています。 • *source-wildcard* を省略すると、0.0.0.0 のワイルドカード マスクが想定されます。これは、発信元アドレスのすべてのビットに一致することを示します。 • オプションで、*source source-wildcard* の代わりとして、キーワード **any** を使用し、発信元および 0.0.0.0 255.255.255.255 の発信元ワイルドカードを指定します。 • この例では、ホスト 172.16.5.22 がアクセス リストに適合します。

	コマンド	目的
ステップ 5	**access-list** *access-list-number* **remark** *remark* 例： `Router(config)# access-list 1 remark Give access to user1`	（任意）アクセス リスト エントリについて、ユーザにわかりやすいコメントを追加します。 • 最大 100 文字の注記を、アクセス リスト エントリの前または後に指定できます。
ステップ 6	**access-list** *access-list-number* **deny** {*source* [*source-wildcard*] | **any**} [**log**] 例： `Router(config)# access-list 1 deny 172.16.7.34 0.0.0.0`	発信元アドレスおよびワイルドカード マスクに基づいて、指定した発信元を拒否します。 • *source-wildcard* を省略すると、0.0.0.0 のワイルドカード マスクが想定されます。これは、発信元アドレスのすべてのビットに一致することを示します。 • オプションで、source source-wildcard の代わりとして、省略形 *any* を使用し、発信元および 0.0.0.0 255.255.255.255 の発信元ワイルドカードを指定します。 • この例では、ホスト 172.16.7.34 はアクセス リストに適合しません。
ステップ 7	アクセス リストの基礎とする発信元を指定し終わるまで、ステップ 3 ～ 6 の組み合わせを繰り返します。	明示的に許可されていないすべてのソースは、アクセス リストの末尾で暗黙的な **deny** 文によって拒否されます。
ステップ 8	**ip wccp** [**vrf** *vrf-name*] **web-cache group-list** *access-list* 例： `Router(config) ip wccp web-cache group-list 1`	パケットを受け入れるコンテンツ エンジンの IP アドレスをルータに示します。
ステップ 9	**ip wccp** [**vrf** *vrf-name*] **web-cache redirect-list** *access-list* 例： `Router(config)# ip wccp web-cache redirect-list 1`	（任意）特定のクライアントのキャッシングをディセーブルにします。

WCCP 発信 ACL チェックのイネーブル化

（注） ハードウェアですべてのリダイレクションを実行する場合、発信 ACL チェック処理をイネーブルにすると、リダイレクションのモードは変わります。ショートカットをインストールする前に、追加の ACL チェックがソフトウェアで実行できるように、最初のパケットは切り替えられます。

手順の概要

1. **enable**
2. **configure terminal**

3. **ip wccp** [**vrf** *vrf-name*] {**web-cache** | *service-number*} [**group-address** *multicast-address*] [**redirect-list** *access-list*] [**group-list** *access-list*] [**password** *password*]
4. **ip wccp check acl outbound**
5. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip wccp** [**vrf** *vrf-name*] {**web-cache** | *service-number*} [**group-address** *multicast-address*] [**redirect-list** *access-list*] [**group-list** *access-list*] [**password** *password*] 例： `Router(config)# ip wccp web-cache`	Cisco Content Engine のサービス グループまたはコンテンツ エンジンのサービス グループのサポートをイネーブルにし、リダイレクト ACL リストまたはグループ ACL を設定します。 （注） **web-cache** キーワードは WCCP バージョン 1 とバージョン 2 に使用でき、*service-number* 引数は WCCP バージョン 2 だけで使用できます。
ステップ 4	**ip wccp check acl outbound** 例： `Router(config)# ip wccp check acl outbound`	発信元インターフェイスで ACL 発信チェックをイネーブルにします。
ステップ 5	**exit** 例： `Router(config)# exit`	グローバル コンフィギュレーションを終了します。

WCCP コンフィギュレーション設定の確認とモニタリング

WCCP のコンフィギュレーション設定を確認およびモニタするには、EXEC モードで次のコマンドを使用します。

手順の概要

1. **enable**
2. **show ip wccp** [**vrf** *vrf-name*] [*service-number* | **web-cache**] [**detail** | **view**]
3. **show ip interface**
4. **more system:running-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**show ip wccp** [**vrf** *vrf-name*] [*service-number* | **web-cache**] [**detail** | **view**] **例：** `Router# show ip wccp 24 detail`	WCCP に関連するグローバル情報を表示します。たとえば、現在実行されているプロトコル バージョン、ルータ サービス グループのコンテンツ エンジンの数、ルータに接続できるコンテンツ エンジン グループ、使用するアクセス リストなどです。引数およびキーワードは次のとおりです。 • *service-number*：（任意）コンテンツ エンジンで制御される Web キャッシュ サービス グループのダイナミック番号。値の範囲は 0 ～ 99 です。Cisco Content Engine を使用する Web キャッシュの場合、逆プロキシ サービスは 99 の値で示されます。 • **web-cache**：（任意）Web キャッシュ サービスの統計情報。 • **detail**：（任意）検出済み、または検出されていない特定のサービス グループまたは Web キャッシュの他のメンバ。 • **view**：（任意）ルータまたはすべての Web キャッシュに関する情報。
ステップ 3	**show ip interface** **例：** `Router# show ip interface`	すべての **ip wccp redirection** コマンドがインターフェイスに設定されているかどうかに関するステータスを表示します。たとえば、「Web キャッシュ リダイレクトがイネーブルかディセーブルか」などです。
ステップ 4	**more system:running-config** **例：** `Router# more system:running-config`	（任意）現在実行されているコンフィギュレーション ファイルのコンテンツを表示します（**show running-config** コマンドと同じです）。

トラブルシューティングのヒント

WCCP をイネーブルにすると、CPU の使用率が非常に高くなるため、問題が発生しました。カウンタによって、直接ルータでバイパス トラフィックを決定し、それが原因かどうかを示すことができます。場合によっては 10% のバイパス トラフィックが標準で、他の状況では 10% が高いこともあります。ただし、25% を超える数値の場合、Web キャッシュの状況をより詳しく調査する必要があります。

バイパス トラフィックのレベルが高いことをカウンタが示している場合、次の手順は、コンテンツ エンジンのバイパス カウンタを確認し、コンテンツ エンジンがトラフィックのバイパスを選択した理由を判定します。さらに詳細に調査するには、コンテンツ エンジン コンソールにログインし、CLI を使用します。カウンタを使用すると、バイパスするトラフィックの割合を決定できます。

WCCP の設定例

例：ルータ上での WCCP バージョンの変更

次に、WCCP バージョンをデフォルトの WCCPv2 から WCCPv1 に変更し、WCCPv1 で Web キャッシュ サービスをイネーブルにする例を示します。

```
Router# show ip wccp

% WCCP version 2 is not enabled

Router# configure terminal
Router(config)# ip wccp version 1
Router(config)# end
Router# show ip wccp

% WCCP version 1 is not enabled
Router# configure terminal
Router(config)# ip wccp web-cache
Router(config)# end
Router# show ip wccp

Global WCCP information:
    Router information:
        Router Identifier:                  10.4.9.8
        Protocol Version:                   1.0
.
.
.
```

例：一般的な WCCPv2 セッションの設定

次に、一般的な WCCPv2 セッションを設定する例を示します。

```
Router# configure terminal
 ip wccp web-cache group-address 224.1.1.100 password password1
 interface ethernet0
 ip wccp web-cache redirect out
 exit
 ip wccp check services all ! Configures a check of all WCCP services.
```

例：ルータとコンテンツ エンジンのパスワードの設定

次に、パスワードが password1 の WCCPv2 パスワードを設定する例を示します。

```
Router# configure terminal
Router(config)# ip wccp web-cache password password1
```

例：Web キャッシュ サービスの設定

```
Router# configure terminal
Router(config)# ip wccp web-cache
Router(config)# interface ethernet 0
Router(config-if)# ip wccp web-cache redirect out
Router(config-if)# exit
Router# copy running-config startup-config
```

次に、イーサネット インターフェイス 0/1 に到達する HTTP トラフィックのリダイレクションをイネーブルにするセッションを設定する例を示します。

```
Router# configure terminal
Router(config)# interface ethernet 0/1
Router(config-if)# ip wccp web-cache redirect in
Router(config-if)# exit
Router# show ip interface ethernet 0/1
.
.
.
WCCP Redirect inbound is enabled
WCCP Redirect exclude is disabled
.
.
.
```

例：逆プロキシ サービスの実行

次の例では、Cisco Cache Engine を使用してサービス グループを設定し、ダイナミック サービス 99 を使用して逆プロキシ サービスを実行しているという前提です。

```
Router# configure terminal
Router(config)# ip wccp 99
Router(config)# interface ethernet 0
Router(config-if)# ip wccp 99 redirect out
```

例：マルチキャスト アドレスへのルータの登録

次に、224.1.1.100 のマルチキャスト アドレスにルータを登録する例を示します。

```
Router(config)# ip wccp web-cache group-address 224.1.1.100
Router(config)# interface ethernet 0
Router(config-if)# ip wccp web cache group-listen
```

次に、224.1.1.1 のマルチキャスト アドレスを使用して、逆プロキシ サービスを実行するようにルータを設定する例を示します。リダイレクションは、インターフェイス イーサネット 0 を介するパケットの発信に適用されます。

```
Router(config)# ip wccp 99 group-address 224.1.1.1
Router(config)# interface ethernet 0
Router(config-if)# ip wccp 99 redirect out
```

例：アクセス リストの使用

セキュリティを改善するには、標準のアクセス リストを使用して、現在のルータに登録するコンテンツ エンジンで有効なアドレスがどの IP アドレスかをルータに通知します。次に、いくつかのサンプル ホストについて、アクセス リスト番号が 10 である標準のアクセス リストのコンフィギュレーション セッションの例を示します。

```
Router(config)# access-list 10 permit host 11.1.1.1
Router(config)# access-list 10 permit host 11.1.1.2
Router(config)# access-list 10 permit host 11.1.1.3
Router(config)# ip wccp web-cache group-list 10
```

特定のクライアント、サーバ、またはクライアント/サーバ ペアのキャッシングをディセーブルにするには、WCCP アクセス リストを使用できます。次に、10.1.1.1 から 12.1.1.1 に送信される要求がキャッシュをバイパスし、その他すべての要求は通常どおりに機能する例を示します。

```
Router(config)# ip wccp web-cache redirect-list 120
Router(config)# access-list 120 deny tcp host 10.1.1.1 any
Router(config)# access-list 120 deny tcp any host 12.1.1.1
Router(config)# access-list 120 permit ip any any
```

次の例では、インターフェイス イーサネット 0/1 を介して受信した Web 関連のパケットを、209.165.200.224 以外の任意のホストにリダイレクトするようにルータを設定します。

```
Router(config)# access-list 100 deny ip any host 209.165.200.224
Router(config)# access-list 100 permit ip any any
Router(config)# ip wccp web-cache redirect-list 100
Router(config)# interface Ethernet 0/1
Router(config-if)# ip wccp web-cache redirect in
```

例：WCCP 発信 ACL チェックの設定

次に、アクセス リストによって、ファスト イーサネット インターフェイス 0/0 を介するネットワーク 10.0.0.0 からのトラフィックを回避する設定例を示します。発信 ACL チェックはイネーブルなので、WCCP はそのトラフィックをリダイレクトしません。WCCP は、パケットのリダイレクト前に、ACL に対してパケットをチェックします。

```
Router(config)# ip wccp web-cache
Router(config)# ip wccp check acl outbound
Router(config)# interface fastethernet0/0
Router(config-if)# ip access-group 10 out
Router(config-if)# exit
Router(config)# ip wccp web-cache redirect-list redirect-out
Router(config)# access-list 10 deny 10.0.0.0 0.255.255.255
Router(config)# access-list 10 permit any
```

発信 ACL チェックをディセーブルにする場合、ネットワーク 10.0.0.0 からの HTTP パケットを Web キャッシュにリダイレクトします。そのネットワーク アドレスを使用するユーザは、ネットワーク管理者が回避しようとしても、Web ページを取得できます。

例：WCCP 設定の確認

次に、特権 EXEC モードで **more system:running-config** コマンドを使用して設定の変更を検証する例を示します。次に、Web キャッシュ サービスおよびダイナミック サービス 99 の両方をルータでイネーブルにする例を示します。

```
Router# more system:running-config

    Building configuration...
    Current configuration:
    !
    version 12.0
    service timestamps debug uptime
    service timestamps log uptime
    no service password-encryption
    service udp-small-servers
    service tcp-small-servers
    !
    hostname router4
    !
    enable secret 5 $1$nSVy$faliJsVQXVPW.KuCxZNTh1
    enable password password1
    !
    ip subnet-zero
    ip wccp web-cache
    ip wccp 99
    ip domain-name cisco.com
    ip name-server 10.1.1.1
    ip name-server 10.1.1.2
    ip name-server 10.1.1.3
    !
    !
    !
    interface Ethernet0
    ip address 10.3.1.2 255.255.255.0
    no ip directed-broadcast
    ip wccp web-cache redirect out
    ip wccp 99 redirect out
    no ip route-cache
    no ip mroute-cache
    !

    interface Ethernet1
    ip address 10.4.1.1 255.255.255.0
    no ip directed-broadcast
    ip wccp 99 redirect out
    no ip route-cache
    no ip mroute-cache
    !
    interface Serial0
    no ip address
    no ip directed-broadcast
    no ip route-cache
    no ip mroute-cache
    shutdown
    !
    interface Serial1
    no ip address
    no ip directed-broadcast
    no ip route-cache
    no ip mroute-cache
    shutdown
    !
```

```
ip default-gateway 10.3.1.1
ip classless
ip route 0.0.0.0 0.0.0.0 10.3.1.1
no ip http server
!
!
!
line con 0
transport input none
line aux 0
transport input all
line vty 0 4
password alaska1
login
!
end
```

次に、Cisco IOS のスイッチング パスであるプロセス、ファスト、および CEF について、バイパスしたパケットの情報を表示する例を示します。

```
Router# show ip wccp web-cache detail

WCCP Client information:
 Web Client ID:          10.10.10.1
 Protocol Version:       2.0
 State:                  Usable
 Initial Hash Info:      00000000000000000000000000000000
                         00000000000000000000000000000000
 Assigned Hash Info:     FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
                         FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
 Hash Allotment:         256 (100.00%)
 Packets Redirected:     4320
 Connect Time:           00:04:53
 Bypassed Packets
 Process:                0
 Fast:                   0
 CEF:                    250
```

show ip wccp web-cache コマンドの詳細については、『*Cisco IOS IP Application Services Command Reference*』を参照してください。

その他の参考資料

関連資料

内容	参照先
Cisco IOS コマンド	『*Cisco IOS Master Commands List, All Releases*』
Cisco ACNS ソフトウェア設定情報	• 『*Cisco ACNS Software Caching Configuration Guide*, Release 4.2』 • Cisco.com の「Cisco ACNS Software」リスト ページ
IP アクセス リストの概要、設定作業、およびコマンド	• 『*IP Access List Features Roadmap*』 • 『*Cisco IOS Security Command Reference*』
IP アドレッシングおよびサービス コマンド、および設定作業	• 『*Cisco IOS IP Addressing Services Configuration Guide*』 • 『*Cisco IOS IP Addressing Services Command Reference*』
WCCP コマンド：コマンド構文、コマンド モード、コマンド履歴、デフォルト設定、使用に関する注意事項および例	『*Cisco IOS IP Application Services Command Reference*』

規格

規格	タイトル
新しい規格または変更された規格はサポートされていません。また、既存の規格に対するサポートに変更はありません。	—

MIB

MIB	MIB リンク
新しい MIB または変更された MIB はサポートされていません。また、既存の MIB に対するサポートに変更はありません。	選択されたプラットフォーム、シスコ ソフトウェア リリース、およびフィーチャ セットの MIB を検索してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
新しい RFC または変更された RFC はサポートされていません。また、既存の RFC に対するサポートに変更はありません。	

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 ・テクニカル サポートを受ける ・ソフトウェアをダウンロードする ・セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける ・ツールおよびリソースへアクセスする - Product Alert の受信登録 - Field Notice の受信登録 - Bug Toolkit を使用した既知の問題の検索 ・Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する ・トレーニング リソースへアクセスする ・TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

WCCP の機能情報

表 1 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。

プラットフォーム サポートとソフトウェア イメージ サポートに関する情報を入手するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator を使用すると、特定のソフトウェア リリース、フィーチャ セット、またはプラットフォームをサポートするソフトウェア イメージを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 表 1 に、特定のソフトウェア リリース トレイン内の機能に対するサポートが導入されたソフトウェア リリースだけを示します。特に断りのないかぎり、そのソフトウェア リリース トレイン以降のリリースでもその機能がサポートされます。

表 1　WCCP の機能情報

機能名	リリース	機能情報
WCCP バイパス カウンタ	12.3(7)T 12.2(25)S	WCCP バイパス カウンタ機能を使用すると、Web キャッシュによってバイパスされ、元のルータに返送され、通常どおりに転送されたパケットのカウントを表示できます。 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。 • 「WCCP バイパス パケット」（P.11） • 「例：WCCP 設定の確認」（P.26） **show ip wccp** コマンドはこの機能によって変更されました。
WCCP クローズド サービス	12.4(11)T	WCCP クローズド サービス機能では、WCCP が常にこのようなサービスのトラフィックを代行受信するように WCCP サービスを設定できますが、このトラフィックを受信するように登録された WCCP クライアント（コンテンツ エンジンなど）がない場合、パケットは破棄されます。 この動作は Application-Oriented Network Services（AONS）アプリケーションをサポートします。AONS は WCCP を使用してトラフィックを透過的に代行受信する必要がありますが、WCCP クライアントがパケットを処理できない場合は、パケットを宛先に転送しません（これは、キャッシュがなくてもユーザから見える動作が変化しないという、キャッシュを補助する WCCP の従来の使用方法とは対照的です）。 この機能に関する詳細については、次の各項を参照してください。 • 「WCCP クローズド サービスおよびオープン サービス」（P.11） • 「クローズド サービスの設定」（P.16） • 「例：一般的な WCCPv2 セッションの設定」（P.23） **ip wccp** コマンドは、この機能によって変更されました。
WCCP Increased Service	12.3(14)T 12.2(33)SRA 12.2(33)SXH	WCCP Increased Service 機能によって、WCCP でサポートされるサービス数が VRF 全体で最大 256 に増えます。 この機能に関する詳細については、次の各項を参照してください。 • 「WCCP サービス グループ」（P.12） • 「クローズド サービスの設定」（P.16） • 「WCCP の設定」（P.14） • 「例：WCCP 設定の確認」（P.26） **ip wccp**、**ip wccp check services all**、**ip wccp outbound-acl-check**、および **show ip wccp** コマンドがこの機能によって変更されました。

表 1　WCCP の機能情報 （続き）

機能名	リリース	機能情報
WCCP レイヤ 2 リダイレクション/フォワーディング	12.4(20)T	WCCP レイヤ 2 リダイレクション/フォワーディング機能を使用すると、直接接続している Cisco Content Engine でレイヤ 2 リダイレクトを使用できます。これは、GRE カプセル化を介するレイヤ 3 リダイレクションよりも効率的です。直接接続しているキャッシュ エンジンを設定して、WCCP レイヤ 2 リダイレクション/フォワーディング機能の使用をネゴシエートできます。WCCP レイヤ 2 リダイレクション/フォワーディング機能には、ルータまたはスイッチに設定は必要ありません。 この機能に関する詳細については、次の各項を参照してください。 • 「WCCP に関する制約事項」（P.2） • 「レイヤ 2 フォワーディング、リダイレクション、および返送」（P.5） • 「HTTP 以外のサービスのサポート」（P.9） この機能に関連する新しいコマンドや変更されたコマンドはありません。
WCCP L2 返送	12.4(20)T	WCCP L2 返送機能を使用すると、レイヤ 3 GRE トンネル内のルータにパケットをトンネル処理するのではなく、発信元および宛先の MAC アドレスを交換することで、コンテンツ エンジンから、レイヤ 2 で直接接続されている WCCP ルータにパケットを返送できます。 この機能に関する詳細については、次の各項を参照してください。 • 「レイヤ 2 フォワーディング、リダイレクション、および返送」（P.5） この機能に関連する新しいコマンドや変更されたコマンドはありません。
WCCP マスク割り当て	12.4(20)T	WCCP マスク割り当て機能では、キャッシュ エンジン割り当て方式として、ACNS/WAAS デバイスのサポートを導入します。 この機能については、次の項に説明があります。 • 「WCCP マスク割り当て」（P.6） この機能に関連する新しいコマンドや変更されたコマンドはありません。

表 1　WCCP の機能情報 （続き）

機能名	リリース	機能情報
WCCP 発信 ACL チェック	12.3(7)T 12.2(25)S	WCCP 発信 ACL チェック機能を使用すると、入力インターフェイスで WCCP によってリダイレクトされるトラフィックが、必ず発信 ACL チェックを受けるようにできます。これは、リダイレクト前に終了インターフェイスで設定できます。 この機能は、Web Cache Communication Protocol（WCCP）バージョン 1 およびバージョン 2 でサポートされます。 この機能に関する詳細については、次の各項を参照してください。 • 「WCCP 発信 ACL チェック」（P.12） • 「WCCP 発信 ACL チェックのイネーブル化」（P.20） • 「例：WCCP 発信 ACL チェックの設定」（P.25） **ip wccp** コマンドおよび **ip wccp check acl outbound** コマンドが、この機能で導入または変更されました。
受信インターフェイスでの WCCP のリダイレクション	12.1(3)T 15.0(1)S	受信インターフェイスでの WCCP のリダイレクション機能によって、特定の WCCP サービスのために入力リダイレクションのインターフェイスを設定できます。インターフェイスでこの機能をイネーブルにすると、そのインターフェイスに到達するすべてのパケットは、指定した WCCP サービスに対して比較されます。パケットが一致する場合、そのパケットはリダイレクトされます。 この機能に関する詳細については、次の各項を参照してください。 • 「WCCP に関する制約事項」（P.2） • 「WCCP の設定」（P.14） • 「例：Web キャッシュ サービスの設定」（P.24） **ip wccp redirect-list** コマンドは、この機能で導入または変更されました。

表 1　WCCP の機能情報 （続き）

機能名	リリース	機能情報
WCCP バージョン 2	12.0(3)T 15.0(1)S	WCCP バージョン 2 のいくつかの機能が強化され、次のように WCCP プロトコルに機能が追加されました。 • 複数のルータがコンテンツ エンジン クラスタにサービスを提供できます。 • 多様な UDP および TCP トラフィックなど、HTTP（TCP ポート 80 トラフィック）以外のトラフィックをリダイレクトできます。 • パスワードと HMAC MD5 規格を使用して、サービス グループの一部になるルータとコンテンツ エンジンを制御できる、オプションの認証機能があります。 • 機能していないコンテンツ エンジンから返送された要求を判断できるパケットのチェック機能があります。 • 個々のコンテンツ エンジンの負荷を調整して、空きリソースを効率的に使用できるようになります。さらに、クライアントに対して高い Quality Of Service（QoS）を確保できます。 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。 • 「WCCP に関する制約事項」（P.2） • 「WCCPv2 の設定」（P.8） • 「HTTP 以外のサービスのサポート」（P.9） • 「例：一般的な WCCPv2 セッションの設定」（P.23） **clear ip wccp**、**ip wccp**、**ip wccp group-listen**、**ip wccp redirect**、**ip wccp redirect exclude in**、**ip wccp version**、**show ip wccp** の各コマンドが、この機能で導入または変更されました。
WCCP VRF のサポート	15.0(1)M、 12.2(33)SRE	WCCP VRF のサポート機能によって、VRF の認識をサポートする既存の WCCPv2 プロトコルが強化されています。 Cisco IOS Release 12.2(33)SRE では、この機能が Cisco 7200 NPE-G2 ルータと Cisco 7304-NPE-G100 ルータ上でのみサポートされます。 この機能に関する詳細については、次の各項を参照してください。 • 「WCCP VRF のサポート」（P.11） • 「WCCP の設定」（P.14） **clear ip wccp**、**debug ip wccp**、**ip wccp**、**ip wccp group-listen**、**ip wccp redirect**、**show ip wccp** の各コマンドが、この機能で導入または変更されました。

ファーストホップ冗長プロトコル（FHRP）

FHRP 機能ロードマップ

この機能ロードマップでは、『*Cisco IOS IP アプリケーション サービス コンフィギュレーション ガイド*』に記載された Cisco IOS FHRP 機能を一覧にし、各機能の説明が記載された参照先を示します。ロードマップは、お使いのリリースで使用できる機能を参照できるように編成されています。目的の機能名を探して、「参照先」列の URL をクリックすると、その機能の説明が記載された参照先にアクセスできます。

以前使用されていた機能の多くは、コンフィギュレーション ファイルに組み込まれています。このロードマップでは、これらについては記載していない機能もあります。このロードマップ情報は、他のソフトウェア リリースやプラットフォームについてもサポートします。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。

機能とリリース サポート

表 1 に、次の Cisco IOS ソフトウェア リリースでサポートされる FHRP 機能の一覧を表示します。

- 「Cisco IOS Release 15.0S」
- 「Cisco IOS Release 12.2S」
- 「Cisco IOS Release 12.2SB」
- 「Cisco IOS Release 12.2SR」
- 「Cisco IOS Release 12.2SX」
- 「Cisco IOS Release 12.2T、12.3、12.3T」
- 「Cisco IOS Release 12.4T」
- 「Cisco IOS XE 3.1.0SG」
- 「その他の Cisco IOS リリース」

プラットフォーム サポートとソフトウェア イメージ サポートに関する情報を入手するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator を使用すると、Cisco IOS、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 1 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 1 に、各ソフトウェアの最新リリースの一覧を示します。また、対象のリリースで使用可能な機能をアルファベット順に紹介します。

表 1　サポート対象の FHRP 機能

リリース	機能名	機能の説明	参照先
Cisco IOS Release 15.0S			
15.0(1)S	FHRP：IP SLA 動作の拡張オブジェクト トラッキング	FHRP : IP SLA 動作の拡張オブジェクト トラッキング機能では、FHRP およびその他の EOT クライアントが IP SLA オブジェクトからの出力を追跡し、提供された情報を使用してアクションを発生させることができます。	*Configuring Enhanced Object Tracking*
	FHRP - HSRP グループ シャットダウン	FHRP - HSRP グループ シャットダウン機能を使用すると、トラッキング対象のオブジェクトがダウンしたときに、HSRP グループのプライオリティを下げるのではなく、ディセーブルな状態になる（ステートが Init になる）ように HSRP グループを設定することができます。	*Configuring HSRP*
	FHRP：オブジェクト追跡リスト	この機能によりトラッキング機能が強化され、リスト内で追跡対象オブジェクトを組み合わせて設定したり、ブール ロジックを使用した柔軟性のある方法でオブジェクトを組み合わせたりすることができます。	*Configuring Enhanced Object Tracking*
	Gateway Load-Balancing Protocol（GLBP; ゲートウェイ ロード バランシング プロトコル）	GLBP は、冗長化されたルータ グループ間でパケットのロード シェアリングを行う一方、機能を停止したルータや回路（HSRP や VRRP など）からのデータ トラフィックを保護します。	*Configuring GLBP*
	HSRP：Hot Standby Router Protocol（ホット スタンバイ ルータ プロトコル）	HSRP は、ファーストホップ IP ルータの透過的なフェールオーバーを可能にするように設計された First Hop Redundancy Protocol（FHRP; ファーストホップ冗長プロトコル）です。	*Configuring HSRP*
	HSRP - ISSU	HSRP - In-Service Software Upgrade（ISSU; インサービス ソフトウェア アップグレード）機能により、HSRP で ISSU がサポートされています。 ISSU は、パケット転送を続行しながら、Cisco IOS ソフトウェアのアップデートや修正を行うことができるプロセスです。	*Configuring HSRP*
	HSRP MD5 認証	HSRP MD5 認証機能は、マルチキャスト HSRP プロトコル パケットの HSRP 部分の MD5 ダイジェストを生成するように拡張されています。この機能により、セキュリティが強化され、HSRP スプーフィング ソフトウェアの脅威に対する保護が得られます。	*Configuring HSRP*

表 1　サポート対象の FHRP 機能 （続き）

リリース	機能名	機能の説明	参照先
	HSRP 複数グループ最適化	HSRP 複数グループ最適化機能により、サブインターフェイスで設定されている複数の HSRP グループのネゴシエーションとメンテナンス方法が改善されました。アクティブ ルータとスタンバイ ルータを選出するために物理インターフェイスに必要なのは、1 つの HSRP グループだけです。このグループがマスター グループと呼ばれます。他の HSRP グループは、各サブインターフェイスに作成されたり、グループ名によってマスター グループとリンクされたりします。リンクされた HSRP グループは、*クライアント グループ*または*従属グループ*と呼ばれます。	*Configuring HSRP*
	HSRP の ICMP リダイレクト サポート	HSRP の ICMP リダイレクト サポート機能により、HSRP を使用して設定されているインターフェイスで ICMP リダイレクトが可能になっています。	*Configuring HSRP*
	HSRP の MPLS VPN サポート	HSRP の Multiprotocol Label Switching（MPLS; マルチプロトコル ラベル スイッチング）Virtual Private Network（VPN; バーチャル プライベート ネットワーク）インターフェイス サポートが役に立つのは、次のいずれかの状態で 2 つの Provider Edge（PE; プロバイダー エッジ）ルータ間でイーサネット LAN が接続されている場合です。	*Configuring HSRP*
	HSRP バージョン 2	HSRP バージョン 2 機能は、今後の機能拡張に備え、HSRP バージョン 1 よりも機能を拡張するために導入されました。HSRP バージョン 2 のパケット形式は、バージョン 1 とは異なります。	*Configuring HSRP*
	SSO：GLBP	GLBP が SSO を認識するようになりました。GLBP は、ルータがセカンダリ RP にフェールオーバーしたことを検出し、GLBP グループの現在の状態を継続することができます。	*Configuring GLBP*
	SSO - HSRP	SSO HSRP は、冗長な Route Processor（RP; ルート プロセッサ）を装備したルータが Stateful Switchover（SSO; ステートフル スイッチオーバー）用に設定されているときの HSRP の動作を変更します。ある RP がアクティブで、もう一方の RP がスタンバイになっているとき、アクティブ RP に障害が発生すると、SSO は処理を引き継ぐスタンバイ RP をイネーブルにします。	*Configuring HSRP*
	Virtual Router Redundancy Protocol	VRRP は、ルータのグループを使用して単一の仮想ルータを形成し、冗長性を実現します。これにより、仮想ルータをデフォルト ゲートウェイとして使用するように、LAN クライアントを設定できます。ルータのグループを表す仮想ルータは、「VRRP グループ」とも呼ばれます。	*Configuring VRRP*

表 1　サポート対象の FHRP 機能 （続き）

リリース	機能名	機能の説明	参照先
Cisco IOS Release 12.2S			
12.2(25)S	拡張トラッキング サポート	拡張トラッキング サポート機能は、HSRP からトラッキング メカニズムを分離させて、独立したトラッキング プロセスを別途生成します。これにより、HSRP 以外の Cisco IOS プロセスがこのトラッキング プロセスを使用できます。この機能を使用すると、インターフェイスのラインプロトコル ステートに加えて他のオブジェクトも追跡できます。	*Configuring Enhanced Object Tracking*
	FHRP : IP SLA 動作の拡張オブジェクト トラッキング	この機能により、FHRP およびその他の拡張オブジェクト トラッキング（EOT）クライアントが、IP SLA オブジェクトの出力を追跡し、提供された情報を使用してアクションを開始できます。	*Configuring Enhanced Object Tracking*
	HSRP MD5 認証	HSRP MD5 認証機能は、マルチキャスト HSRP プロトコル パケットの HSRP 部分の MD5 ダイジェストを生成するように拡張されています。この機能により、セキュリティが強化され、HSRP スプーフィング ソフトウェアの脅威に対する保護が得られます。	*Configuring HSRP*
	HSRP バージョン 2	HSRP バージョン 2 機能は、今後の機能拡張に備え、HSRP バージョン 1 よりも機能を拡張するために導入されました。HSRP バージョン 2 のパケット形式は、バージョン 1 とは異なります。	*Configuring HSRP*
	SSO - HSRP	SSO HSRP は、冗長な Route Processor（RP; ルート プロセッサ）を装備したルータが Stateful Switchover（SSO; ステートフル スイッチオーバー）用に設定されているときの HSRP の動作を変更します。ある RP がアクティブで、もう一方の RP がスタンバイになっているとき、アクティブ RP に障害が発生すると、SSO は処理を引き継ぐスタンバイ RP をイネーブルにします。	*Configuring HSRP*
12.2(18)S	GLBP MD5 認証	MD5 認証は、代替となるプレーン テキスト認証スキームよりも高いセキュリティを実現します。	*Configuring GLBP*

表 1　サポート対象の FHRP 機能 （続き）

リリース	機能名	機能の説明	参照先
12.2(14)S	Gateway Load Balancing Protocol	Gateway Load Balancing Protocol（GLBP; ゲートウェイ ロード バランシング プロトコル）は、Hot Standby Router Protocol（HSRP; ホット スタンバイ ルータ プロトコル）や Virtual Router Redundancy Protocol（VRRP; 仮想ルータ冗長プロトコル）のように、機能を停止したルータや回路からデータ トラフィックを保護します。このとき、冗長化されたルータのグループ間でパケットのロード シェアリングを行うことができます。	*Configuring GLBP*
	HSRP：ホットスタンバイ ルータ プロトコルと IPSec	HSRP は、スタンバイ コマンドライン インターフェイス（CLI）コマンドを使用して LAN インターフェイス上に設定できます。インターフェイスから、ローカル IPsec ID またはローカル トンネル エンドポイントとしてスタンバイ IP アドレスを使用できます。	*IPsec VPN High Availability Enhancements*
	Virtual Router Redundancy Protocol	VRRP は、ルータのグループを使用して単一の仮想ルータを形成し、冗長性を実現します。これにより、仮想ルータをデフォルト ゲートウェイとして使用するように、LAN クライアントを設定できます。ルータのグループを表す仮想ルータは、「VRRP グループ」とも呼ばれます。	*Configuring VRRP*
Cisco IOS Release 12.2SB			
12.2(31)SB2	FHRP：オブジェクト追跡リスト	この機能によりトラッキング機能が強化され、リスト内で追跡対象オブジェクトを組み合わせて設定したり、ブール ロジックを使用した柔軟性のある方法でオブジェクトを組み合わせたりすることができます。	*Configuring Enhanced Object Tracking*
	ISSU と GLBP	GLBP は In Service Software Upgrade（ISSU; インサービス ソフトウェア アップグレード）をサポートします。ISSU を使用すると、アクティブおよびスタンバイの Route Processor（RP; ルート プロセッサ）またはラインカード上で異なるバージョンの Cisco IOS ソフトウェアが実行されている場合でも、ハイアベイラビリティ（HA）システムを SSO モードで実行できるようになります。	*Configuring GLBP*
	SSO：GLBP	GLBP が SSO を認識するようになりました。GLBP は、ルータがセカンダリ RP にフェールオーバーしたことを検出し、GLBP グループの現在の状態を継続することができます。	*Configuring GLBP*

表 1　サポート対象の FHRP 機能 （続き）

リリース	機能名	機能の説明	参照先
12.2(28)SB	拡張トラッキング サポート	拡張トラッキング サポート機能は、HSRP からトラッキング メカニズムを分離させて、独立したトラッキング プロセスを別途生成します。これにより、HSRP 以外の Cisco IOS プロセスがこのトラッキング プロセスを使用できます。この機能を使用すると、インターフェイスのラインプロトコル ステートに加えて他のオブジェクトも追跡できます。	*Configuring Enhanced Object Tracking*
	HSRP の MPLS VPN サポート	HSRP の Multiprotocol Label Switching（MPLS; マルチプロトコル ラベル スイッチング）Virtual Private Network（VPN; バーチャル プライベート ネットワーク）インターフェイス サポートが役に立つのは、次のいずれかの状態で 2 つの Provider Edge（PE; プロバイダー エッジ）ルータ間でイーサネット LAN が接続されている場合です。	*Configuring HSRP*
Cisco IOS Release 12.2SR			
12.2(33)SRE	FHRP : **rtr** キーワードの EOT の廃止	この機能により、**track rtr** コマンドは **track ip sla** コマンドで置き換えられました。	*Configuring Enhanced Object Tracking*
12.2(33)SRC	FHRP - HSRP グループ シャットダウン	FHRP - HSRP グループ シャットダウン機能を使用すると、トラッキング対象のオブジェクトがダウンしたときに、HSRP グループのプライオリティを下げるのではなく、ディセーブルな状態になる（ステートが Init になる）ように HSRP グループを設定することができます。	*Configuring HSRP*
	ICMP Router Discovery Protocol	ICMP Router Discovery Protocol（IRDP）を使用すると、IPv4 ホストが他の（ローカルではない）IP ネットワークに対する IPv4 接続を提供するルータを特定できるようになります。	*Configuring IRDP*
	ISSU と VRRP	VRRP は In Service Software Upgrade（ISSU; インサービス ソフトウェア アップグレード）をサポートします。ISSU を使用すると、アクティブおよびスタンバイの Route Processor（RP; ルート プロセッサ）またはラインカード上で異なるバージョンの Cisco IOS ソフトウェアが実行されている場合でも、ハイアベイラビリティ（HA）システムをステートフル スイッチオーバー（SSO）モードで実行できるようになります。	*Configuring VRRP*
	SSO と VRRP	VRRP が SSO を認識するようになりました。VRRP は、ルータがセカンダリ RP にフェールオーバーしたことを検出し、VRRP グループの現在の状態を継続することができます。	*Configuring VRRP*

表 1　サポート対象の FHRP 機能 （続き）

リリース	機能名	機能の説明	参照先
12.2(33) SRB1	ISSU と GLBP	GLBP は In Service Software Upgrade (ISSU; インサービス ソフトウェア アップグレード）をサポートします。ISSU を使用すると、アクティブおよびスタンバイの Route Processor（RP; ルート プロセッサ）またはラインカード上で異なるバージョンの Cisco IOS ソフトウェアが実行されている場合でも、ハイアベイラビリティ（HA）システムを SSO モードで実行できるようになります。	*Configuring GLBP*
	HSRP - ISSU	HSRP - In-Service Software Upgrade（ISSU; インサービス ソフトウェア アップグレード）機能により、HSRP で ISSU がサポートされています。 ISSU は、パケット転送を続行しながら、Cisco IOS ソフトウェアのアップデートや修正を行うことができるプロセスです。	*Configuring HSRP*
12.2(33)SRB	FHRP - HSRP 複数グループ最適化	HSRP 複数グループ最適化機能により、サブインターフェイスで設定されている複数の HSRP グループのネゴシエーションとメンテナンス方法が改善されました。アクティブ ルータとスタンバイ ルータを選出するために物理インターフェイスに必要なのは、1 つの HSRP グループだけです。このグループがマスター グループと呼ばれます。他の HSRP グループは、各サブインターフェイスに作成されたり、グループ名によってマスター グループとリンクされたりします。リンクされた HSRP グループは、*クライアント グループ*または*従属グループ*と呼ばれます。	*Configuring HSRP*
	FHRP - HSRP の IPv6 サポート	IPv6 のサポートが追加されました。 詳細については、『*Cisco IOS IPv6 Configuration Guide*, Release 12.4T』の「Configuring First Hop Redundancy Protocols」を参照してください。	*Configuring HSRP*
	FHRP：拡張オブジェクト トラッキングと Embedded Event Manager との統合	EOT が EEM と統合され、Embedded Event Manager（EEM）は追跡対象オブジェクトのステータス変更を報告し、EOT は EEM オブジェクトを追跡できるようになりました。	*Configuring Enhanced Object Tracking*
	SSO：GLBP	GLBP が SSO を認識するようになりました。GLBP は、ルータがセカンダリ RP にフェールオーバーしたことを検出し、GLBP グループの現在の状態を継続することができます。	*Configuring GLBP*

表 1　サポート対象の FHRP 機能 （続き）

リリース	機能名	機能の説明	参照先
12.2(33)SRA	拡張トラッキング サポート	拡張トラッキング サポート機能は、HSRP からトラッキング メカニズムを分離させて、独立したトラッキング プロセスを別途生成します。これにより、HSRP 以外の Cisco IOS プロセスがこのトラッキング プロセスを使用できます。この機能を使用すると、インターフェイスのラインプロトコル ステートに加えて他のオブジェクトも追跡できます。	*Configuring Enhanced Object Tracking*
	FHRP：IP SLA 動作の拡張オブジェクト トラッキング	この機能により、FHRP およびその他の EOT クライアントが、IP SLA オブジェクトの出力を追跡し、提供された情報を使用してアクションを開始できます。	*Configuring Enhanced Object Tracking*
	FHRP：オブジェクト追跡リスト	この機能によりトラッキング機能が強化され、リスト内で追跡対象オブジェクトを組み合わせて設定したり、ブール ロジックを使用した柔軟性のある方法でオブジェクトを組み合わせたりすることができます。	*Configuring Enhanced Object Tracking*
	HSRP MD5 認証	HSRP MD5 認証機能は、マルチキャスト HSRP プロトコル パケットの HSRP 部分の MD5 ダイジェストを生成するように拡張されています。この機能により、セキュリティが強化され、HSRP スプーフィング ソフトウェアの脅威に対する保護が得られます。	*Configuring HSRP*
	SSO - HSRP	SSO HSRP は、冗長な RP を装備したルータが SSO 用に設定されているときの HSRP の動作を変更します。ある RP がアクティブで、もう一方の RP がスタンバイになっているとき、アクティブ RP に障害が発生すると、SSO は処理を引き継ぐスタンバイ RP をイネーブルにします。	*Configuring HSRP*
Cisco IOS Release 12.2SX			
12.2(33)SXI4	HSRP グローバル IPv6 アドレス	HSRP は、ファーストホップ IPv6 ルータの透過的フェールオーバーを可能にするように設計された FHRP です。	*Configuring First Hop Redundancy Protocols in IPv6*
12.2(33)SXI1	FHRP：**rtr** キーワードの EOT の廃止	この機能により、**track rtr** コマンドは **track ip sla** コマンドで置き変えられました。	*Configuring Enhanced Object Tracking*

表 1　サポート対象の FHRP 機能 （続き）

リリース	機能名	機能の説明	参照先
12.2(33)SXI	FHRP - HSRP グループ シャットダウン	FHRP - HSRP グループ シャットダウン機能を使用すると、トラッキング対象のオブジェクトがダウンしたときに、HSRP グループのプライオリティを下げるのではなく、ディセーブルな状態になる（ステートが Init になる）ように HSRP グループを設定することができます。	*Configuring HSRP*
	FHRP - HSRP の IPv6 サポート	IPv6 のサポートが追加されました。 詳細については、『*Cisco IOS IPv6 Configuration Guide*, Release 12.4T』の「Configuring First Hop Redundancy Protocols」を参照してください。	*Configuring HSRP*
	GLBP クライアント キャッシュ	GLBP クライアント キャッシュには、GLBP グループをデフォルト ゲートウェイとして使用しているネットワーク ホストに関する情報が含まれています。GLBP クライアント キャッシュには、特定の GLBP グループを使用する各ホストの MAC アドレス、各ネットワーク ホストに割り当てられている GLBP フォワーダの数、GLBP グループの各フォワーダに現在割り当てられているネットワーク ホストの総数が格納されます。また、各ネットワーク ホストによって使用されるプロトコル アドレス、ホストとフォワーダの割り当てが最後に更新されてから経過した時間も格納されます。	*Configuring GLBP*
	HSRP 複数グループ最適化	HSRP 複数グループ最適化機能により、サブインターフェイスで設定されている複数の HSRP グループのネゴシエーションとメンテナンス方法が改善されました。アクティブ ルータとスタンバイ ルータを選出するために物理インターフェイスに必要なのは、1 つの HSRP グループだけです。このグループがマスター グループと呼ばれます。他の HSRP グループは、各サブインターフェイスに作成されたり、グループ名によってマスター グループとリンクされたりします。リンクされた HSRP グループは、*クライアント グループ*または*従属グループ*と呼ばれます。	*Configuring HSRP*
	HSRP gratuitous ARP	HSRP gratuitous ARP 機能により、HSRP は ARP キャッシュ内のエントリが正しいことを確認し、1 つまたは複数のアクティブ HSRP グループから gratuitous ARP パケットを定期的に送信するように設定されます。	*Configuring HSRP*
	SSO と VRRP	VRRP が SSO を認識するようになりました。VRRP は、ルータがセカンダリ RP にフェールオーバーしたことを検出し、VRRP グループの現在の状態を継続することができます。	*Configuring VRRP*

表 1　サポート対象の FHRP 機能 （続き）

リリース	機能名	機能の説明	参照先
12.2(33)SXH	拡張トラッキング サポート	拡張トラッキング サポート機能は、HSRP からトラッキング メカニズムを分離させて、独立したトラッキング プロセスを別途生成します。これにより、HSRP 以外の Cisco IOS プロセスがこのトラッキング プロセスを使用できます。この機能を使用すると、インターフェイスのラインプロトコル ステートに加えて他のオブジェクトも追跡できます。	*Configuring Enhanced Object Tracking*
	FHRP：IP SLA 動作の拡張オブジェクト トラッキング	この機能により、FHRP およびその他の EOT クライアントが、IP SLA オブジェクトの出力を追跡し、提供された情報を使用してアクションを開始できます。	*Configuring Enhanced Object Tracking*
	FHRP：オブジェクト追跡リスト	この機能によりトラッキング機能が強化され、リスト内で追跡対象オブジェクトを組み合わせて設定したり、ブール ロジックを使用した柔軟性のある方法でオブジェクトを組み合わせたりすることができます。	*Configuring Enhanced Object Tracking*
	GLBP MD5 認証	MD5 認証は、代替となるプレーン テキスト認証スキームよりも高いセキュリティを実現します。	*Configuring GLBP*
	HSRP MD5 認証	HSRP MD5 認証機能は、マルチキャスト HSRP プロトコル パケットの HSRP 部分の MD5 ダイジェストを生成するように拡張されています。この機能により、セキュリティが強化され、HSRP スプーフィング ソフトウェアの脅威に対する保護が得られます。	*Configuring HSRP*
	SSO：GLBP	GLBP が SSO を認識するようになりました。GLBP は、ルータがセカンダリ RP にフェールオーバーしたことを検出し、GLBP グループの現在の状態を継続することができます。	*Configuring GLBP*
	SSO - HSRP	SSO HSRP は、冗長な Route Processor（RP; ルート プロセッサ）を装備したルータが Stateful Switchover（SSO; ステートフル スイッチオーバー）用に設定されているときの HSRP の動作を変更します。ある RP がアクティブで、もう一方の RP がスタンバイになっているとき、アクティブ RP に障害が発生すると、SSO は処理を引き継ぐスタンバイ RP をイネーブルにします。	*Configuring HSRP*
Cisco IOS Release 12.2T、12.3、12.3T			
12.3(14)T	FHRP—VRRP 拡張	FHRP—VRRP 拡張機能により、次のサポートが追加されます。 • MD5 認証：VRRP に設定されているルータに追加されます。HSRP と同様に、RFC 2338 に規定されている方法よりも簡単な方法を使用した、ピアの認証方法を提供します。 • Bridged Virtual Interface（BVI）：BVI に VRRP を設定する機能を追加します。この機能は、BVI に既存の HSRP サポートに類似しています。	*Configuring VRRP*
12.3(11)T	VRRP MIB—RFC 2787	この機能により、SNMP ベースのネットワーク管理で使用できるように MIB の機能が強化されました。VRRP を使用するルータの設定、モニタ、および制御をサポートするようになりました。	*Configuring VRRP*

表 1　サポート対象の FHRP 機能 （続き）

リリース	機能名	機能の説明	参照先
12.3(8)T	FHRP：オブジェクト追跡リスト	この機能によりトラッキング機能が強化され、リスト内で追跡対象オブジェクトを組み合わせて設定したり、ブール ロジックを使用した柔軟性のある方法でオブジェクトを組み合わせたりすることができます。	*Configuring Enhanced Object Tracking*
12.3(4)T	FHRP：IP SLA 動作の拡張オブジェクト トラッキング	この機能により、FHRP およびその他の EOT クライアントが、IP SLA オブジェクトの出力を追跡し、提供された情報を使用してアクションを開始できます。	*Configuring Enhanced Object Tracking*
	HSRP バージョン 2	HSRP バージョン 2 機能は、今後の機能拡張に備え、HSRP バージョン 1 よりも機能を拡張するために導入されました。HSRP バージョン 2 のパケット形式は、バージョン 1 とは異なります。	*Configuring HSRP*
12.3(2)T	GLBP MD5 認証	MD5 認証は、代替となるプレーン テキスト認証スキームよりも高いセキュリティを実現します。	*Configuring GLBP*
	HSRP MD5 認証	HSRP MD5 認証機能は、マルチキャスト HSRP プロトコル パケットの HSRP 部分の MD5 ダイジェストを生成するように拡張されています。この機能により、セキュリティが強化され、HSRP スプーフィング ソフトウェアの脅威に対する保護が得られます。	*Configuring HSRP*
	VRRP オブジェクト トラッキング	VRRP オブジェクト トラッキング機能により VRRP の機能が拡張され、ルータ内の特定のオブジェクトを追跡して VRRP グループの仮想ルータのプライオリティ レベルを変更できるようになりました。	*Configuring VRRP*
12.2(15)T	拡張トラッキング サポート	拡張トラッキング サポート機能は、HSRP からトラッキング メカニズムを分離させて、独立したトラッキング プロセスを別途生成します。これにより、HSRP 以外の Cisco IOS プロセスがこのトラッキング プロセスを使用できます。この機能を使用すると、インターフェイスのラインプロトコル ステートに加えて他のオブジェクトも追跡できます。	*Configuring Enhanced Object Tracking*
	Gateway Load Balancing Protocol	GLBP は、冗長化されたルータ グループ間でパケットのロード シェアリングを行う一方、機能を停止したルータや回路（HSRP や VRRP など）からのデータ トラフィックを保護します。	*Configuring GLBP*
12.2(13)T	Virtual Router Redundancy Protocol	VRRP は、ルータのグループを使用して単一の仮想ルータを形成し、冗長性を実現します。これにより、仮想ルータをデフォルト ゲートウェイとして使用するように、LAN クライアントを設定できます。ルータのグループを表す仮想ルータは、「VRRP グループ」とも呼ばれます。	*Configuring VRRP*
12.2(11)T	HSRP：ホットスタンバイ ルータ プロトコルと IPSec	HSRP は、スタンバイ コマンドライン インターフェイス（CLI）コマンドを使用して LAN インターフェイス上に設定できます。インターフェイスから、ローカル IPsec ID またはローカル トンネル エンドポイントとしてスタンバイ IP アドレスを使用できます。	*IPsec VPN High Availability Enhancements*

表 1　サポート対象の FHRP 機能 （続き）

リリース	機能名	機能の説明	参照先
12.2(8)T	HSRP の MPLS VPN サポート	HSRP の Multiprotocol Label Switching（MPLS; マルチプロトコル ラベル スイッチング）Virtual Private Network（VPN; バーチャル プライベート ネットワーク）インターフェイス サポートが役に立つのは、次のいずれかの状態で 2 つの Provider Edge（PE; プロバイダー エッジ）ルータ間でイーサネット LAN が接続されている場合です。	*Configuring HSRP*
Cisco IOS Release 12.4T			
12.4(20)T	FHRP : **rtr** キーワードの EOT の廃止	この機能により、**track rtr** コマンドは **track ip sla** コマンドで置き換えられました。	*Configuring Enhanced Object Tracking*
12.4(15)T	GLBP クライアント キャッシュ	GLBP クライアント キャッシュには、GLBP グループをデフォルト ゲートウェイとして使用しているネットワーク ホストに関する情報が含まれています。GLBP クライアント キャッシュには、特定の GLBP グループを使用する各ホストの MAC アドレス、各ネットワーク ホストに割り当てられている GLBP フォワーダの数、GLBP グループの各フォワーダに現在割り当てられているネットワーク ホストの総数が格納されます。また、各ネットワーク ホストによって使用されるプロトコル アドレス、ホストとフォワーダの割り当てが最後に更新されてから経過した時間も格納されます。	*Configuring GLBP*
12.4(11)T	FHRP - HSRP BFD ピアリング	HSRP の BFD ピアリング機能により、HSRP グループ メンバーのヘルス モニタリング システムで Bidirectional Forwarding Detection（BFD; 双方向フォワーディング検出）を使用できるようになりました。以前は、グループ メンバーのモニタリングには、かなり大規模で、生成とチェックに CPU メモリを消費する HSRP マルチキャスト メッセージだけが利用されていました。単一のインターフェイスが大量のグループをホストするアーキテクチャでは、CPU メモリの消費量と処理のオーバーヘッドが少ないプロトコルが必要です。BFD によって、この問題が解消されているほか、CPU にあまり負担をかけずに 1 秒未満のヘルス モニタリング（ミリ秒単位の障害検出）が実現されています。	*Configuring HSRP*
	FHRP - Enhanced Object Tracking Support for Mobile IP	FHRP - Enhanced Object Tracking Support for Mobile IP 機能は、ルータ上の Home Agent、Gateway GPRS Support Node（GGSN; ゲートウェイ GPRS サポート ノード）、または Packet Data Serving Node（PDSN）トラフィックのプレゼンスを追跡するためにモバイル ワイヤレス アプリケーションが必要とする新しいトラッキング オブジェクトを提供します。	*Configuring Enhanced Object Tracking*

表 1　サポート対象の FHRP 機能 （続き）

リリース	機能名	機能の説明	参照先
12.4(9)T	EOT によるキャリア遅延サポート	EOT によるキャリア遅延サポート機能により、EOT はインターフェイスのステータスを追跡するときにキャリア遅延タイマーを考慮に入れることができます。	*Configuring Enhanced Object Tracking*
	FHRP - HSRP グループ シャットダウン	FHRP - HSRP グループ シャットダウン機能を使用すると、トラッキング対象のオブジェクトがダウンしたときに、HSRP グループのプライオリティを下げるのではなく、ディセーブルな状態になる（ステートが Init になる）ように HSRP グループを設定することができます。	*Configuring HSRP*
12.4(6)T	HSRP 複数グループ最適化	HSRP 複数グループ最適化機能により、サブインターフェイスで設定されている複数の HSRP グループのネゴシエーションとメンテナンス方法が改善されました。アクティブ ルータとスタンバイ ルータを選出するために物理インターフェイスに必要なのは、1 つの HSRP グループだけです。このグループが *マスター グループ*と呼ばれます。他の HSRP グループは、各サブインターフェイスに作成されたり、グループ名によってマスター グループとリンクされたりします。リンクされた HSRP グループは、*クライアント グループ*または*従属グループ*と呼ばれます。	*Configuring HSRP*
12.4(2)T	FHRP：拡張オブジェクト トラッキングと Embedded Event Manager	EOT が EEM と統合され、EEM は追跡対象オブジェクトのステータス変更を報告し、EOT は EEM オブジェクトを追跡できるようになりました。	*Configuring Enhanced Object Tracking*

表 1　サポート対象の FHRP 機能 （続き）

リリース	機能名	機能の説明	参照先
Cisco IOS XE 3.1.0SG			
Cisco IOS XE 3.1.0SG	拡張トラッキング サポート	拡張トラッキング サポート機能は、HSRP からトラッキング メカニズムを分離させて、独立したトラッキング プロセスを別途生成します。これにより、HSRP 以外の Cisco IOS プロセスがこのトラッキング プロセスを使用できます。この機能を使用すると、インターフェイスのラインプロトコル ステートに加えて他のオブジェクトも追跡できます。	*Configuring Enhanced Object Tracking*
	FHRP：オブジェクト追跡リスト	この機能によりトラッキング機能が強化され、リスト内で追跡対象オブジェクトを組み合わせて設定したり、ブール ロジックを使用した柔軟性のある方法でオブジェクトを組み合わせたりすることができます。	*Configuring Enhanced Object Tracking*
	Gateway Load-Balancing Protocol（GLBP; ゲートウェイ ロード バランシング プロトコル）	GLBP は、冗長化されたルータ グループ間でパケットのロード シェアリングを行う一方、機能を停止したルータや回路（HSRP や VRRP など）からのデータ トラフィックを保護します。	*Configuring GLBP*
	GLBP MD5 認証	MD5 認証は、代替となるプレーン テキスト認証スキームよりも高いセキュリティを実現します。	*Configuring GLBP*
	HSRP - ISSU	HSRP - In-Service Software Upgrade（ISSU; インサービス ソフトウェア アップグレード）機能により、HSRP で ISSU がサポートされています。 ISSU は、パケット転送を続行しながら、Cisco IOS ソフトウェアのアップデートや修正を行うことができるプロセスです。	*Configuring HSRP*
	HSRP MD5 認証	HSRP MD5 認証機能は、マルチキャスト HSRP プロトコル パケットの HSRP 部分の MD5 ダイジェストを生成するように拡張されています。この機能により、セキュリティが強化され、HSRP スプーフィング ソフトウェアの脅威に対する保護が得られます。	*Configuring HSRP*
	HSRP バージョン 2	HSRP バージョン 2 機能は、今後の機能拡張に備え、HSRP バージョン 1 よりも機能を拡張するために導入されました。HSRP バージョン 2 のパケット形式は、バージョン 1 とは異なります。	*Configuring HSRP*
	SSO - HSRP	SSO HSRP は、冗長な Route Processor（RP; ルート プロセッサ）を装備したルータが Stateful Switchover（SSO; ステートフル スイッチオーバー）用に設定されているときの HSRP の動作を変更します。ある RP がアクティブで、もう一方の RP がスタンバイになっているとき、アクティブ RP に障害が発生すると、SSO は処理を引き継ぐスタンバイ RP をイネーブルにします。	*Configuring HSRP*
	Virtual Router Redundancy Protocol	VRRP は、ルータのグループを使用して単一の仮想ルータを形成し、冗長性を実現します。これにより、仮想ルータをデフォルト ゲートウェイとして使用するように、LAN クライアントを設定できます。ルータのグループを表す仮想ルータは、「VRRP グループ」とも呼ばれます。	*Configuring VRRP*

表 1　サポート対象の FHRP 機能 （続き）

リリース	機能名	機能の説明	参照先
その他の Cisco IOS リリース			
12.1(3)T	HSRP の ICMP リダイレクト サポート	HSRP の ICMP リダイレクト サポート機能により、HSRP を使用して設定されているインターフェイスで ICMP リダイレクトが可能になっています。	*Configuring HSRP*
12.2(27)SBC	FHRP：IP SLA 動作の拡張オブジェクト トラッキング	FHRP : IP SLA 動作の拡張オブジェクト トラッキング機能では、FHRP およびその他の EOT クライアントが IP SLA オブジェクトからの出力を追跡し、提供された情報を使用してアクションを発生させることができます。	*Configuring Enhanced Object Tracking*
12.2(31)SGA	HSRP - ISSU	HSRP - In-Service Software Upgrade（ISSU; インサービス ソフトウェア アップグレード）機能により、HSRP で ISSU がサポートされています。 ISSU は、パケット転送を続行しながら、Cisco IOS ソフトウェアのアップデートや修正を行うことができるプロセスです。	*Configuring HSRP*

GLBP の設定

Gateway Load Balancing Protocol（GLBP; ゲートウェイ ロード バランシング プロトコル）は、Hot Standby Router Protocol（HSRP; ホット スタンバイ ルータ プロトコル）や Virtual Router Redundancy Protocol（VRRP; 仮想ルータ冗長プロトコル）のように、機能を停止したルータや回路からデータ トラフィックを保護します。このとき、冗長化されたルータのグループ間でパケットのロード シェアリングを行うことができます。

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、「GLBP の機能情報」（P.26）を参照してください。

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

この章の構成

GLBP の制約事項

Enhanced Object Tracking（EOT; 拡張オブジェクト トラッキング）はステートフル スイッチオーバー（SSO）を認識しないため、SSO モードで GLBP と併用することはできません。

GLBP の前提条件

GLBP を設定する前に、ルータが物理インターフェイス上で複数の MAC アドレスをサポートできることを確認します。設定している GLBP フォワーダごとに、追加の MAC アドレスが使用されます。

GLBP について

GLBP の概要

GLBP は、IEEE 802.3 LAN 上の単一のデフォルト ゲートウェイを使用して設定されている IP ホストの自動ルータ バックアップを提供します。LAN 上の複数のファーストホップ ルータを連結し、IP パケットの転送負荷を共有しながら単一の仮想ファーストホップ IP ルータを提供します。LAN 上にあるその他のルータは、冗長化された GLBP ルータとして動作できます。このルータは、既存のフォワーディング ルータが機能しなくなった場合にアクティブになります。

GLBP は、ユーザに対しては HSRP や VRRP と同様の機能を実行します。HSRP や VRRP では、仮想 IP アドレスを使用して設定されている仮想ルータ グループに複数のルータを参加させることができます。グループの仮想 IP アドレスに送信されたパケットを転送するアクティブ ルータとして、1 つのメンバが選択されます。グループ内の他のルータは、アクティブ ルータが機能を停止するまで冗長化されます。これらのスタンバイ ルータには、プロトコルが使用していない、未使用の帯域幅があります。1 つのルータ セットに複数の仮想ルータ グループを設定できますが、そのホストに設定するデフォルト ゲートウェイは異なるようにする必要があります。結果として、追加の管理上の負担がかかります。GLBP には、単一の仮想 IP アドレスと複数の仮想 MAC アドレスを使用して、複数のルータ（ゲートウェイ）上でのロード バランシングを提供するというメリットがあります。転送負荷は、GLBP グループ内のすべてのルータ間で共有されます。単一のルータだけで処理して、他のルータがアイドルのままになっているということはありません。各ホストは、同じ仮想 IP アドレスで設定され、仮想ルータ グループ内のすべてのルータが参加して

パケットの転送を行います。GLBP メンバは、Hello メッセージを使用して相互に通信します。このメッセージは 3 秒ごとにマルチキャスト アドレス 224.0.0.102、User Datagram Protocol（UDP; ユーザ データグラム プロトコル）ポート 3222（送信元と宛先）に送信されます。

GLBP アクティブ仮想ゲートウェイ

GLBP グループのメンバは、そのグループの Active Virtual Gateway（AVG; アクティブ仮想ゲートウェイ）となるゲートウェイを 1 つ選択します。他のグループ メンバは、AVG が使用できなくなった場合に AVG のバックアップを提供します。AVG の機能として、仮想 MAC アドレスを GLBP グループの各メンバに割り当てることが挙げられます。各ゲートウェイは、AVG によって割り当てられた仮想 MAC アドレスに送信されたパケットの転送を行います。これらのゲートウェイは仮想 MAC アドレスの「アクティブ仮想フォワーダ（AVF）」と呼ばれます。

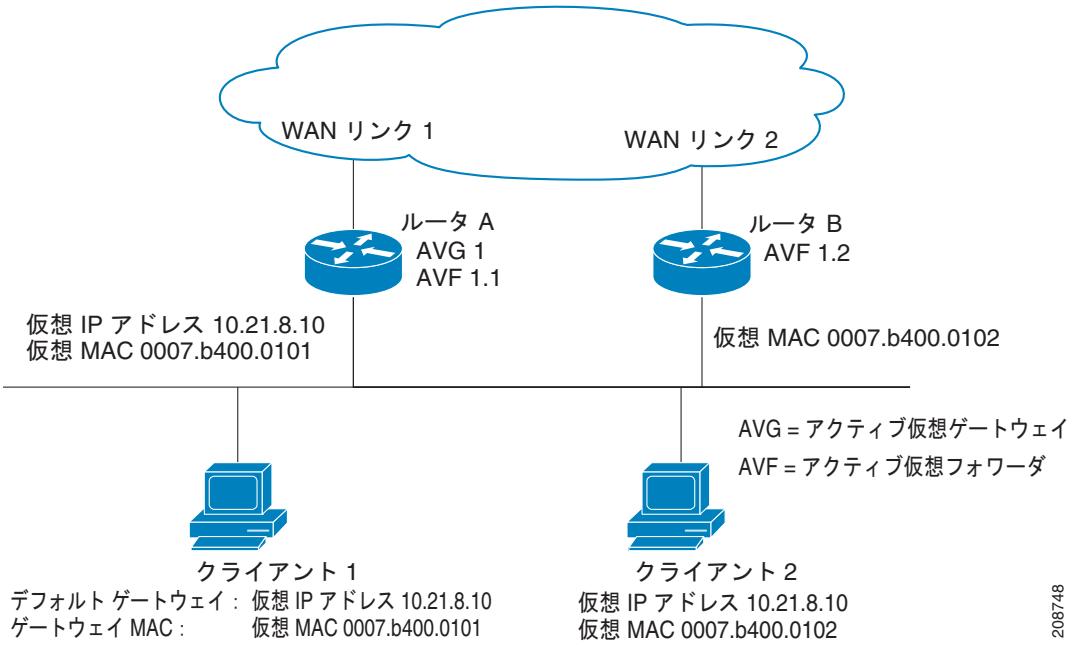
AVG は、仮想 IP アドレスの Address Resolution Protocol（ARP; アドレス解決プロトコル）要求への応答も行います。異なる仮想 MAC アドレスを使用して ARP 要求に応答することで、AVG によるロード シェアリングが実現します。

Cisco IOS Release 15.0(1)M1、12.4(24)T2、および 15.1(2)T よりも前のリリースでは、**no glbp load-balancing** コマンドが設定されている場合は、必ず、AVG がその AVF の MAC アドレスで ARP 要求に応答します。

Cisco IOS Release 15.0(1)M1、12.4(24)T2、および 15.1(2)T 以降のリリースでは、**no glbp load-balancing** コマンドが設定されている場合は、AVG が AVF を備えていなければ、先頭の VF の MAC アドレスで ARP 要求に応答します。そのため、その VF が現在の AVG に戻るまでは、トラフィックが別のゲートウェイ経由でルーティングされる可能性があります。

図 1 では、ルータ A は GLBP グループの AVG で、仮想 IP アドレス 10.21.8.10 に関する処理を行います。ルータ A は仮想 MAC アドレス 0007.b400.0101 の AVF でもあります。ルータ B は同じ GLBP グループのメンバで、仮想 MAC アドレス 0007.b400.0102 の AVF として指定されています。クライアント 1 のデフォルト ゲートウェイ IP アドレスは 10.21.8.10、ゲートウェイ MAC アドレスは 0007.b400.0101 です。クライアント 2 は、同じデフォルト ゲートウェイ IP アドレスを共有しますが、ゲートウェイ MAC アドレス 0007.b400.0102 を受信します。これは、ルータ B はルータ A とトラフィックの負荷を共有しているためです。

図 1　GLBP トポロジ



ルータ A が使用できなくなっても、クライアント 1 が WAN にアクセスできなくなることはありません。これは、ルータ B が、ルータ A の仮想 MAC アドレスに送信されたパケットの転送を行うためです。また、独自の仮想 MAC アドレスに送信されたパケットについても処理を実行します。ルータ B は、GLBP グループ全体で AVG のロールを担います。GLBP グループ内のルータが機能を停止しても、GLBP メンバ間の通信は継続されます。

GLBP 仮想 MAC アドレス割り当て

GLBP グループは、グループごとに最大 4 つの仮想 MAC アドレスを設定できます。グループの各メンバへの仮想 MAC アドレスの割り当ては、AVG が行います。他のグループ メンバは、Hello メッセージを通じて AVG を検出すると、仮想 MAC アドレスを要求します。ゲートウェイは、順番に、次の MAC アドレスを割り当てられます。AVG によって仮想 MAC アドレスが割り当てられた仮想フォワーダは、「プライマリ仮想フォワーダ」と呼ばれます。GLBP グループの他のメンバは、Hello メッセージから仮想 MAC アドレスを学習します。仮想 MAC アドレスを学習した仮想フォワーダは、「セカンダリ仮想フォワーダ」と呼ばれます。

GLBP 仮想ゲートウェイの冗長化

GLBP は、HSRP と同じ方法で仮想ゲートウェイの冗長化を行います。1 つのゲートウェイが AVG として選択され、別のゲートウェイがスタンバイ仮想ゲートウェイとして選択されます。残りのゲートウェイは、リスン ステートになります。

AVG の機能が停止すると、スタンバイ仮想ゲートウェイが該当する仮想 IP アドレスの処理を担当します。新しいスタンバイ仮想ゲートウェイは、リスン ステートにあるゲートウェイの中から選ばれます。

GLBP 仮想フォワーダの冗長化

仮想フォワーダの冗長化は、AVF で使用する仮想ゲートウェイの冗長化に類似しています。AVF の機能が停止すると、リスン ステートにあるセカンダリ仮想フォワーダの 1 つが、該当する仮想 MAC アドレスの処理を担当します。

新しい AVF は、別のフォワーダ番号のプライマリ仮想フォワーダにもなります。GLBP は、2 つのタイマーを使用して古いフォワーダ番号からホストを移行します。このタイマーは、ゲートウェイがアクティブ仮想フォワーダ状態になるとすぐに作動を開始します。GLBP は Hello メッセージを使用して、タイマーの現在の状態を伝えます。

AVG が継続して古い仮想フォワーダ MAC アドレスにホストをリダイレクトしている時間が、リダイレクト時間になります。リダイレクト時間が経過すると、AVG は ARP 応答で古い仮想フォワーダ MAC アドレスを使用するのを停止しますが、仮想フォワーダは、古い仮想フォワーダ MAC アドレスに送信されたパケットの転送を引き続き行います。

仮想フォワーダが有効である時間は、セカンダリ ホールド時間になります。セカンダリ ホールド時間が経過すると、GLBP グループのすべてのゲートウェイから仮想フォワーダが削除されます。期限の切れた仮想フォワーダ番号は、AVG によって再割り当てされるようになります。

GLBP ゲートウェイ プライオリティ

各 GLBP ゲートウェイが果たすロールと、AVG の機能が停止したときにどのようなことが発生するかについては、GLBP ゲートウェイ プライオリティによって決まります。

また、GLBP ルータがバックアップ仮想ゲートウェイとして機能するかどうかや、現在の AVG の機能が停止したときに AVG になる順序を決定するのもプライオリティです。**glbp priority** コマンドを使用して 1 ～ 255 の値を設定し、各バックアップ仮想ゲートウェイのプライオリティを設定できます。

図 1 では、ルータ A（LAN トポロジの AVG）の機能が停止すると、選択プロセスが行われ、処理を引き継ぐバックアップ仮想ゲートウェイが決定されます。この例では、グループ内の他のメンバはルータ B だけであるため、このルータが自動的に新しい AVG になります。同じ GLBP グループ内に別のルータが存在しており、そのルータにより高いプライオリティが設定されている場合は、高いプライオリティが設定されているそのルータが選択されます。両方のルータのプライオリティが同じである場合は、IP アドレスが大きい方のバックアップ仮想ゲートウェイが選択され、アクティブ仮想ゲートウェイになります。

デフォルトでは、GLBP 仮想ゲートウェイのプリエンプティブ スキームはディセーブルになっています。バックアップ仮想ゲートウェイが AVG になるのは、現在の AVG が機能を停止した場合だけです。この場合、仮想ゲートウェイに割り当てられているプライオリティは関係ありません。GLBP 仮想ゲートウェイ プリエンプティブ スキームをイネーブルにするには、**glbp preempt** コマンドを使用します。プリエンプションにより、バックアップ仮想ゲートウェイに現在の AVG よりも高いプライオリティが割り当てられている場合でも、バックアップ仮想ゲートウェイが AVG になることができます。

GLBP ゲートウェイの重み付けと追跡

GLBP は重み付けスキームを使用して、GLBP グループ内の各ルータの転送機能を指定できます。GLBP グループ内のルータに割り当てられている重み付けを使用して、そのルータがパケットを転送するかどうかを指定します。転送する場合は、パケット転送を行う LAN 上のホストの比率を指定します。GLBP グループの重み付けが特定の値を下回った場合は転送をディセーブルにするように、しきい値を設定できます。また、別のしきい値を上回ったときに転送を自動的に再度イネーブルにすることができます。

GLBP グループの重み付けは、ルータ内のインターフェイスのステートを追跡することで、自動的な調整が可能です。追跡対象のインターフェイスがダウンすると、GLBP グループの重み付けは指定された値の分だけ減じられます。別のインターフェイスを追跡して、GLBP の重み付けを減じることができます（減じる分量は変化させることができます）。

デフォルトでは、GLBP 仮想フォワーダ プリエンプティブ スキームは、30 秒遅延してイネーブルにされます。バックアップ仮想フォワーダは、現在の AVF の重み付けが 30 秒間にわたって低い重みしきい値を下回った場合に、AVF になることができます。GLBP フォワーダ プリエンプティブ スキームをディセーブルにするには、**no glbp forwarder preempt** コマンドを使用します。遅延時間を変更するには、**glbp forwarder preempt delay minimum** コマンドを使用します。

GLBP クライアント キャッシュ

GLBP クライアント キャッシュには、GLBP グループをデフォルト ゲートウェイとして使用しているネットワーク ホストに関する情報が含まれています。

GLBP グループの Active Virtual Gateway（AVG）が、ネットワーク ホストから GLBP 仮想 IP アドレスの IPv4 Address Resolution Protocol（ARP; アドレス解決プロトコル）要求または IPv6 Neighbor Discovery（ND; ネイバ ディスカバリ）要求を受け取ると、GLBP クライアント キャッシュに新しいエントリが作成されます。キャッシュ エントリには、ARP 要求または ND 要求を送信したホスト、および AVG が割り当てたフォワーダに関する情報が含まれています。

GLBP クライアント キャッシュには、特定の GLBP グループを使用する各ホストの MAC アドレス、各ネットワーク ホストに割り当てられている GLBP フォワーダの数、GLBP グループの各フォワーダに現在割り当てられているネットワーク ホストの総数が格納されます。また、各ネットワーク ホストによって使用されるプロトコル アドレス、ホストとフォワーダの割り当てが最後に更新されてから経過した時間も格納されます。

GLBP クライアント キャッシュに GLBP グループのネットワーク ホスト（最大 2000）に関する情報を格納することもできます。一般には、最大 1000 のネットワーク ホストが設定されることが想定されています。**glbp client-cache maximum** コマンドを使用すると、各 GLBP グループを使用するネットワーク ホストの数に基づいて、各 GLBP グループごとにキャッシュされるネットワーク ホストの最大数を低く設定することができます。このコマンドにより、GLBP グループごとに、使用されるキャッシュ メモリの分量を制限できます。GLBP クライアント キャッシュが設定されたクライアントの最大数に達しているときに、新しいクライアントを追加すると、最も長い間更新されていないクライアント エントリが破棄されます。このような状況に陥ることは、設定された上限が小さすぎることを示します。

GLBP クライアント キャッシュによって使用されるメモリの分量は、GLBP グループを使用するネットワーク ホスト（クライアント キャッシュがイネーブルになっているもの）の数に左右されます。各ホストには、少なくとも 20 バイトが必要です。GLBP グループごとに、追加で 3200 バイトが必要になります。

GLBP グループで現在 AVG のロールを果たしているルータで **show glbp detail** コマンドを使用すると、GLBP クライアント キャッシュの内容を表示できます。GLBP グループの別のルータで **show glbp detail** コマンドを発行すると、クライアント キャッシュ情報を参照するには、このコマンドを AVG 上で再発行するようにメッセージが表示されます。**show glbp detail** コマンドでは、GLBP クライアント キャッシュの使用状況、およびフォワーダ間でのクライアントの分散に関する統計情報も表示されます。キャッシュ タイムアウトとクライアント制限パラメータが適切に設定されていれば、正確な統計情報を得られます。ネットワーク上のエンド ホストの数が制限値を超えておらず、エンド ホストの最大 ARP キャッシュ タイムアウトが GLBP クライアント キャッシュ タイムアウトを超えていない場合は、値は適切であると言えます。

各 GLBP グループの GLBP クライアント キャッシュは、**glbp client-cache** コマンドを使用して個別にイネーブルまたはディセーブルに設定できます。デフォルトでは、GLBP クライアント キャッシュはディセーブルになっています。GLBP クライアント キャッシュをイネーブルに設定できるグループの数に制限はありません。

GLBP キャッシュ エントリは、**glbp client-cache maximum** コマンドに **timeout** キーワード オプションを指定して、指定時間が経過した後にタイムアウトするように設定できます。

GLBP MD5 認証

GLBP MD5 認証は、信頼性とセキュリティを向上させるために業界標準の MD5 アルゴリズムを採用しています。MD5 認証は、代替となるプレーン テキスト認証スキームよりも高いセキュリティを実現し、スプーフィング ソフトウェアから保護します。

MD5 認証を使用すると、各 GLBP グループ メンバが秘密キーを使用して、発信パケットの一部であるキー付き MD5 ハッシュを生成できます。着信パケットのキー付きハッシュが生成されると、生成されたハッシュと着信パケット内のハッシュが一致しない場合、パケットは無視されます。

MD5 ハッシュのキーは、キー ストリングを使用して設定内で直接指定することも、キー チェーンを通して間接的に指定することもできます。キー ストリングは 100 文字以下にする必要があります。

ルータは、GLBP グループと認証設定が異なるルータから届いた GLBP パケットを無視します。GLBP には、次の 3 つの認証スキームがあります。

- 認証なし
- プレーン テキスト認証
- MD5 認証

GLBP パケットは、次のいずれの場合も拒否されます。

- ルータと着信パケットの認証スキームが異なる。
- ルータと着信パケットの MD5 ダイジェストが異なる。
- ルータと着信パケットのテキスト認証文字列が異なる。

ISSU と GLBP

GLBP は In Service Software Upgrade（ISSU; インサービス ソフトウェア アップグレード）をサポートします。In Service Software Upgrade（ISSU）を使用すると、アクティブおよびスタンバイの Route Processor（RP; ルート プロセッサ）またはラインカード上で異なるバージョンの Cisco IOS ソフトウェアが実行されている場合でも、ハイアベイラビリティ（HA）システムをステートフル スイッチオーバー（SSO）モードで実行できるようになります。

ISSU は、サポートされる Cisco IOS リリースから別のリリースへアップグレードまたはダウングレードする機能を提供します。この場合、パケット転送は継続して行われ、セッションは維持されるため、予定されるシステムの停止時間を短くすることができます。アップグレードまたはダウングレードする機能は、アクティブ RP およびスタンバイ RP 上で異なるバージョンのソフトウェアを実行することで実現します。これにより、RP 間でステート情報を維持する時間が短くなります。この機能により、システムをアップグレード対象（またはダウングレード対象）のソフトウェアを実行するセカンダリ RP に切り替えることができ、セッションを切断することなく、またパケットの損失も最小限に抑えながら、継続してパケットを転送できます。この機能は、デフォルトでイネーブルにされています。

ISSU の詳細については、次の URL に掲載されている『*Cisco IOS In Service Software Upgrade Process*』を参照してください。

http://www.cisco.com/en/US/docs/ios/ha/configuration/guide/ha-inserv_updg.html

7600 シリーズ ルータでの ISSU の詳細については、次の URL に掲載されている『*ISSU and eFSU on Cisco 7600 Series Routers*』を参照してください。

http://www.cisco.com/en/US/docs/routers/7600/ios/12.2SR/configuration/guide/efsuovrw.html

GLBP SSO

GLBP SSO 機能が導入されたため、GLBP はステートフル スイッチオーバー（SSO）を認識するようになりました。GLBP は、ルータがセカンダリ RP にフェールオーバーしたことを検出し、グループの現在の状態を継続することができます。

SSO は、デュアル RP をサポートするネットワーキングデバイス（通常はエッジ デバイス）で機能します。1 台の RP をアクティブ プロセッサとして設定し、他の RP をスタンバイ プロセッサとして設定することで、RP 冗長化を実現します。また、RP 間の重要なステート情報を同期するため、ネットワーク ステート情報は RP 間でダイナミックに維持されます。

GLBP が SSO を認識する前に、RP が冗長化されたルータに GLBP を展開した場合、アクティブ RP とスタンバイ RP 間のロールがスイッチオーバーされると、ルータの GLBP グループ メンバとしてのアクティビティは破棄され、ルータはリロードされた場合と同様にグループに再び参加することになります。GLBP SSO 機能により、スイッチオーバーが行われても、GLBP は継続してグループ メンバとしてのアクティビティを継続できます。冗長化された RP 間の GLBP ステート情報は維持されるため、スタンバイ RP はスイッチオーバーの実行中も実行後も GLBP 内で引き続きルータのアクティビティを実行できます。

この機能は、デフォルトでイネーブルにされています。この機能をディセーブルにするには、グローバル コンフィギュレーション モードで **no glbp sso** コマンドを使用します。

詳細については、『*Stateful Switchover*』を参照してください。

GLBP の利点

ロード シェアリング

LAN クライアントからのトラフィックを複数のルータで共有するように GLBP を設定できるため、利用可能なルータ間でより公平にトラフィックの負荷を共有できます。

複数の仮想ルータ

GLBP は、ルータの物理インターフェイスごとに、最大 1024 台の仮想ルータ（GLBP グループ）をサポートします。また、グループごとに最大 4 つの仮想フォワーダをサポートします。

プリエンプション

GLBP の冗長性スキームにより、アクティブ仮想ゲートウェイのプリエンプトが可能になり、より高いプライオリティが設定されたバックアップ仮想ゲートウェイを利用できるようになります。フォワーダ プリエンプションも同様に動作しますが、フォワーダ プリエンプションではプライオリティではなく重み付けを使用する点が異なります。また、フォワーダ プリエンプションはデフォルトでイネーブルになっています。

認証

信頼性やセキュリティを向上させて GLBP スプーフィング ソフトウェアからの保護を強化するため、業界標準の Message Digest 5（MD5; メッセージ ダイジェスト 5）アルゴリズムを使用することもできます。GLBP グループ内で、他のルータとは異なる認証文字列を使用するルータは、他のグループ メンバに無視されます。別の方法として、GLBP グループ メンバ間で簡易テキスト パスワード認証スキームを使用して、設定エラーを検出することもできます。

GLBP の設定方法

GLBP のイネーブル化と確認

インターフェイス上で GLBP をイネーブルにし、設定と操作を確認するには、次の手順を実行します。GLBP グループ内の各ゲートウェイは、同じグループ番号を使用して設定する必要があります。また、GLBP グループ内の少なくとも 1 つのゲートウェイは、そのグループで使う仮想 IP アドレスを使用して設定しなければなりません。その他、必要となるすべてのパラメータは学習することができます。

前提条件

インターフェイスで VLAN を使用している場合、GLBP のグループ番号は VLAN ごとに異なる番号を使用する必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip address** *ip-address mask* [**secondary**]
5. **glbp** *group* **ip** [*ip-address* [**secondary**]]
6. **exit**
7. **show glbp** [*interface-type interface-number*] [*group*] [*state*] [**brief**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**interface** *type number* **例：** `Router(config)# interface fastethernet 0/0`	インターフェイス タイプおよび番号を指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ip address** *ip-address mask* [**secondary**] **例：** `Router(config-if)# ip address 10.21.8.32 255.255.255.0`	インターフェイスのプライマリ IP アドレスまたはセカンダリ IP アドレスを指定します。
ステップ 5	**glbp** *group* **ip** [*ip-address* [**secondary**]] **例：** `Router(config-if)# glbp 10 ip 10.21.8.10`	インターフェイス上で GLBP をイネーブルにし、仮想ゲートウェイのプライマリ IP アドレスを指定します。 • プライマリ IP アドレスを指定すると、もう一度 **glbp** *group* **ip** コマンドを **secondary** キーワードとともに使用して、このグループでサポートする追加の IP アドレスを指定できます。
ステップ 6	**exit** **例：** `Router(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了し、ルータをグローバル コンフィギュレーション モードに戻します。
ステップ 7	**show glbp** [*interface-type interface-number*] [*group*] [*state*] [**brief**] **例：** `Router(config)# show glbp 10`	（任意）ルータの GLBP グループに関する情報を表示します。 • オプションの **brief** キーワードを使用すると、各仮想ゲートウェイまたは仮想フォワーダに関する情報が 1 行で表示されます。 • 「例」で、このタスクのコマンド出力を参照してください。

例

次に、ルータ上の GLBP グループ 10 のステータスに関する出力例を示します。

```
Router# show glbp 10

FastEthernet0/0 - Group 10
  State is Active
    2 state changes, last state change 23:50:33
  Virtual IP address is 10.21.8.10
  Hello time 5 sec, hold time 18 sec
    Next hello sent in 4.300 secs
  Redirect time 1800 sec, forwarder time-out 28800 sec
  Authentication text, string "authword"
  Preemption enabled, min delay 60 sec
  Active is local
  Standby is unknown
  Priority 254 (configured)
  Weighting 105 (configured 110), thresholds: lower 95, upper 105
    Track object 2 state Down decrement 5
  Load balancing: host-dependent
  There is 1 forwarder (1 active)
  Forwarder 1
    State is Active
```

```
  1 state change, last state change 23:50:15
MAC address is 0007.b400.0101 (default)
Owner ID is 0005.0050.6c08
Redirection enabled
Preemption enabled, min delay 60 sec
Active is local, weighting 105
```

GLBP のカスタマイズ

GLBP の動作のカスタマイズはオプションです。GLBP グループをイネーブルにするとすぐに、そのグループは動作を開始することに注意してください。GLBP をカスタマイズする前に GLBP グループをイネーブルにすると、ルータがグループの制御を引き継ぎ、機能のカスタマイズを完了する前に AVG になることがあります。このため、GLBP をカスタマイズする場合には、カスタマイズを行ってから GLBP をイネーブルにすることを推奨します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip address** *ip-address mask* [**secondary**]
5. **glbp** *group* **timers** [**msec**] *hellotime* [**msec**] *holdtime*
6. **glbp** *group* **timers redirect** *redirect timeout*
7. **glbp** *group* **load-balancing** [**host-dependent** | **round-robin** | **weighted**]
8. **glbp** *group* **priority** *level*
9. **glbp** *group* **preempt** [**delay minimum** *seconds*]
10. **glbp** *group* **client-cache maximum** *number* [**timeout** *minutes*]
11. **glbp** *group* **name** *redundancy-name*
12. **exit**
13. **no glbp sso**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* 例： `Router(config)# interface fastethernet 0/0`	インターフェイス タイプおよび番号を指定し、インターフェイス コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	**ip address** *ip-address mask* [**secondary**] **例：** `Router(config-if)# ip address 10.21.8.32 255.255.255.0`	インターフェイスのプライマリ IP アドレスまたはセカンダリ IP アドレスを指定します。
ステップ 5	**glbp** *group* **timers** [**msec**] *hellotime* [**msec**] *holdtime* **例：** `Router(config-if)# glbp 10 timers 5 18`	GLBP グループで AVG が連続して送信する hello パケットの間隔を設定します。 • *holdtime* 引数を使用して、hello パケット内の仮想ゲートウェイおよび仮想フォワーダ情報が有効と見なされるまでのインターバル（秒）を指定します。 • オプションの **msec** キーワードを指定すると、引数の単位は（デフォルトの秒ではなく）ミリ秒を表すことになります。
ステップ 6	**glbp** *group* **timers redirect** *redirect timeout* **例：** `Router(config-if)# glbp 10 timers redirect 1800 28800`	AVG が継続してクライアントを AVF にリダイレクトする時間間隔を設定します。デフォルトは 600 秒（10 分）です。 • *timeout* 引数は、セカンダリ仮想フォワーダが無効になるまでのインターバル（秒）を指定します。デフォルトは 14,400 秒（4 時間）です。 **（注）** *redirect* 引数のゼロ（0）値は、指定できる値の範囲から除外することはできません。Cisco IOS ソフトウェアの事前設定でゼロ（0）値を使用しているため、アップグレードに悪影響を及ぼすことになります。ただし、ゼロ（0）値に設定することは推奨しません。この値を使用すると、リダイレクト タイマーが期限切れになりません。リダイレクト タイマーが期限切れにならないと、ルータが機能を停止したときに、バックアップにリダイレクトされず、機能を停止したルータに割り当てられている新しいホストが継続して動作します。
ステップ 7	**glbp** *group* **load-balancing** [**host-dependent** | **round-robin** | **weighted**] **例：** `Router(config-if)# glbp 10 load-balancing host-dependent`	GLBP AVG で採用するロード バランシングの方法を指定します。
ステップ 8	**glbp** *group* **priority** *level* **例：** `Router(config-if)# glbp 10 priority 254`	GLBP グループ内のゲートウェイのプライオリティ レベルを設定します。 • デフォルト値は 100 です。
ステップ 9	**glbp** *group* **preempt** [**delay minimum** *seconds*] **例：** `Router(config-if)# glbp 10 preempt delay minimum 60`	現在の AVG よりも高いプライオリティが設定されている場合、GLBP グループの AVG として引き継ぐルータを指定します。 • このコマンドは、デフォルトでディセーブルになっています。 • オプションの **delay** キーワードと **minimum** キーワード、および *seconds* 引数を使用して、AVG のプリエンプションが発生するまでの最小遅延時間（秒）を指定します。

	コマンドまたはアクション	目的
ステップ 10	**glbp** *group* **client-cache maximum** *number* [**timeout** *minutes*] 例： `Router(config-if)# glbp 10 client-cache maximum 1200 timeout 245`	（任意）GLBP クライアント キャッシュをイネーブルにします。 • このコマンドは、デフォルトでディセーブルになっています。 • *number* 引数を使用して、キャッシュがこの GLBP グループのためにホールドするクライアントの最大数を指定します。範囲は 8 ～ 2000 です。 • オプションの **timeout** *minutes* キーワードと引数のペアを使用して、クライアント情報が最後に更新されてから、クライアント エントリが GLBP クライアント キャッシュに保管される最大時間を設定します。範囲は、1 ～ 1440 分（1 日）です。 **（注）** IPv4 ネットワークでは、最大限に予測されるエンド ホストの Address Resolution Protocol（ARP; アドレス解決プロトコル）キャッシュ タイムアウト値よりもやや長い GLBP クライアント キャッシュ タイムアウト値を設定することを推奨します。
ステップ 11	**glbp** *group* **name** *redundancy-name* 例： `Router(config-if)# glbp 10 name abcompany`	GLBP グループに名前を割り当てることで、IP 冗長性をイネーブルにします。 • GLBP が冗長化されたクライアントは、同じ GLBP グループ名を使用して設定する必要があります。このようにすることで、冗長化されたクライアントと GLBP グループを接続できます。
ステップ 12	**exit** 例： `Router(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了し、ルータをグローバル コンフィギュレーション モードに戻します。
ステップ 13	**no glbp sso** 例： `Router(config)# no glbp sso`	（任意）SSO の GLBP サポートをディセーブルにします。

キー ストリングを使用した GLBP MD5 認証の設定

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip address** *ip-address mask* [**secondary**]
5. **glbp** *group-number* **authentication md5 key-string** [**0** | **7**] *key*
6. **glbp** *group-number* **ip** [*ip-address* [**secondary**]]
7. 通信を行う各ルータ上でステップ 1 ～ 6 を繰り返します。
8. **end**
9. **show glbp**

手順の詳細

	コマンド	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* **例：** `Router(config)# interface Ethernet0/1`	インターフェイス タイプを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ip address** *ip-address mask* [**secondary**] **例：** `Router(config-if)# ip address 10.0.0.1 255.255.255.0`	インターフェイスのプライマリ IP アドレスまたはセカンダリ IP アドレスを指定します。
ステップ 5	**glbp** *group-number* **authentication md5 key-string** [**0** | **7**] *key* **例：** `Router(config-if)# glbp 1 authentication md5 key-string d00b4r987654321a`	GLBP MD5 認証の認証キーを設定します。 • キー ストリングは 100 文字以下にする必要があります。 • *key* 引数にはプレフィクスを指定しません。**0** を指定すると、キーは暗号化されていないことを示します。 • **7** を指定すると、キーは暗号化されていることを示します。**service password-encryption** グローバル コンフィギュレーション コマンドがイネーブルになっていると、key-string 認証キーは自動的に暗号化されます。
ステップ 6	**glbp** *group-number* **ip** [*ip-address* [**secondary**]] **例：** `Router(config-if)# glbp 1 ip 10.0.0.10`	インターフェイス上で GLBP をイネーブルにし、仮想ゲートウェイのプライマリ IP アドレスを指定します。
ステップ 7	通信を行う各ルータ上でステップ 1 ～ 6 を繰り返します。	—
ステップ 8	**end** **例：** `Router(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 9	**show glbp** **例：** `Router# show glbp`	（任意）GLBP 情報を表示します。 • このコマンドを使用して、設定を確認します。キー ストリングと認証タイプは、設定されている場合に表示されます。

キー チェーンを使用した GLBP MD5 認証の設定

キー チェーンを使用して GLBP MD5 認証を設定するには、次の手順を実行します。キー チェーンを使用すると、キー チェーンの設定に基づき、場合に応じて異なるキー ストリングを使用できます。GLBP は適切なキー チェーンを照会し、特定のキー チェーンに対して現在アクティブになっているキーとキー ID を取得します。

手順の概要

1. **enable**
2. **configure terminal**
3. **key chain** *name-of-chain*
4. **key** *key-id*
5. **key-string** *string*
6. **exit**
7. exit
8. **interface** *type number*
9. **ip address** *ip-address mask* [**secondary**]
10. **glbp** *group-number* **authentication md5 key-chain** *name-of-chain*
11. **glbp** *group-number* **ip** [*ip-address* [**secondary**]]
12. 通信を行う各ルータ上でステップ 1 ～ 10 を繰り返します。
13. **end**
14. **show glbp**
15. **show key chain**

手順の詳細

	コマンド	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードなど、高位の権限レベルをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**key chain** *name-of-chain* 例： `Router(config)# key chain glbp2`	ルーティング プロトコルの認証をイネーブルにし、認証キーのグループを識別します。
ステップ 4	**key** *key-id* 例： `Router(config-keychain)# key 100`	キー チェーンの認証キーを識別します。 • *key-id* は、数値で指定する必要があります。

	コマンド	目的
ステップ 5	**key-string** *string* **例：** `Router(config-keychain-key)# key-string xmen382`	キーの認証文字列を指定します。 • *string* には、1 ～ 80 文字の大文字と小文字の英数字を指定できます。ただし、最初の文字を数値にすることはできません。
ステップ 6	**exit** **例：** `Router(config-keychain-key)# exit`	キーチェーン コンフィギュレーション モードに戻ります。
ステップ 7	**exit** **例：** `Router(config-keychain)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 8	**interface** *type number* **例：** `Router(config)# interface Ethernet0/1`	インターフェイス タイプを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 9	**ip address** *ip-address mask* [**secondary**] **例：** `Router(config-if)# ip address 10.21.0.1 255.255.255.0`	インターフェイスのプライマリ IP アドレスまたはセカンダリ IP アドレスを指定します。
ステップ 10	**glbp** *group-number* **authentication md5 key-chain** *name-of-chain* **例：** `Router(config-if)# glbp 1 authentication md5 key-chain glbp2`	GLBP MD5 認証の認証 MD5 キー チェーンを設定します。 • キー チェーン名は、ステップ 3 で指定した名前と一致する必要があります。
ステップ 11	**glbp** *group-number* **ip** [*ip-address* [**secondary**]] **例：** `Router(config-if)# glbp 1 ip 10.21.0.12`	インターフェイス上で GLBP をイネーブルにし、仮想ゲートウェイのプライマリ IP アドレスを指定します。
ステップ 12	通信を行う各ルータ上でステップ 1 ～ 10 を繰り返します。	—
ステップ 13	**end** **例：** `Router(config-if)# end`	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 14	**show glbp** 例： `Router# show glbp`	（任意）GLBP 情報を表示します。 • このコマンドを使用して、設定を確認します。キー チェーンと認証タイプは、設定されている場合に表示されます。
ステップ 15	**show key chain** 例： `Router# show key chain`	（任意）認証キー情報を表示します。

GLBP テキスト認証の設定

この認証方法では、最小限のセキュリティが提供されます。高いセキュリティが必要な場合は、MD5 認証を使用してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip address** *ip-address mask* [**secondary**]
5. **glbp** *group-number* **authentication text** *string*
6. **glbp** *group-number* **ip** [*ip-address* [**secondary**]]
7. 通信を行う各ルータ上でステップ 1 ～ 6 を繰り返します。
8. **end**
9. **show glbp**

手順の詳細

	コマンド	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードなど、高位の権限レベルをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* 例： `Router(config)# interface Ethernet0/1`	インターフェイス タイプを設定し、インターフェイス コンフィギュレーション モードを開始します。

	コマンド	目的
ステップ 4	**ip address** *ip-address mask* [**secondary**] **例：** `Router(config-if)# ip address 10.0.0.1 255.255.255.0`	インターフェイスのプライマリ IP アドレスまたはセカンダリ IP アドレスを指定します。
ステップ 5	**glbp** *group-number* **authentication text** *string* **例：** `Router(config-if)# glbp 10 authentication text stringxyz`	グループ内の他のルータから受信した GLBP パケットを認証します。 • 認証を設定する場合、GLBP グループ内のすべてのルータで同じ認証文字列を使用する必要があります。
ステップ 6	**glbp** *group-number* **ip** [*ip-address* [**secondary**]] **例：** `Router(config-if)# glbp 1 ip 10.0.0.10`	インターフェイス上で GLBP をイネーブルにし、仮想ゲートウェイのプライマリ IP アドレスを指定します。
ステップ 7	通信を行う各ルータ上でステップ 1 ～ 6 を繰り返します。	—
ステップ 8	**end** **例：** `Router(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 9	**show glbp** **例：** `Router# show glbp`	（任意）GLBP 情報を表示します。 • このコマンドを使用して、設定を確認します。

GLBP 重み値とオブジェクト トラッキングの設定

GLBP 重み値とオブジェクト トラッキングを設定するには、次の手順を実行します。

GLBP 重み付けにより、GLBP グループが仮想フォワーダとして動作できるかどうかが決定されます。初期の重み値は設定可能で、オプションでしきい値を指定できます。インターフェイス ステートの追跡が可能で、インターフェイスがダウンした場合に重み値を減らすように設定できます。GLBP グループの重み付けが指定の値を下回ると、グループがアクティブ仮想フォワーダになることはありません。重み付けが指定の値を上回ると、グループは再びアクティブ仮想フォワーダとしてのロールを実行できるようになります。

手順の概要

1. **enable**
2. **configure terminal**
3. **track** *object-number* **interface** *type number* {**line-protocol** | **ip routing**}
4. **exit**
5. **interface** *type number*
6. **glbp** *group* **weighting** *maximum* [**lower** *lower*] [**upper** *upper*]
7. **glbp** *group* **weighting track** *object-number* [**decrement** *value*]
8. **glbp** *group* **forwarder preempt** [**delay minimum** *seconds*]
9. **end**
10. **show track** [*object-number* | **brief**] [**interface** [**brief**] | **ip route** [**brief**] | **resolution** | **timers**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**track** *object-number* **interface** *type number* {**line-protocol** | **ip routing**} 例： `Router(config)# track 2 interface POS 6/0 ip routing`	インターフェイスを追跡し、インターフェイスのステートに変更が生じるとGLBP ゲートウェイの重み付けを変更して、トラッキング コンフィギュレーション モードを開始するように設定します。 • このコマンドを使って、**glbp weighting track** コマンドで使用されるインターフェイスおよび対応するオブジェクト番号を設定します。 • **line-protocol** キーワードは、インターフェイスがアップしているかどうかを追跡します。**ip routing** キーワードは、インターフェイス上で IP ルーティングがイネーブルになっており、IP アドレスが設定されていることを確認します。
ステップ 4	**exit** 例： `Router(config-track)# exit`	グローバル コンフィギュレーション モードに戻ります。

	コマンドまたはアクション	目的
ステップ 5	**interface** *type number* **例：** `Router(config)# interface fastethernet 0/0`	インターフェイス コンフィギュレーション モードを開始します。
ステップ 6	**glbp** *group* **weighting** *maximum* [**lower** *lower*] [**upper** *upper*] **例：** `Router(config-if)# glbp 10 weighting 110 lower 95 upper 105`	GLBP ゲートウェイの初期の重み値、上限しきい値、および下限しきい値を指定します。
ステップ 7	**glbp** *group* **weighting track** *object-number* [**decrement** *value*] **例：** `Router(config-if)# glbp 10 weighting track 2 decrement 5`	GLBP ゲートウェイの重み付けに影響を与える、追跡対象のオブジェクトを指定します。 • *value* 引数により、追跡対象オブジェクトが機能を停止した場合に、GLBP ゲートウェイの重み付けで減じる値を指定します。
ステップ 8	**glbp** *group* **forwarder preempt** [**delay minimum** *seconds*] **例：** `Router(config-if)# glbp 10 forwarder preempt delay minimum 60`	GLBP グループの現在の AVF の値が重みしきい値よりも低くなった場合に、GLBP グループの AVF としてのロールを引き継ぐルータを設定します。 • このコマンドはデフォルトでイネーブルに設定され、30 秒遅延するようになっています。 • オプションの **delay** キーワードと **minimum** キーワード、および *seconds* 引数を使用して、AVF のプリエンプションが発生するまでの最小遅延時間（秒）を指定します。
ステップ 9	**end** **例：** `Router(config-if)# exit`	特権 EXEC モードに戻ります。
ステップ 10	**show track** [*object-number* | **brief**] [**interface** [**brief**]| **ip route** [**brief**] | **resolution** | **timers**] **例：** `Router# show track 2`	トラッキング情報を表示します。

GLBP のトラブルシューティング

GLBP には、GLBP の動作に関連するさまざまなイベントについての診断内容をコンソールに表示できるように、5 つの特権 EXEC モード コマンドが導入されています。**debug condition glbp**、**debug glbp errors**、**debug glbp events**、**debug glbp packets**、および **debug glbp terse** コマンドを使用すると、大量の情報が出力され、ルータのパフォーマンスが著しく低下するため、これらのコマンドはトラブルシューティングを行うときにのみ使用するようにしてください。**debug glbp** コマンドを使用したときの影響を最小限に抑えるには、次の手順を実行します。

この手順により、コンソール ポートが文字単位のプロセッサ割り込みを行わなくなるため、**debug condition glbp** コマンドまたは **debug glbp** コマンドを使用することでルータにかかる負荷が最小限に抑えられます。コンソールに直接接続できない場合は、ターミナル サーバ経由でこの手順を実行できます。ただし、Telnet 接続を切断しなければならない場合は、デバッグ出力の生成でプロセッサに負荷がかかりルータが応答できないことに起因して、再接続できないことがあります。

前提条件

この手順を実行するには、GLBP を実行しているルータがコンソールに直接接続されている必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **no logging console**
4. Telnet を使用してルータ ポートにアクセスし、ステップ 1 および 2 を繰り返します。
5. **end**
6. **terminal monitor**
7. **debug condition glbp** *interface-type interface-number group* [*forwarder*]
8. **terminal no monitor**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**no logging console** 例： `Router(config)# no logging console`	コンソール ターミナルへのロギングをすべてディセーブルにします。 • コンソールへのロギングを再びイネーブルにするには、グローバル コンフィギュレーション モードで **logging console** コマンドを使用します。

	コマンドまたはアクション	目的
ステップ 4	Telnet を使用してルータ ポートにアクセスし、ステップ 1 および 2 を繰り返します。	再帰的 Telnet セッションでグローバル コンフィギュレーション モードを開始します。これにより、出力をコンソール ポートからリダイレクトできるようになります。
ステップ 5	**end** **例：** `Router(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**terminal monitor** **例：** `Router# terminal monitor`	仮想端末でのロギング出力をイネーブルにします。
ステップ 7	**debug condition glbp** *interface-type interface-number group* [*forwarder*] **例：** `Router# debug condition glbp fastethernet 0/0 10 1`	GLBP 状態についてのデバッグ メッセージを表示します。 • 特定の **debug condition glbp** コマンドまたは **debug glbp** コマンドのみを入力し、特定のサブコンポーネントに対する出力を分離してプロセッサにかかる負荷を最小限に抑えるようにします。適切な引数とキーワードを使用し、特定のサブコンポーネントについての詳細なデバッグ情報を生成します。 • 完了したら、特定の **no debug condition glbp** コマンドまたは **no debug glbp** コマンドを入力します。
ステップ 8	**terminal no monitor** **例：** `Router# terminal no monitor`	仮想端末でのロギング出力をディセーブルにします。

GLBP の設定例

例：GLBP 設定のカスタマイズ

次に、図 1 に示すルータ A を設定する例を示します。

```
Router(config)# interface fastethernet 0/0
Router(config-if)# ip address 10.21.8.32 255.255.255.0
Router(config-if)# glbp 10 timers 5 18
Router(config-if)# glbp 10 timers redirect 1800 28800
Router(config-if)# glbp 10 load-balancing host-dependent
Router(config-if)# glbp 10 priority 254
Router(config-if)# glbp 10 preempt delay minimum 60
Router(config-if)# glbp 10 client-cache maximum 1200 timeout 245
```

例：キー ストリングを使用した GLBP MD5 認証の設定

次に、キー ストリングを使用して GLBP MD5 認証を設定する例を示します。

```
Router(config)# interface Ethernet0/1
Router(config-if)# ip address 10.0.0.1 255.255.255.0
Router(config-if)# glbp 2 authentication md5 key-string ThisStringIsTheSecretKey
Router(config-if)# glbp 2 ip 10.0.0.10
```

例：キー チェーンを使用した GLBP MD5 認証の設定

次の例では、特定のキー チェーンに対して現在アクティブになっているキーとキー ID を取得するため、GLBP にはキー チェーン「AuthenticateGLBP」が必要です。

```
Router(config)# key chain AuthenticateGLBP
Router(config-keychain)# key 1
Router(config-keychain-key)# key-string ThisIsASecretKey
Router(config-keychain-key)# exit
Router(config-keychain)# exit
Router(config)# interface Ethernet0/1
Router(config-if)# ip address 10.0.0.1 255.255.255.0
Router(config-if)# glbp 2 authentication md5 key-chain AuthenticateGLBP
Router(config-if)# glbp 2 ip 10.0.0.10
```

例：GLBP テキスト認証の設定

次に、テキスト ストリングを使用して GLBP テキスト認証を設定する例を示します。

```
Router(config)# interface fastethernet 0/0
Router(config-if)# ip address 10.21.8.32 255.255.255.0
Router(config-if)# glbp 10 authentication text stringxyz
Router(config-if)# glbp 10 ip 10.21.8.10
```

例：GLBP 重み付けの設定

次の例では、図 1 のルータ A は POS インターフェイス 5/0 および 6/0 の IP ルーティング ステートを追跡するように設定されています。初期の GLBP 重み付けについては、上限しきい値と下限しきい値が設定され、重み付けは 10 ずつ減じるように設定されています。POS インターフェイス 5/0 および 6/0 がダウンすると、ルータの重み値が減じられます。

```
Router(config)# track 1 interface POS 5/0 ip routing
Router(config)# track 2 interface POS 6/0 ip routing
Router(config)# interface fastethernet 0/0
Router(config-if)# glbp 10 weighting 110 lower 95 upper 105
Router(config-if)# glbp 10 weighting track 1 decrement 10
Router(config-if)# glbp 10 weighting track 2 decrement 10
Router(config-if)# glbp 10 forwarder preempt delay minimum 60
```

例：GLBP 設定のイネーブル化

次の例では、図 1 のルータ A は GLBP をイネーブルにするように設定されています。GLBP グループ 10 には、仮想 IP アドレス 10.21.8.10 が指定されています。

```
Router(config)# interface fastethernet 0/0
Router(config-if)# ip address 10.21.8.32 255.255.255.0
Router(config-if)# glbp 10 ip 10.21.8.10
```

その他の参考資料

関連資料

内容	参照先
GLBP コマンド：コマンド構文、コマンド モード、コマンド履歴、デフォルト設定、使用に関する注意事項および例	『*Cisco IOS IP Application Services Command Reference*』
In Service Software Upgrade（ISSU; インサービス ソフトウェア アップグレード）の設定	「Cisco IOS In Service Software Upgrade Process」モジュール
キー チェーンおよびキー管理用コマンド：コマンド構文の詳細、コマンド モード、コマンド履歴、デフォルト設定、使用に関する注意事項、および例	『*Cisco IOS IP Routing : RIP Command Reference*』
オブジェクト トラッキング	「Configuring Enhanced Object Tracking」モジュール
ステートフル スイッチオーバー	「Stateful Switchover」モジュール
VRRP	「Configuring VRRP」モジュール
HSRP	「Configuring HSRP」モジュール

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
この機能がサポートする新しい MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択されたプラットフォーム、シスコ ソフトウェア リリース、およびフィーチャ セットの MIB を検索してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
この機能がサポートする新規 RFC または改訂 RFC はありません。また、この機能による既存 RFC のサポートに変更はありません。	—

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。以下を含むさまざまな作業にこの Web サイトが役立ちます。 ・テクニカル サポートを受ける ・ソフトウェアをダウンロードする ・セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける ・ツールおよびリソースへアクセスする - Product Alert の受信登録 - Field Notice の受信登録 - Bug Toolkit を使用した既知の問題の検索 ・Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する ・トレーニング リソースへアクセスする ・TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

GLBP の機能情報

表 1 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。

プラットフォーム サポートとソフトウェア イメージ サポートに関する情報を入手するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator を使用すると、特定のソフトウェア リリース、フィーチャ セット、またはプラットフォームをサポートするソフトウェア イメージを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 表 1 に、特定のソフトウェア リリース トレイン内の機能に対するサポートが導入されたソフトウェア リリースだけを示します。特に断りのないかぎり、そのソフトウェア リリース トレイン以降のリリースでもその機能がサポートされます。

表 1　GLBP の機能情報

機能名	リリース	機能設定情報
Gateway Load Balancing Protocol	Cisco IOS XE 3.1.0SG 12.2(14)S 12.2(15)T 15.0(1)S	GLBP は、冗長化されたルータ グループ間でパケットのロード シェアリングを行う一方、機能を停止したルータや回路（HSRP や VRRP など）からのデータ トラフィックを保護します。 このコンフィギュレーション モジュールのすべての項では、この機能についての情報を提供します。 この機能により、次のコマンドが導入または変更されました。**glbp forwarder preempt**、**glbp ip**、**glbp load-balancing**、**glbp name**、**glbp preempt**、**glbp priority**、**glbp sso**、**glbp timers**、**glbp timers redirect**、**glbp weighting**、**glbp weighting track**、**show glbp**。
GLBP クライアント キャッシュ	12.4(15)T 12.2(33)SXI	GLBP クライアント キャッシュには、GLBP グループをデフォルト ゲートウェイとして使用しているネットワーク ホストに関する情報が含まれています。 GLBP クライアント キャッシュには、特定の GLBP グループを使用する各ホストの MAC アドレス、各ネットワーク ホストに割り当てられている GLBP フォワーダの数、GLBP グループの各フォワーダに現在割り当てられているネットワーク ホストの総数が格納されます。また、各ネットワーク ホストによって使用されるプロトコル アドレス、ホストとフォワーダの割り当てが最後に更新されてから経過した時間も格納されます。 この機能に関する詳細については、次の各項を参照してください。 • 「GLBP クライアント キャッシュ」（P.6） • 「GLBP のカスタマイズ」（P.11） **glbp client-cache maximum** および **show glbp** の各コマンドがこの機能により導入または変更されました。

表 1　GLBP の機能情報 （続き）

機能名	リリース	機能設定情報
GLBP MD5 認証	Cisco IOS XE 3.1.0SG 12.2(18)S 12.3(2)T 12.2(33)SXH	MD5 認証は、代替となるプレーン テキスト認証スキームよりも高いセキュリティを実現します。MD5 認証を使用すると、各 GLBP グループ メンバが秘密キーを使用して、発信パケットの一部であるキー付き MD5 ハッシュを生成できます。着信パケットのキー付きハッシュが生成されると、生成されたハッシュと着信パケット内のハッシュが一致しない場合、パケットは無視されます。 この機能に関する詳細については、次の各項を参照してください。 • 「GLBP MD5 認証」（P.7） • 「キー ストリングを使用した GLBP MD5 認証の設定」（P.13） • 「キー チェーンを使用した GLBP MD5 認証の設定」（P.15） • 「例 : キー ストリングを使用した GLBP MD5 認証の設定」（P.23） • 「例 : キー チェーンを使用した GLBP MD5 認証の設定」（P.23） **glbp authentication** および **show glbp** の各コマンドがこの機能により変更されました。
ISSU と GLBP	12.2(31)SB2 12.2(33)SRB1	GLBP は In Service Software Upgrade（ISSU; インサービス ソフトウェア アップグレード）をサポートします。ISSU を使用すると、アクティブおよびスタンバイの Route Processor（RP; ルート プロセッサ）またはライン カード上で異なるバージョンの Cisco IOS ソフトウェアが実行されている場合でも、ハイアベイラビリティ（HA）システムをステートフル スイッチオーバー（SSO）モードで実行できるようになります。 この機能は、ソフトウェア アップグレード中に予定されたシステム停止中も同じレベルの HA 機能を提供します。不測のシステム停止が発生した場合も、SSO を使用できます。つまり、システムをセカンダリ RP に切り替えることができ、セッションを切断することなく、またパケットの損失も最小限に抑えながら、継続してパケットを転送できます。 この機能は、デフォルトでイネーブルにされています。 この機能に関する詳細については、次の各項を参照してください。 • 「ISSU と GLBP」（P.7） この機能により、新規追加または変更されたコマンドはありません。

表 1　GLBP の機能情報 （続き）

機能名	リリース	機能設定情報
SSO：GLBP	12.2(31)SB2 12.2(33)SRB 12.2(33)SXH 15.0(1)S	GLBP が SSO を認識するようになりました。GLBP は、ルータがセカンダリ RP にフェールオーバーしたことを検出し、GLBP グループの現在の状態を継続することができます。 別の RP がインストールされ、プライマリ RP が機能を停止した場合にはその処理を引き継ぐように設定されても、SSO を認識する前であるときは GLBP はこれを認識できません。プライマリが機能を停止すると、GLBP デバイスは GLBP グループに参加しなくなります。また、そのロールに応じて、グループ内の他のルータにアクティブ ルータとしてのロールが引き継がれます。このように機能が強化され、GLBP がセカンダリ RP に対するフェールオーバーを検出できるようになったため、GLBP グループに何ら変化は生じません。セカンダリ RP が機能を停止した場合、プライマリ RP が以前として利用できない状態であると、GLBP グループはこの状態を検出して新たなアクティブ GLBP ルータを再度選定します。 この機能は、デフォルトでイネーブルにされています。 この機能に関する詳細については、次の各項を参照してください。 • 「GLBP SSO」（P.8） • 「GLBP のカスタマイズ」（P.11） **debug glbp events**、**glbp sso**、**show glbp** の各コマンドがこの機能により導入または変更されました。

用語集

AVF：Active Virtual Forwarder（アクティブ仮想フォワーダ）。GLBP グループ内の 1 つの仮想フォワーダが、指定の仮想 MAC アドレスのアクティブ仮想フォワーダとして選定されます。選定されたフォワーダは、指定の MAC アドレスに対するパケットの転送を処理します。1 つの GLBP グループに複数のアクティブ仮想フォワーダを存在させることができます。

AVG：Active Virtual Gateway（アクティブ仮想ゲートウェイ）。GLBP グループ内の 1 つの仮想ゲートウェイが、アクティブ仮想ゲートウェイとして選定されます。選定されたゲートウェイは、プロトコル動作を処理します。

GLBP グループ：Gateway Load Balancing Protocol グループ。接続された イーサネット インターフェイス上で同じ GLBP グループ番号を持つ、1 つまたは複数の GLBP ゲートウェイ。

GLBP ゲートウェイ：Gateway Load Balancing Protocol ゲートウェイ。GLBP を実行するルータまたはゲートウェイ。各 GLBP ゲートウェイは、1 つまたは複数の GLBP グループに参加できます。

ISSU：In Service Software Upgrade（インサービス ソフトウェア アップグレード）。パケット転送の実行中に Cisco IOS ソフトウェアの更新や変更を可能にするプロセス。ほとんどのネットワークでは、予定されているソフトウェア アップグレードがダウンタイムの大きな原因になっています。ISSU を使用すると、パケット転送を続行しながら Cisco IOS ソフトウェアを修正できるので、ネットワークの可用性が向上し、予定されているソフトウェア アップグレードによるダウンタイムを短縮することができます。

NSF：Nonstop Forwarding（ノンストップ フォワーディング）。機能停止状態からの回復処理を行っているルータに対してトラフィックの転送を継続するルータの機能。また、障害からの回復中であるルータは、自身に送信されたトラフィックをピアによって正しく転送することができます。

RP：Route Processor（ルート プロセッサ）。シャーシの中央制御装置の総称です。一般に、プラットフォーム固有の用語が使用されます（Cisco 7500 では RSP、Cisco 10000 では PRE、Cisco 7600 では SUP+MSFC など）。

RPR：Route Processor Redundancy（ルート プロセッサ冗長性）。RPR は、High System Availability（HSA）機能に代替方法を提供します。HSA を使用すると、システムはアクティブ RP が機能を停止したときにスタンバイ RP をリセットして使用できます。RPR を活用すると、アクティブ RP に致命的なエラーが発生したときにアクティブ RP とスタンバイ RP の間で迅速なスイッチオーバーが行われるため、不測のダウンタイムを減らすことができます。

RPR+：RPR の拡張。スタンバイ RP が完全に初期化されます。

SSO：Stateful Switchover（ステートフル スイッチオーバー）。アクティブ装置とスタンバイ装置間のステート情報を保持するためのアプリケーションおよび機能をイネーブルにします。

vIP：仮想 IP アドレス。IPv4 アドレス。設定された各 GLBP グループには、必ず 1 つの仮想 IP アドレスがあります。仮想 IP アドレスは、少なくとも 1 つの GLBP グループ メンバに設定する必要があります。他の GLBP グループ メンバは、Hello メッセージを通して仮想 IP アドレスを学習します。

アクティブ RP：Route Processor（RP; ルート プロセッサ）はシステムの制御、ネットワーク サービスの提供、ルーティング プロトコルの実行、システム管理インターフェイスの有効化を実行します。

スイッチオーバー：システム制御とルーティング プロトコルの実行がアクティブ RP からスタンバイ RP に移行するイベント。スイッチオーバーは、手動操作によって、またはハードウェア/ソフトウェアの機能停止によって発生します。スイッチオーバーには、個々のユニットのシステム制御とパケット転送を組み合わせるシステムでのパケット転送機能の移行が含まれることがあります。

スタンバイ RP：完全に初期化され、アクティブ RP から制御を引き受ける準備が整った RP。手動または機能停止によってスイッチオーバーが発生します。

チェックポインティング：クライアント固有のステート データを保存または同期する処理。このデータは、冗長性のあるスイッチオーバーを実現するため、リモートのピア クライアントに転送されます。また、プロセスを再開始するため、ローカル ルータに転送されます。有効なチェックポインティング セッションが確立すると、チェックポイントされたステート データは順番に破損のない状態でリモートのピア クライアントに配信されることが保証されます。

HSRP の設定

Hot Standby Router Protocol（HSRP; ホット スタンバイ ルータ プロトコル）は、ファーストホップ IP ルータのフェールオーバーを透過的に実行できるように作成された First Hop Redundancy Protocol（FHRP; ファーストホップ冗長プロトコル）です。HSRP によるネットワークの高可用性は、イーサネットの IP ホスト、Fiber Distributed Data Interface（FDDI; ファイバ分散データ インターフェイス）、Bridge-Group Virtual Interface（BVI; ブリッジ グループ仮想インターフェイス）、LAN Emulation（LANE; LAN エミュレーション）、またはデフォルト ゲートウェイ IP アドレスを使用して設定されているトークン リング ネットワークでファーストホップ ルーティングの冗長性を確保することによって実現されます。HSRP は、アクティブ ルータとスタンバイ ルータを選択するために一連のルータで使用されます。一連のルータ インターフェイスでは、アクティブ ルータはパケットのルーティング用に選択されたルータであり、スタンバイ ルータは、アクティブ ルータに障害が発生したり、事前に設定した条件に一致したりしたときに処理を引き継ぐルータです。

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、「HSRP の機能情報」（P.67）を参照してください。

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

この章の構成

HSRP の制約事項

- HSRP は、マルチアクセス、マルチキャスト、またはブロードキャストに対応したイーサネット LAN で使用するように設計されており、既存のダイナミック プロトコルの代用として想定されているわけではありません。
- HSRP は、イーサネット、FDDI、BVI、LANE、またはトークン リングのインターフェイスで設定できます。各トークン リング インターフェイスは最大で 3 つのホット スタンバイ グループに対応し、グループ番号は 0、1、2 が割り当てられます。
- Lance イーサネット ハードウェアを使用する Cisco 2500 シリーズ、Cisco 3000 シリーズ、Cisco 4000 シリーズ、Cisco 4500 の各ルータは、1 つのイーサネット インターフェイス上の複数のホット スタンバイ グループをサポートしていません。PQUICC イーサネット ハードウェアを使用する Cisco 800 シリーズと Cisco 1600 シリーズは、1 つのイーサネット インターフェイス上の複数のホット スタンバイ グループをサポートしていません。1 つの回避策として、インターフェイス コンフィギュレーション コマンド **standby use-bia** を使用することができます。このコマンドは、事前に割り当てられた MAC アドレスではなく、インターフェイスのバーンドイン アドレスを仮想 MAC アドレスとして使用します。
- HSRP の Bidirectional Forwarding Detection（BFD; 双方向フォワーディング検出）サポートは、すべてのプラットフォームとインターフェイスで有効とは限りません。
- 同一の HSRP グループ番号または HSRP MAC アドレスを、同じメジャー インターフェイスの別々のサブインターフェイスで設定することはできません。

（注） この制限は、Cisco IOS Release 12.4(14)、12.4(15)T、12.2(33)SRB、12.2(33)SXH と、これらの Cisco IOS リリースの以降のリリースで解消されています。

- Enhanced Object Tracking（EOT; 拡張オブジェクト トラッキング）は、Stateful Switchover（SSO; ステートフル スイッチオーバー）対応ではなく、SSO モードで HSRP と使用することはできません。

HSRP の概要

HSRP の動作

ほとんどの IP ホストには､デフォルト ゲートウェイとして設定された 1 台のルータの IP アドレスが指定されています。HSRP を使用すると、ルータの IP アドレスではなく、HSRP 仮想 IP アドレスがホストのデフォルト ゲートウェイとして設定されます。

HSRP は、ICMP Router Discovery Protocol（IRDP）などのルータ ディスカバリ プロトコルをサポートしないホストや、選択したルータがリロードしたときやオフになったときに新しいルータに切り替える機能を備えていないホストには特に有効です。また、既存の TCP セッションはフェールオーバーが発生しても存続するため、このプロトコルでは IP トラフィックをルーティングするためにネクスト ホップを動的に選択するホストの回復をさらに透過的に実行できます。

HSRP は、ネットワーク セグメントで設定されている場合、仮想 MAC アドレスと、HSRP を実行しているルータのグループで共有される IP アドレスを用意します。この HSRP ルータ グループのアドレスが *仮想 IP アドレス*と呼ばれます。グループのうちの 1 台がプロトコルによって選択され、アクティブ ルータになります。アクティブ ルータはグループの MAC アドレスを宛先とするパケットを受け取ってルーティングします。HSRP を実行している *n* 台のルータでは、*n* + 1 個の IP アドレスと MAC アドレスが割り当てられます。

指定されたアクティブ ルータの障害を HSRP が検出すると、選択されているスタンバイ ルータがホット スタンバイ グループの MAC アドレスと IP アドレスの制御を引き継ぎます。このとき、新しいスタンバイ ルータも選択されます。

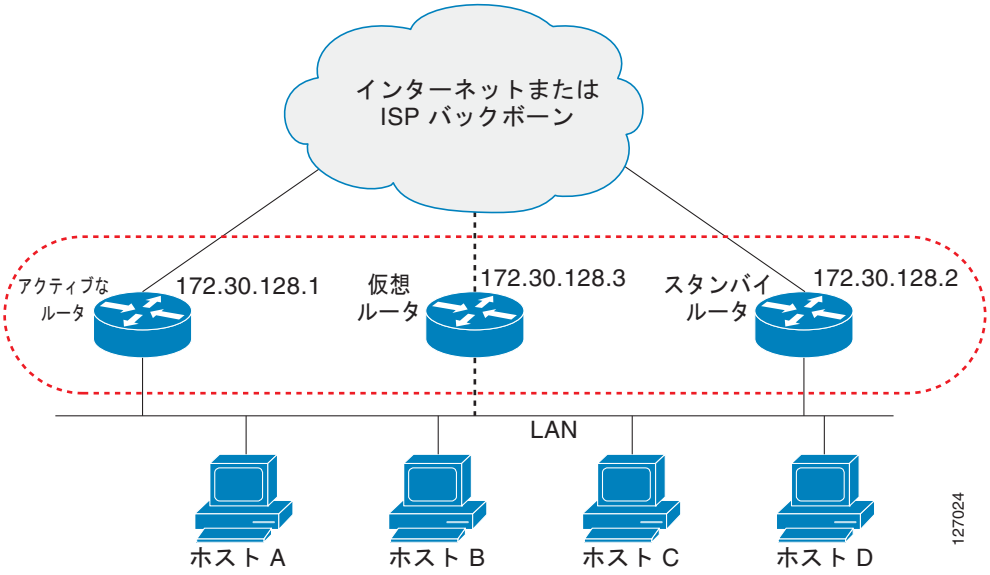
HSRP が設定されているルータのうち、どのルータをデフォルトのアクティブ ルータにするかを決定するために HSRP でプライオリティ メカニズムが使用されます。ルータをアクティブ ルータとして設定するためには、HSRP が設定された他のいずれのルータよりも高いプライオリティを割り当てます。デフォルトのプライオリティは 100 であるため、それを超えるプライオリティを 1 台のルータだけに割り当てれば、それがデフォルトのアクティブ ルータになります。

HSRP を実行しているルータは、User Datagram Protocol（UDP; ユーザ データグラム プロトコル）ベースのマルチキャスト hello メッセージを送信および受信して、ルータの障害を検出したり、アクティブ ルータとスタンバイ ルータを割り当てたりします。設定した時間内にアクティブ ルータが hello メッセージを送信できないと、プライオリティが最も高いスタンバイ ルータがアクティブ ルータになります。このようにパケット転送機能が別のルータに移行しても、ネットワークのいずれのホストにもまったく影響はありません。

複数のホット スタンバイ グループをインターフェイスに設定できるので、冗長ルータおよびロード シェアリングを余すところなく活用できるようになっています。

図 1 は、HSRP 用に構成されたネットワークを示しています。仮想 MAC アドレスおよび IP アドレスを共有することによって、複数台のルータが 1 台の*仮想ルータ*として機能します。仮想ルータは物理的には存在しませんが、互いのバックアップになるように設定されている複数のルータの共有のデフォルト ゲートウェイになります。LAN 上のホストは、アクティブ ルータの IP アドレスを使用して設定する必要はありません。その代わりに、仮想ルータの IP アドレス（仮想 IP アドレス）をデフォルト ゲートウェイとして使用して設定します。設定した時間内にアクティブ ルータが hello メッセージを送信できない場合、スタンバイ ルータが処理を引き継いで仮想アドレスに対応するアクティブ ルータになり、アクティブ ルータの役割を引き受けます。

図 1　　HSRP のトポロジ



HSRP は Inter-Switch Link（ISL; スイッチ間リンク）でカプセル化を行うことによってサポートされます。『*Cisco IOS LAN Switching Configuration Guide*』（リリース 12.4）の「Configuring Routing Between VLAN」という章の「Virtual LANs」を参照してください。

HSRP バージョン 2 の設計

HSRP バージョン 2 は、バージョン 1 の次の問題が解消されるように設計されています。

- 以前は、ミリ秒のタイマー値はアドバタイズまたは検出されませんでした。HSRP バージョン 2 では、ミリ秒のタイマー値がアドバタイズおよび検出されます。この変更により、あらゆる状況での HSRP グループの安定性が確保されています。
- グループ番号の範囲が 0 ～ 255 に制限されていました。HSRP バージョン 2 では、グループ番号の範囲が 0 ～ 4095 に拡大されています。

- HSRP バージョン 2 では、管理性とトラブルシューティング機能が向上しています。HSRP バージョン 1 では、発信元 MAC アドレスが HSRP 仮想 MAC アドレスであったため、メッセージを送信した物理ルータをアクティブな HSRP hello メッセージから特定する方法がありませんでした。HSRP バージョン 2 のパケット形式には、メッセージの送信元を一意に特定するための 6 バイトの識別子フィールドが組み込まれています。通常は、インターフェイスの MAC アドレスがこのフィールドに格納されます。
- HSRP hello メッセージの送信にマルチキャスト アドレス 224.0.0.2 が使用されていました。このアドレスは、Cisco Group Management Protocol（CGMP; シスコ グループ管理プロトコル）の脱退処理と競合することがあります。

バージョン 1 は HSRP のデフォルトのバージョンです。

HSRP バージョン 2 は、新しい IP マルチキャスト アドレス 224.0.0.102 を使用して hello パケットを送信します。バージョン 1 で使用されるマルチキャスト アドレス 224.0.0.2 は使用されません。この新しいマルチキャスト アドレスにより、CGMP の脱退処理を HSRP と同時にイネーブルにすることができます。

HSRP バージョン 2 では、グループ番号の範囲が拡張され、0 ～ 4095 までの番号を使用できるようなったため、0000.0C9F.F000 ～ 0000.0C9F.FFFF の新しい MAC アドレス範囲を使用できます。グループ番号の範囲が拡張されたといっても、インターフェイスがそれほどの数の HSRP グループをサポートできる（サポートするはずである）ということではありません。グループ番号の範囲が拡張されたのは、グループ番号をサブインターフェイスの VLAN 番号に一致させることができるようにするためです。

各グループに新しい仮想 MAC アドレスが指定されるため、HSRP バージョンを変更するときは、各グループが再度初期化されます。

HSRP バージョン 2 のパケット形式は、バージョン 1 とは異なります。このパケット形式には、Type-Length-Value（TLV; タイプ、長さ、値）形式が使用されています。HSRP バージョン 1 のルータが受信した HSRP バージョン 2 のパケットのタイプ フィールドは、HSRP バージョン 1 によってバージョン フィールドにマッピングされ、それ以降は無視されます。

また、Gateway Load Balancing Protocol（GLBP; ゲートウェイ ロード バランシング プロトコル）でも、HSRP バージョン 2 によって解消されている HSRP バージョン 1 の同じ問題が解消されます。GLBP の詳細については、『*Configuring GLBP* 』を参照してください。

HSRP の設定の変更

Cisco IOS Release 12.2(33)SXI、12.4(24)T、12.2(33)SRE 以降のリリースでは、セカンダリ インターフェイスの IP アドレスのサブネットに一致する仮想 IP アドレスで HSRP グループを設定できます。

セカンダリ インターフェイスの IP アドレスと同じネットワーク ID で HSRP グループの仮想 IP アドレスを設定すると、HSRP メッセージの送信元アドレスは最適なインターフェイス アドレスに自動的に設定されます。この設定の変更により、次の設定が可能になっています。

```
interface Ethernet1/0
 ip address 192.168.1.1 255.255.255.0
 ip address 192.168.2.1 255.255.255.0 secondary
 standby 1 ip 192.168.1.254
 standby 1 priority 105
 standby 1 preempt
 standby 2 ip 192.168.2.254 !Same network ID as secondary interface
```

Cisco IOS Release 12.2(33)SXI、12.4(24)T、12.2(33)SRE よりも前のリリースでは、HSRP 仮想 IP アドレスのネットワーク ID がプライマリ インターフェイスのアドレスと同じ場合を除き、HSRP グループは INIT ステートのままです。

さらに、設定されているインターフェイス アドレスがないのに HSRP グループ アドレスを設定すると、次の警告メッセージが表示されます。

```
% Warning: address is not within a subnet on this interface
```

HSRP の利点

冗長性
HSRP には、実績があり、大規模ネットワークで広範に導入されている冗長性方式が採用されています。

高速なフェールオーバー
HSRP では、ファーストホップ ルータのフェールオーバーが、透過的かつ高速に実行されます。

プリエンプション
プリエンプションにより、スタンバイ ルータがアクティブになるのを一定時間遅らせることができます（この時間は設定可能です）。

認証
HSRP の Message Digest 5（MD5; メッセージ ダイジェスト 5）アルゴリズム認証は、HSRP スプーフィング ソフトウェアから保護し、業界標準の MD5 アルゴリズムを使用して信頼性とセキュリティを向上させています。

HSRP グループとグループのアトリビュート

Command-Line Interface（CLI; コマンドライン インターフェイス）を使用して、グループのアトリビュートを次に適用できます。

- 1 つの HSRP グループ：インターフェイス コンフィギュレーション モードで実行され、1 つのグループに適用されます。
- インターフェイスのすべてのグループ：インターフェイス コンフィギュレーション モードで実行され、インターフェイスのすべてのグループに適用されます。
- すべてのインターフェイスのすべてのグループ：グローバル コンフィギュレーション モードで実行され、すべてのインターフェイスのすべてのグループに適用されます。

HSRP のプリエンプション

新規にリロードされたルータが HSRP アクティブ ルータになったとき、HSRP アクティブ ルータが既に存在していた場合は、HSRP のプリエンプションが機能していないように見えることがあります。この現象が発生する原因は、新しい HSRP アクティブ ルータが現在の HSRP アクティブ ルータから hello パケットを受信しておらず、プリエンプション設定が新しいルータの決定で考慮されないためです。

この現象は、インターフェイスが受信するパケットで遅延が発生することのある、Cisco 7600 シリーズのルータなどの一部の大規模なプラットフォームで発生する可能性があります。

通常は、すべての HSRP ルータを次のように設定することを推奨します。

standby delay minimum 30 reload 60

インターフェイス コンフィギュレーション コマンド **standby delay minimum reload** は、インターフェイスが起動した後、指定した時間が経過するまで HSRP グループの初期化を遅延します。

これは、HSRP プリエンプションによる遅延をイネーブルにするインターフェイス コンフィギュレーション コマンド **standby preempt delay** とは別のコマンドです。

HSRP のプライオリティとプリエンプション

プリエンプションを設定すると、プライオリティが最も高い HSRP ルータがすぐにアクティブ ルータになることができます。プライオリティの判定は、まず設定されているプライオリティ値で行われ、次に IP アドレスで行われます。値が同じ場合は、プライマリ IP アドレスが比較され、IP アドレスが高いほうが優先されます。いずれの場合も、値が高いほうがプライオリティが高くなります。ルータを設定するときにインターフェイス コンフィギュレーション コマンド **standby preempt** を使用しないと、そのルータは、他のすべてのルータよりもプライオリティが高い場合でもアクティブなルータになりません。

プライオリティが同じで、高い IP アドレスが設定されているスタンバイ ルータがアクティブ ルータに取って代わることはありません。

ルータは、最初に起動したとき、完全なルーティング テーブルを保持していません。プリエンプションの遅延を設定して、設定した時間にわたってプリエンプションを遅延することができます。この遅延により、ルータはアクティブ ルータになる前にルーティング テーブルを構築することができます。

プリエンプションがイネーブルになっていない場合、アクティブ ルータから hello メッセージを受け取っていなくても、あるルータがアクティブ ルータに取って代わっているように見えることがあります。

オブジェクト トラッキングが HSRP ルータのプライオリティに与える影響

オブジェクト トラッキングが設定されている場合に、追跡対象のオブジェクトがダウンすると、デバイスのプライオリティはダイナミックに変化します。トラッキング プロセスは、追跡対象オブジェクトを定期的にポーリングし、値に変化がないかどうかを確認します。トラッキング対象のオブジェクトの変化は、すぐに HSRP に伝えられるか、指定した遅延時間が経過してから HSRP に伝えられます。オブジェクトの値は、アップまたはダウンとして報告されます。トラッキング可能なオブジェクトには、インターフェイスのライン プロトコル ステートや IP ルートの到達可能性などがあります。指定したオブジェクトがダウンすると、HSRP プライオリティが引き下げられます。このとき、プライオリティの高いほうの HSRP ルータは、**standby preempt** が設定されていれば、アクティブ ルータになることができます。オブジェクト トラッキングの詳細については、「HSRP のオブジェクト トラッキングの設定」（P.26）を参照してください。

HSRP のアドレス指定

HSRP ルータが互いに通信するときは、HSRP hello パケットをやり取りします。このパケットは、UDP ポート 1985 の宛先 IP マルチキャスト アドレス 224.0.0.2（すべてのルータとの通信に使用される予約済みのマルチキャスト アドレス）に送信されます。アクティブ ルータは、それ自身に設定されている IP アドレスと HSRP 仮想 MAC アドレスを hello パケットの送信元とし、スタンバイ ルータは、それ自身に設定されている IP アドレスとインターフェイス MAC アドレスを hello パケットの送信元とします。この MAC アドレスは、バーンドイン MAC アドレス（BIA）である場合も、そうでない場合もあります。

ホストは、HSRP 仮想 IP アドレスとしてデフォルト ゲートウェイを使用して設定されるため、HSRP 仮想 IP アドレスに関連付けられている MAC アドレスと通信する必要があります。この MAC アドレスは、0000.0C07.ACxy で構成される仮想 MAC アドレスです。この *xy* はそれぞれのインターフェイスに基づいた 16 進数の HSRP グループ番号です。たとえば、HSRP グループ 1 は 0000.0C07.AC01 という HSRP 仮想 MAC アドレスを使用します。隣接する LAN セグメントのホストは通常の Address Resolution Protocol（ARP; アドレス解決プロトコル）を使用して、対応する MAC アドレスを解決します。

トークン リング インターフェイスは、HSRP MAC アドレスに機能アドレスを使用します。機能アドレスは、使用できる唯一の汎用マルチキャスト メカニズムです。使用可能なトークン リングの機能アドレスの数は限られており、大半は他の機能のために予約されています。HSRP で使用可能なアドレスは次の 3 つだけです。

- c000.0001.0000（グループ 0）
- c000.0002.0000（グループ 1）
- c000.0004.0000（グループ 2）

したがって、インターフェイス コンフィギュレーション コマンド **standby use-bia** が設定されている場合を除き、トークン リング インターフェイスで設定できる HSRP グループは 3 つだけです。

HSRP バージョン 2 は、新しい IP マルチキャスト アドレス 224.0.0.102 を使用して hello パケットを送信します。バージョン 1 で使用されるマルチキャスト アドレス 224.0.0.2 は使用されません。この新しいマルチキャスト アドレスにより、Cisco Group Management Protocol（CGMP; シスコ グループ管理プロトコル）の脱退処理を HSRP と同時にイネーブルにすることができます。

HSRP バージョン 2 では、グループ番号の範囲が拡張され、0 ～ 4095 までの番号を使用できるようなったため、0000.0C9F.F000 ～ 0000.0C9F.FFFF の新しい MAC アドレス範囲を使用できます。

HSRP 仮想 MAC アドレスと BIA MAC アドレス

各 HSRP ルータの仮想 MAC アドレスはルータで自動的に生成されます。ただし、Advanced Peer-to-Peer Networking（APPN; 拡張分散ネットワーク機能）などの一部のネットワーク実装では、MAC アドレスを使用して、ルーティングのためのファーストホップを特定します。この場合、グループで **standby mac-address** コマンドを使用して仮想 MAC アドレスを指定できるようになっていなければならないことがよくあります。このようなプロトコルでは、仮想 IP アドレスは重要ではありません。

standby use-bia コマンドは、トークン リング インターフェイスの HSRP MAC アドレスに機能アドレスを使用するという制限を解消するために実装されています。このコマンドを使用すると、HSRP グループは HSRP 仮想 MAC アドレスではなく、インターフェイスの BIA MAC アドレスを使用できるようになります。HSRP が複数リングのソースルート ブリッジング環境で実行されていて、異なるリングに HSRP ルータが存在する場合に、**standby use-bia** コマンドを設定すると、Routing Information Field（RIF; ルーティング情報フィールド）に関する混乱を防ぐことができます。

standby use-bia コマンドはインターフェイスに適用され、**standby mac-address** コマンドは HSRP グループに適用されます。

HSRP タイマー

各 HSRP ルータには、hello メッセージのタイミング管理に使用されるアクティブ タイマー、スタンバイ タイマー、hello タイマーの 3 つのタイマーがあります。タイマーが時間切れになると、ルータは新しい HSRP ステートに変化します。タイマー値が設定されていないルータやアクセス サーバは、アクティブ ルータやスタンバイ ルータからタイマー値を取得できます。アクティブ ルータに設定されているタイマーは、常に他のいずれのタイマー設定よりも優先されます。ホット スタンバイ グループのすべてのルータは同じタイマー値を使用する必要があります。

HSRP バージョン 1 では、ミリ秒のタイマー値が使用されている場合を除き、アクティブでないルータはタイマー値をアクティブ ルータから取得します。ミリ秒のタイマー値が使用されている場合は、すべてのルータはミリ秒のタイマー値を使用して設定されていなければなりません。このルールは、hello 時間とホールド時間のどちらかがミリ秒単位で指定されている場合に当てはまります。この設定が必要なのは、HSRP hello パケットはタイマー値を秒単位でアドバタイズするためです。HSRP バージョン 2 には、この制限はありません。このバージョンではタイマー値がミリ秒単位でアドバタイズされます。

HSRP の MAC リフレッシュ間隔

HSRP が FDDI で動作している場合、ラーニング ブリッジやスイッチの MAC キャッシュをリフレッシュするためにパケットを送信する間隔を変更することができます。FDDI インターフェイスの HSRP hello パケットが使用するのは MAC 仮想アドレスではなく Burned-In Address（BIA; バーンドイン アドレス）です。リフレッシュ パケットは、スイッチやラーニング ブリッジの MAC キャッシュを最新の状態に保ちます。また、複数グループのスレーブとして設定されている HSRP グループは定期的に hello メッセージを送信しないため、このような HSRP グループに対しても使用されます。

FDDI リングでのリフレッシュ間隔を延長または短縮して、帯域幅をさらに効率的に使用することができます。MAC リフレッシュ パケットが不要な場合（FDDI を使用しているがラーニング ブリッジやスイッチが存在しない場合）は、MAC リフレッシュ パケットが送信されないようにすることが可能です。

HSRP のテキスト認証

HSRP は、認証されていない HSRP メッセージを無視します。デフォルトの認証タイプはテキスト認証です。

HSRP 認証は、サービス拒絶攻撃を引き起こす偽の HSRP hello パケットから保護します。たとえば、ルータ A のプライオリティが 120 で、これがアクティブ ルータであるとします。あるホストが、プライオリティが 130 の偽の HSRP hello パケットを送信すると、ルータ A はアクティブ ルータとしての動作を停止します。ルータ A に偽の HSRP hello パケットを無視するような認証が設定されていれば、ルータ A はアクティブ ルータのままです。

HSRP パケットが拒否されるのは、次のいずれかの場合です。

- ルータと着信パケットの認証方式が異なる。
- ルータと着信パケットのテキスト認証文字列が異なる。

HSRP MD5 認証

HSRP MD5 認証の導入前、HSRP は単純なプレーン テキスト文字列でプロトコル パケットを認証していました。HSRP MD5 認証は、マルチキャスト HSRP プロトコル パケットの HSRP 部分の MD5 ダイジェストを生成するように拡張された認証方式です。この機能により、セキュリティが強化され、HSRP スプーフィング ソフトウェアの脅威に対する保護が得られます。

MD5 認証は、代替となるプレーン テキスト認証スキームよりも高いセキュリティを実現します。HSRP グループの各メンバーは秘密キーを使用して、発信パケットの一部となるキー付き MD5 ハッシュを生成できます。着信パケットからはキー付きハッシュが生成されますが、このハッシュと着信パケット内のハッシュが一致しない場合は、パケットは無視されます。

MD5 ハッシュのキーは、キー ストリングを使用して設定に直接指定することもできますし、キーチェーンを通して間接的に提供することもできます。

HSRP には次の 2 つの認証方式があります。

- プレーン テキスト認証
- MD5 認証

HSRP 認証は、サービス拒絶攻撃を引き起こす偽の HSRP hello パケットから保護します。たとえば、ルータ A のプライオリティが 120 で、これがアクティブ ルータであるとします。あるホストが、プライオリティが 130 の偽の HSRP hello パケットを送信すると、ルータ A はアクティブ ルータとしての動作を停止します。ルータ A に偽の HSRP hello パケットを無視するような認証が設定されていれば、ルータ A はアクティブ ルータのままです。

HSRP パケットが拒否されるのは、次のいずれかの場合です。

- ルータと着信パケットの認証方式が異なる。
- ルータと着信パケットの MD5 ダイジェストが異なる。
- ルータと着信パケットのテキスト認証文字列が異なる。

HSRP の IPv6 サポート

ほとんどの IPv4 ホストでは、1 台のルータの IP アドレスがデフォルト ゲートウェイとして設定されています。HSRP を使用すると、ルータの IP アドレスではなく、HSRP 仮想 IP アドレスがホストのデフォルト ゲートウェイとして設定されます。2 つの HSRP グループを使用し、ある仮想 IP アドレスでホストの半分を設定し、別の仮想 IP アドレスで残りのホストを設定することによって、簡単なロードシェアリングが実現できます。

それに対して、IPv6 ホストは IPv6 ネイバー探索の Router Advertisement（RA; ルータ アドバタイズメント）メッセージを使用して、使用可能な IPv6 ルータを検出します。メッセージは定期的にマルチキャストされるほか、ホストから要求されることもあります。HSRP は IPv6 ホストに仮想ファーストホップのみを伝えるように設計されています。

HSRP IPv6 グループには、HSRP グループ番号から生成される仮想 MAC アドレスと、デフォルトで HSRP 仮想 MAC アドレスから生成される仮想 IPv6 リンクローカル アドレスがあります。HSRP IPv6 が使用する MAC アドレス範囲は 0005.73A0.0000 ～ 0005.73A0.0FFF です。HSRP グループがアクティブになっているときは、HSRP 仮想 IPv6 リンクローカル アドレスに RA が定期的に送信されます。HSRP グループがアクティブ ステートではなくなると、最後の RA が送信された後、定期的な RA の送信は停止します。

最後の RA が送信された後、インターフェイスのリンクローカル アドレスへの 定期的な RA の送信は停止しますが、インターフェイスには少なくとも 1 つの 仮想 IPv6 リンクローカル アドレスが設定されています。インターフェイスの IPv6 リンクローカル アドレスには、RA に関して挙げられているものを除き、制限は発生しません。他のプロトコルは、このアドレスに対するパケットの送信と受信を引き続き実行します。

HSRP が設定されているルータのうち、どのルータをデフォルトのアクティブ ルータにするかを決定するために HSRP でプライオリティ メカニズムが使用されます。ルータをアクティブ ルータとして設定するためには、HSRP が設定された他のいずれのルータよりも高いプライオリティを割り当てます。デフォルトのプライオリティは 100 であるため、それを超えるプライオリティを 1 台のルータだけに割り当てれば、それがデフォルトのアクティブ ルータになります。

詳細については、『*Cisco IOS IPv6 Configuration Guide*』の「Configuring First Hop Redundancy Protocols in IPv6」を参照してください。

HSRP のメッセージとステート

HSRP を使用して設定されているルータは、次の 3 種類のマルチキャスト メッセージをやり取りします。

- hello : hello メッセージは、ルータの HSRP プライオリティとステートに関する情報を他の HSRP ルータに伝達します。
- coup : スタンバイ ルータは、アクティブ ルータの機能を引き継ぐときに coup メッセージを送信します。
- resign : アクティブ ルータであるルータは、シャットダウンする直前や、もっとプライオリティの高いルータから hello メッセージまたは coup メッセージを受け取ったときに、このメッセージを送信します。

常に、HSRP を使用して設定されているルータは次のいずれかのステートになっています。

- Active：ルータはパケット転送機能を実行しています。
- Standby：ルータはアクティブ ルータに障害が発生した場合にパケット転送機能を引き継ぐことができる状態になっています。
- Speak：ルータは hello メッセージの送受信中です。
- Listen：ルータは hello メッセージの受信中です。
- Learn：ルータは、仮想 IP アドレスを特定しておらず、アクティブ ルータからの認証済みの hello メッセージをまだ受信していません。このステートでは、ルータはアクティブ ルータからのメッセージを引き続き待機します。
- Init または Disabled：ルータは HSRP に参加する準備ができていないか、参加できない状態です。対応するインターフェイスが起動されていない可能性があります。スヌーピングによって検出されたネットワークの他のルータで設定されている HSRP グループは、Init ステートであると表示されます。また、停止しているインターフェイスを使用してローカルで設定されているグループや、指定したインターフェイス IP アドレスを持たないグループも、Init ステートであると表示されます。

Cisco IOS Release 12.2(33)SXH 以降の Cisco IOS 12.2SX リリース、Cisco IOS Release 12.2(33)SRB 以降の Cisco IOS 12.2SR リリース、Cisco IOS Release 12.4(8) 以降の Cisco IOS 12.4 リリースでは、HSRP は、HSRP ステートの変化に関する syslog メッセージにログ レベル 5 を使用してイベントをログ記録し、ルータの syslog バッファがプライオリティの低いレベル 6 のメッセージでいっぱいにならないようにしています。

これらのリリースよりも前の Cisco IOS ソフトウェアは、HSRP ステートの変化に関する syslog メッセージにログ レベル 6 を使用します。

HSRP と ARP

HSRP は、ホストがプロキシ ARP に対応するように設定されているときも機能します。アクティブ HSRP ルータは、ローカル LAN に存在しないホストの ARP 要求を受信すると、仮想ルータの MAC アドレスを使用して応答します。このアクティブ ルータが使用不能になるか、リモート LAN への接続が失われると、アクティブ ルータになったルータが、仮想ルータ宛てにアドレス指定されたパケットを受信し、適切に転送します。インターフェイスがホット スタンバイ状態になっていない場合は、プロキシ ARP 応答は実行されません。

HSRP gratuitous ARP

HSRP gratuitous ARP 機能により、HSRP は ARP キャッシュ内のエントリが正しいことを確認し、1 つまたは複数のアクティブ HSRP グループから gratuitous ARP パケットを定期的に送信するように設定されます。HSRP は、デフォルトでは HSRP グループのステートが Active に変化したときに、そのグループから gratuitous ARP パケットを 3 個送信します。最初の 1 個はグループがアクティブになったときに送信しますが、残りの 2 個が送信されるのは 2 秒後と 4 秒後です。

HSRP gratuitous ARP 機能によって HSRP の機能が拡張され、アクティブ HSRP グループから送信される gratuitous ARP パケットの数と頻度を設定できるようになっています。指定した間隔で特定の数の gratuitous ARP パケットが送信されるように設定するには、**standby arp gratuitous** コマンドをインターフェイス コンフィギュレーション モードで使用します。

アクティブなグループごとに 1 つの gratuitous ARP パケットを送信するように HSRP を設定するには、**standby send arp** コマンドを EXE モードで使用します。**standby send arp** コマンドが設定されると、HSRP は gratuitous ARP パケットを送信する前に ARP キャッシュのエントリが正しいことを確認します。ARP エントリが正しくない場合、HSRP は ARP エントリを再度追加します。スタティック ARP エントリやエイリアス ARP エントリは HSRP によって上書きされることはありません。

standby send arp コマンドを設定すると、CPU 利用率の高いプロセスや設定が開始される前にホストの ARP キャッシュが更新される状態になります。

適度にソフトウェア スイッチングされた IP トラフィックと大量の ARP トラフィックが一緒になって CPU 利用率が 50% を上回ると、ARP リフレッシュ要求が正常に実行されず、一部のアプリケーション サーバがデフォルト ゲートウェイの ARP エントリを失って、残りのネットワークと通信できなくなります。場合によっては、大規模なアクセス リストをイネーブル化するなどの操作によってホストからの ARP 要求が遅延して、ホストにデフォルト ゲートウェイがない状態が短時間発生することがあります。HSRP アクティブ ルータから定期的に送信される gratuitous ARP パケットは、期限切れになる前にホストの ARP キャッシュをリフレッシュします。

HSRP のオブジェクト トラッキング

オブジェクト トラッキングにより、HSRP からトラッキング メカニズムが分離され、HSRP だけでなく、他のプロセスも使用可能な独立したトラッキング プロセスが別に生成されます。デバイスのプライオリティがオブジェクト トラッキング用に設定されているときに、トラッキング対象のオブジェクトがダウンすると、デバイスのプライオリティが動的に変更されることがあります。トラッキング可能なオブジェクトには、インターフェイスのライン プロトコル ステートや IP ルートの到達可能性などがあります。指定したオブジェクトがダウンすると、HSRP プライオリティが引き下げられます。

HSRP、Virtual Router Redundancy Protocol（VRRP; 仮想ルータ冗長プロトコル）、Gateway Load Balancing Protocol（GLBP; ゲートウェイ ロード バランシング プロトコル）などのクライアント プロセスは、オブジェクトのトラッキングを登録し、トラッキング対象オブジェクトのステートが変化したときに通知を得ることができるようになっています。

オブジェクト トラッキングの詳細については、『*Configuring Enhanced Object Tracking*』を参照してください。

HSRP の ICMP リダイレクト サポート

ICMP は、ネットワーク層のインターネット プロトコルで、IP 処理に関連するエラーなどの情報をレポートするメッセージ パケットを生成します。ICMP はエラー パケットをホストに送信したり、リダイレクト パケットをホストに送信したりすることができます。

HSRP を実行しているときは、HSRP グループに属するルータのインターフェイス（または実際の）IP アドレスをホストが検出しないようにすることが重要です。ICMP によってホストがルータの実際の IP アドレスにリダイレクトされた場合、そのルータに後で障害が発生すると、そのホストからのパケットは失われます。

ICMP リダイレクト メッセージは、HSRP を使用して設定されているインターフェイスで自動的にイネーブルになります。この機能は、ネクストホップ IP アドレスが HSRP 仮想 IP アドレスに変更されることのある HSRP で発信 ICMP リダイレクト メッセージをフィルタリングすることによって効果を発揮します。

アクティブ HSRP ルータへの ICMP リダイレクト

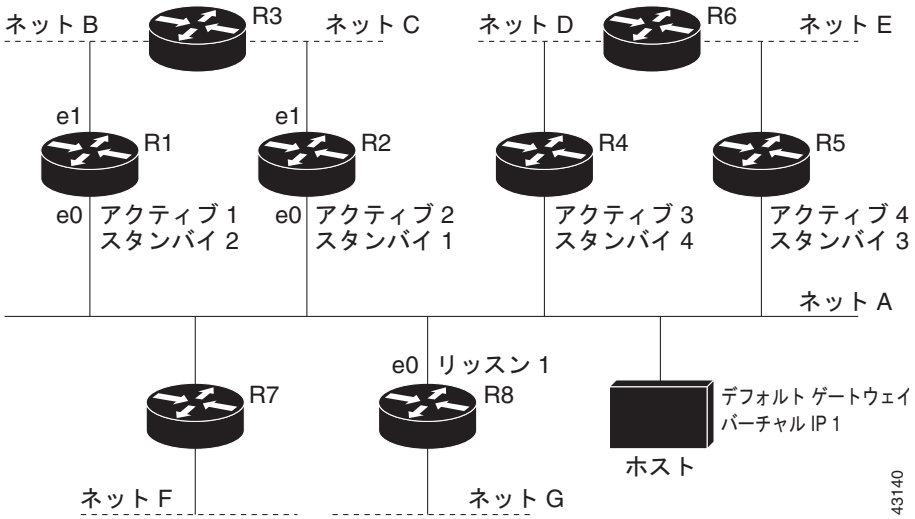
ネクストホップ IP アドレスは、そのネットワークの アクティブ HSRP ルータのリストと比較されます。一致が見つかると、実際のネクストホップ IP アドレスが、対応する仮想 IP アドレスに置き換えられ、リダイレクト メッセージの続行が許可されます。

一致が見つからない場合、ICMP リダイレクト メッセージが送信されるのは、新しいネクストホップ IP アドレスに対応するルータが HSRP を実行していない場合だけです。パッシブ HSRP ルータへのリダイレクトは許可されません（パッシブ HSRP ルータとは、HSRP を実行しているが、インターフェイスのアクティブ HSRP グループが存在しないルータです）。

最適に動作するためには、HSRP を実行しているネットワークの各ルータには、そのネットワークのインターフェイスのアクティブ HSRP グループが少なくとも 1 つ存在する必要があります。各 HSRP ルータが同じグループのメンバーである必要はありません。各 HSRP ルータはネットワークの HSRP パケットをすべてスヌーピングして、アクティブ ルータのリスト（仮想 IP アドレスと実際の IP アドレス）を管理します。

図 2 のネットワークに注目してください。このネットワークでは、HSRP ICMP リダイレクション フィルタがサポートされています。

図 2　　HSRP ICMP リダイレクション フィルタをサポートするネットワーク



ホストは、ネット D の別のホストにパケットを送信する場合、まずパケットをデフォルト ゲートウェイ（HSRP グループ 1 の仮想 IP アドレス）に送信します。

ホストから受信したパケットを次に示します。

```
dest MAC          = HSRP group 1 virtual MAC
source MAC        = Host MAC
dest IP           = host-on-netD IP
source IP         = Host IP
```

ルータ R1 は、このパケットを受信し、ルータ R4 のネット D へのパスのほうが適切であると判断したため、ルータ R4 の実際の IP アドレスにホストをリダイレクトするリダイレクト メッセージを送信する準備を行います（実際の IP アドレスのみが R1 のルーティング テーブルに含まれているため）。

ルータ R1 によって送信された最初の ICMP リダイレクト メッセージを次に示します。

```
dest MAC          = Host MAC
source MAC        = router R1 MAC
```

```
dest IP          = Host IP
source IP        = router R1 IP
gateway to use   = router R4 IP
```

このリダイレクトが発生する前、ルータ R1 の HSRP プロセスでルータ R4 がグループ 3 のアクティブ HSRP ルータであることが特定されるため、リダイレクト メッセージのネクストホップがルータ R4 の実際の IP アドレスからグループ 3 の仮想 IP アドレスに変更されます。さらに、リダイレクト メッセージを発生させた宛先 MAC アドレスから、ホストがグループ 1 の仮想 IP アドレスをゲートウェイとして使用したことが特定されるため、リダイレクト メッセージの送信元 IP アドレスがグループ 1 の仮想 IP アドレスに変更されます。

修正された ICMP リダイレクト メッセージでは、次の 2 つのフィールド（*）が修正されています。

```
dest MAC         = Host MAC
source MAC       = router R1 MAC
dest IP          = Host IP
source IP*       = HSRP group 1 virtual IP
gateway to use*  = HSRP group 3 virtual IP
```

2 回目の修正が必要な理由は、ホストが ICMP リダイレクト メッセージの送信元 IP アドレスを自身のデフォルト ゲートウェイと比較するためです。これらのアドレスが一致しない場合、ICMP リダイレクト メッセージは無視されます。この段階で、ホストのルーティング テーブルの構成は、デフォルト ゲートウェイ、グループ 1 の仮想 IP アドレス、グループ 3 の仮想 IP アドレスを通るネット D へのルートから成っています。

パッシブ HSRP ルータへの ICMP リダイレクト

パッシブ HSRP ルータへのリダイレクトは許可されません。ホストが HSRP ルータの実際の IP アドレスを検出した場合、冗長性が失われることがあります。

図 2 では、ルータ R8 はパッシブ HSRP ルータであるため、R8 へのリダイレクトは許可されません。この場合、ホストからネット D へのパケットは、まずルータ R1 に到着した後、ルータ R4 に転送されます（つまり、ネットワークを 2 回通過します）。

パッシブ HSRP ルータのあるネットワーク構成は、誤った構成と見なされます。HSRP ICMP リダイレクトが最適に動作するためには、ネットワークの HSRP を実行している各ルータに、少なくとも 1 つのアクティブ HSRP グループが存在していなければなりません。

非 HSRP ルータへの ICMP リダイレクト

ローカル インターフェイスで HSRP を実行していないルータへのリダイレクトは許可されます。非 HSRP ルータの実際の IP アドレスをホストが検出しても、冗長性が失われることはありません。

図 2 では、ルータ R7 は HSRP を実行していないので、R7 へのリダイレクトが許可されます。この場合、ネクストホップ IP アドレスは変更されません。送信元 IP アドレスは元のパケットの宛先 MAC アドレスに応じて変更されます。このリダイレクトの送信を停止するには、**no standby redirect unknown** コマンドを使用します。

パッシブ HSRP ルータのアドバタイズメント

パッシブ HSRP ルータは、HSRP アドバタイズメント メッセージの送信を定期的に行うほか、パッシブ ステートに入るときやパッシブ ステートから出るときに行います。したがって、すべての HSRP ルータが、ネットワークにある任意の HSRP ルータの HSRP グループのステートを判別できます。このアドバタイズメントは、次のように HSRP インターフェイスのステートをネットワークの他の HSRP ルータに伝えます。

- Dormant : インターフェイスには HSRP グループがありません。最後のグループが削除されるときに 1 つのアドバタイズメントが一度送信されます。
- Passive : インターフェイスには、非アクティブのグループが少なくとも 1 つありますが、アクティブなグループはありません。アドバタイズメントは定期的に送信されます。
- Active : インターフェイスには、アクティブなグループが少なくとも 1 つあります。最初のグループがアクティブになるときに 1 つのアドバタイズメントが送信されます。

アドバタイズメントの間隔とホールドダウン時間の調整は、**standby redirect timers** コマンドを使用して行います。

送信されない ICMP リダイレクト

HSRP ルータが、リダイレクトを発生させたパケットを送信するときに、ホストが使用した IP アドレスを一意に特定できない場合、リダイレクト メッセージは送信されません。HSRP ルータは元のパケットの宛先 MAC アドレスを使用して、この IP アドレスの特定を行います。インターフェイス コンフィギュレーション コマンド **standby use-bia** の使用がインターフェイスで指定されているような特定の構成では、リダイレクトは送信できません。この場合、HSRP グループはその仮想 MAC アドレスとしてインターフェイス MAC アドレスを使用します。この時点では、HSRP ルータはホストのデフォルト ゲートウェイが実際の IP アドレスであるか、インターフェイスでアクティブな HSRP 仮想 IP アドレスの 1 つであるかを特定することはできません。

Cisco 800 シリーズ、Cisco 1000 シリーズ、Cisco 1600 シリーズ、Cisco 2500 シリーズ、Cisco 3000 シリーズ、Cisco 4500 シリーズのルータでは、HSRP と ICMP リダイレクトを使用することはできません。これは、イーサネット コントローラが 1 つの MAC アドレスしかサポートしていないためです。

ICMP パケットの IP 送信元アドレスは、ICMP パケットを発生させたパケットでホストによって使用されているゲートウェイ アドレスと一致している必要があります。一致していない場合、ホストは ICMP リダイレクト パケットを拒否します。HSRP ルータは送信先 MAC アドレスを使用してホストのゲートウェイ IP アドレスを特定します。その HSRP ルータが複数の IP アドレスに対して同じ MAC アドレスを使用している場合、ホストのゲートウェイ IP アドレスを一意に特定することは不可能であり、リダイレクト メッセージは送信されません。

次の出力サンプルは、ホストによって使用されているゲートウェイを HSRP ルータが一意に特定できない場合に **debug standby events icmp** EXEC コマンドを実行して得られたものです。

```
10:43:08: HSRP: ICMP redirect not sent to 20.0.0.4 for dest 30.0.0.2
10:43:08: HSRP: could not uniquely determine IP address for mac 00d0.bbd3.bc22
```

HSRP グループ シャットダウン

FHRP - HSRP グループ シャットダウン機能を使用すると、トラッキング対象のオブジェクトがダウンしたときに、HSRP グループのプライオリティを下げるのではなく、ディセーブルな状態になる（ステートが Init になる）ように HSRP グループを設定することができます。HSRP グループ シャットダウンを設定するには、**shutdown** キーワードとともに **standby track** コマンドを使用します。

あるオブジェクトが HSRP グループによってすでにトラッキングされている場合、HSRP グループ シャットダウン機能を使用するようにこのトラッキング設定を変更することはできません。先に、**no standby track** コマンドを使用してトラッキング設定を解除し、**shutdown** キーワードとともに **standby track** コマンドを使用してトラッキング設定を再度設定する必要があります。

次の例は、HSRP グループ シャットダウン機能が追加されるようにトラッキング対象のオブジェクトの設定を変更する方法を示しています。

```
no standby 1 track 101 decrement 10
standby 1 track 101 shutdown
```

HSRP の MPLS VPN サポート

HSRP の Multiprotocol Label Switching（MPLS; マルチプロトコル ラベル スイッチング）Virtual Private Network（VPN; バーチャル プライベート ネットワーク）インターフェイス サポートが役に立つのは、次のいずれかの状態で 2 つの Provider Edge（PE; プロバイダー エッジ）ルータ間でイーサネット LAN が接続されている場合です。

- Customer Edge（CE; カスタマー エッジ）ルータに HSRP 仮想 IP アドレスへのデフォルト ルートがある。
- 1 つまたは複数のホストで、HSRP 仮想 IP アドレスがデフォルト ゲートウェイとして設定されている。

各 VPN は 1 つまたは複数の VPN Routing and Forwarding（VRF; VPN ルーティングおよびフォワーディング）インスタンスに関連付けられています。VRF は次の要素で構成されています。

- IP ルーティング テーブル
- Cisco Express Forwarding（CEF; シスコ エクスプレス フォワーディング）テーブル
- CEF フォワーディング テーブルを使用する一連のインターフェイス
- ルーティング テーブルの情報を管理する一連のルールおよびルーティング プロトコル パラメータ

VPN ルーティング情報は、各 VRF の IP ルーティング テーブルと CEF テーブルに格納されています。各 VRF の一連のルーティング テーブルと CEF テーブルは別々に維持されます。これらのテーブルにより、VPN の外側に情報が転送されないようになっているほか、VPN の外側のパケットも VPN 内のルータに転送されないようになっています。

HSRP は、デフォルトのルーティング テーブル インスタンスを使用して ARP エントリと IP ハッシュ テーブル エントリ（エイリアス）を追加します。ただし、VRF フォワーディングがインターフェイスで設定されているときは別のルーティング テーブル インスタンスが使用されるため、HSRP 仮想 IP アドレスに対する ARP および ICMP のエコー要求は失敗します。

HSRP の MPLS VPN サポートにより、HSRP 仮想 IP アドレスがデフォルトのルーティング テーブルではなく、正しい IP ルーティング テーブルに確実に追加されます。

HSRP 複数グループ最適化

同じ物理インターフェイスに設定されるサブインターフェイスが増え続けて数百にものぼり、各サブインターフェイスには固有の HSRP グループがある状態になっています。この複数の HSRP グループのネゴシエーションやメンテナンスは、ネットワーク トラフィックや CPU 使用率に悪影響を及ぼすことがあります。

アクティブ ルータとスタンバイ ルータを選出するために物理インターフェイスに必要なのは、1 つの HSRP グループだけです。このグループが *マスター グループ*と呼ばれます。他の HSRP グループは、各サブインターフェイスに作成されたり、グループ名によってマスター グループとリンクされたりします。リンクされた HSRP グループは、*クライアント グループ*または*スレーブ グループ*と呼ばれます。

クライアント グループの HSRP グループ ステートは、マスター グループと同じです。また、クライアント グループはどの種類のルータ選出メカニズムにも参加しません。

クライアント グループは、スイッチやラーニング ブリッジの仮想 MAC アドレスをリフレッシュするために、定期的にメッセージを送信します。リフレッシュ メッセージが送信される頻度は、マスター グループから送信されるプロトコル選択メッセージに比べて、はるかに低いことがあります。

HSRP - ISSU

In-Service Software Upgrade（ISSU; インサービス ソフトウェア アップグレード）プロセスにより、パケット 転送を続行しながら、Cisco IOS ソフトウェアをアップデートまたは修正することができます。ほとんどのネットワークでは、予定されているソフトウェア アップグレードがダウンタイムの大きな原因になっています。ISSU を使用すると、パケット転送を続行しながら Cisco IOS ソフトウェアを修正できるので、ネットワークの可用性が向上し、予定されているソフトウェア アップグレードによるダウンタイムを短縮することができます。このマニュアルでは、ISSU の概念が説明されているほか、ISSU をシステムで実行するのに必要な手順が説明されています。

ISSU の詳細については、次の URL に掲載されている『*Cisco IOS In Service Software Upgrade Process*』を参照してください。

http://www.cisco.com/en/US/docs/ios/ha/configuration/guide/ha-inserv_updg.html

7600 シリーズ ルータでの ISSU の詳細については、次の URL に掲載されている『*ISSU and eFSU on Cisco 7600 Series Routers*』を参照してください。

http://www.cisco.com/en/US/docs/routers/7600/ios/12.2SR/configuration/guide/efsuovrw.html

Cisco Catalyst 4500 シリーズのスイッチでの ISSU の詳細については、次の URL に掲載されている『*Catalyst 4500 Series Switch Cisco IOS Software Configuration Guide*, Release 12.2(31)SGA』の「Configuring the Cisco IOS In Service Software Upgrade Process」という章を参照してください。

http://www.cisco.com/en/US/docs/switches/lan/catalyst4500/12.2/31sga/configuration/guide/issu.html

SSO HSRP

SSO HSRP は、冗長な Route Processor（RP; ルート プロセッサ）を装備したルータが Stateful Switchover（SSO; ステートフル スイッチオーバー）冗長モード用に設定されているときの HSRP の動作を変更します。ある RP がアクティブで、もう一方の RP がスタンバイになっているとき、アクティブ RP に障害が発生すると、SSO は処理を引き継ぐスタンバイ RP をイネーブルにします。

この機能を使用すると、HSRP の SSO 情報がスタンバイ RP に同期されるため、HSRP 仮想 IP アドレスを使用して送信されるトラフィックをスイッチオーバー中も引き続き転送できるほか、データの損失やパスの変更も発生しません。さらに、HSRP アクティブ ルータの両方の RP に障害が発生しても、スタンバイ状態の HSRP ルータが HSRP アクティブ ルータとして処理を引き継ぎます。

この機能は、動作の冗長モードが SSO に設定されている場合にデフォルトでイネーブルになっています。

デュアル ルート プロセッサの SSO とシスコ ノンストップ フォワーディング

SSO は、デュアル RP をサポートするネットワーキング デバイス（通常はエッジ デバイス）で機能します。1 台の RP をアクティブ プロセッサとして設定し、他の RP をスタンバイ プロセッサとして設定することで、RP 冗長化を実現します。また、RP 間の重要なステート情報を同期するため、ネットワーク ステート情報は RP 間でダイナミックに維持されます。

一般的に、SSO は Cisco NonStop Forwarding（NSF; ノンストップ フォワーディング）とともに使用されます。Cisco NSF を使用すると、ルーティング プロトコルに関する情報をスイッチオーバー後に復旧している間、データ パケットの転送を既知のルートに沿って続行できます。NSF を使用している場合、ユーザがサービスの停止に遭遇することはあまりありません。

HSRP と SSO の協調動作

SSO HSRP により、Cisco IOS HSRP サブシステム ソフトウェアはスタンバイ RP が装備されていることと、システムが SSO 冗長モードで設定されていることを検出できます。さらに、アクティブ RP に障害が発生しても、HSRP グループ自体には何の変化も発生せず、トラフィックは現在アクティブなゲートウェイ ルータを通じて引き続き転送されます。

この機能が登場する前は、アクティブ ルータのプライマリ RP に障害が発生すると、プライマリ RP は HSRP グループへの参加を停止し、HSRP アクティブ ルータとして処理を引き継ぐ、グループの別のルータをアクティブにしていました。

SSO HSRP は、RP のスイッチオーバーを通じて HSRP 仮想 IP アドレス宛てのトラフィックの転送パスを維持するために必要です。

エッジ ルータで SSO を設定すると、イーサネット トラフィックが HSRP スタンバイ ルータにスイッチ オーバーされなくても、イーサネット リンクのトラフィックは RP のフェールオーバー中も存続できます（プリエンプションが有効になっている場合は、その後、フェールバックされます）。

（注） SSO が他の接続のトラフィック フローを保持しているときに HSRP トラフィックを冗長デバイスにスイッチする必要がある LAN セグメントがある場合は、**no standby sso** コマンドを使用して SSO HSRP をディセーブルにすることができます。

HSRP の BFD ピアリング

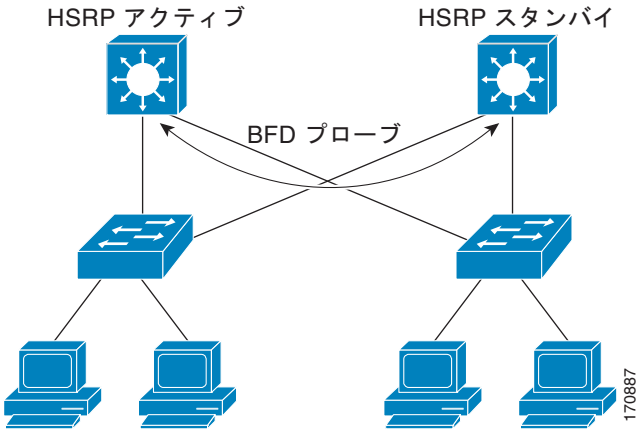
HSRP の BFD ピアリング機能により、HSRP グループ メンバーのヘルス モニタリング システムで BFD を使用できるようになりました。HSRP は、HSRP グループ メンバーのヘルス モニタリング システムの一部として BFD をサポートしています。BFD がないと、HSRP はマルチプロセス システムの 1 つのプロセスとして動作するため、ミリ秒の hello タイマーやホールド タイマーを使用して大量のグループに対応できるように適切なタイミングでスケジュールされることが保証されません。BFD は疑似プリエンプティブ プロセスとして動作するため、必要なときに実行されることが保証されます。複数の HSRP グループに早期フェールオーバー通知を実行できるのは、2 台のルータ間の 1 つの BFD セッションだけです。

この機能は、デフォルトでイネーブルにされています。HSRP スタンバイ ルータは、HSRP アクティブ ルータの実際の IP アドレスを HSRP hello メッセージから検出します。また、BFD クライアントとして登録し、アクティブ ルータが使用不能になった場合に通知するように要求します。

BFD は、インターフェイス、データ リンク、フォワーディング プレーンを含め、2 台の隣接ルータ間の転送パスの障害を検出する、オーバーヘッドが少なく、処理時間が短い方式です。また、BFD はインターフェイス レベルやルーティング プロトコル レベルでイネーブルにする検出プロトコルです。Cisco は、ルータ間の BFD ネイバーセッションをアクティブ化および維持するために 2 つのシステム間で BFD 制御パケットを送信する BFD 非同期モードをサポートしています。このため、BFD セッションを作成するためには、両方のシステム（または BFD ピア）で BFD を設定する必要があります。BFD がインターフェイスでイネーブルになっているとともに、HSRP 用にルータ レベルでイネーブルになっている場合、BFD セッションが作成されて、BFD タイマーがネゴシエートされ、ネゴシエートされた間隔で BFD ピアが互いに BFD 制御パケットの送信を開始します。

BFD による BFD ピアの障害検出が高速なのは、使用されているメディア タイプ、カプセル化、トポロジ、ルーティング プロトコル（BGP、EIGRP、HSRP、IS-IS、OSPF）が何であっても同じです。障害検出通知をローカル ルータのルーティング プロトコルにすばやく送信してルーティング テーブルの再計算プロセスを開始することによって、BFD はネットワーク全体のコンバージェンス時間を大幅に削減するのに役立っています。図 3 は、HSRP と BFD を実行している 2 台のルータのある単純なネットワークを示しています。

図 3　　HSRP の BFD ピアリング



BFD の詳細については、次の URL にアクセスして『*Cisco IOS IP Routing Configuration Guide*』の「Bidirectional Forwarding Detection」を参照してください。

http://www.cisco.com/en/US/docs/ios/iproute/configuration/guide/irp_bfd.html

HSRP MIB トラップ

HSRP Management Information Base（MIB; 管理情報ベース）は、Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）の GET 操作をサポートしているので、ネットワーク デバイスはネットワークの HSRP グループに関するレポートをネットワーク管理ステーションから取得することができます。

HSRP MIB トラップのサポートのイネーブル化は CLI で行います。また MIB はレポートの取得に使用されます。各トラップは、ルータがアクティブ ステートやスタンバイ ステートになったり、それらのステートから移行したりしたときにネットワーク管理ステーションに通知します。CLI からエントリを設定すると、直ちに、MIB でのそのグループの RowStatus がアクティブ ステートになります。

Cisco IOS ソフトウェアがサポートしているのは読み取り専用の MIB で、SET 操作はサポートしていません。

この機能は次の 4 つの MIB テーブルをサポートしています。

- CISCO-HSRP-MIB.my で定義されている cHsrpGrpEntry テーブル
- CISCO-HSRP-EXT-MIB.my で定義されている cHsrpExtIfTrackedEntry、cHsrpExtSecAddrEntry、cHsrpExtIfEntry

cHsrpGrpEntry テーブルは、各 HSRP グループの情報から構成されており、その他のテーブルは CISCO-HSRP-EXT-MIB.my で定義されている HSRP の Cisco 拡張で構成されています。

HSRP の設定方法

HSRP のイネーブル化

ここでは、HSRP をイネーブルにする作業を行います。

インターフェイス コンフィギュレーション コマンド **standby ip** は、設定されているインターフェイスで HSRP をアクティブ化します。指定されている IP アドレスがある場合は、そのアドレスがホット スタンバイ グループの仮想 IP アドレスとして使用されます。指定したルータが HSRP によって選出されるようにするには、グループの少なくとも 1 台のルータに仮想 IP アドレスを設定する必要があります。このアドレスはグループの他のルータによって検出されます。

前提条件

認証、タイマー、プライオリティ、プリエンプションなど、HSRP で多くのアトリビュートを設定できます。先にアトリビュートを設定してから、HSRP グループをイネーブルにするのが最も効率的な方法です。

この方法では、他のルータでの認証エラー メッセージや予期しないステートの変化が発生しません。これらの現象は、グループを先にイネーブルにし、他の設定を入力するまでに十分に長い遅延（1 つまたは 2 つのホールド タイム）があった場合に発生することがあります。

常に HSRP IP アドレスを指定することを推奨します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip address** *ip-address mask*
5. **standby** [*group-number*] **ip** [*ip-address* [**secondary**]]
6. **end**
7. **show standby** [**all**] [**brief**]
8. **show standby** *type number* [*group-number* | **all**] [**brief**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* 例： `Router(config)# interface ethernet 0`	インターフェイス タイプを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ip address** *ip-address mask* 例： `Router(config-if)# ip address 172.16.6.5 255.255.255.0`	インターフェイスの IP アドレスを設定します。
ステップ 5	**standby** [*group-number*] **ip** [*ip-address* [**secondary**]] 例： `Router(config-if)# standby 1 ip 172.16.6.100`	HSRP をアクティブにします。 • グループ番号は、指定しなければデフォルト値の 0 に設定されます。グループ番号の範囲は、HSRP バージョン 1 の場合は 0 ～ 255 で、HSRP バージョン 2 の場合は 0 ～ 4095 です。 • *ip-address* は仮想ルータの仮想 IP アドレスです。指定したルータが HSRP によって選出されるようにするには、グループの少なくとも 1 台のルータに仮想 IP アドレスを設定する必要があります。このアドレスはグループの他のルータによって検出されます。
ステップ 6	**end** 例： `Router(config-if)# end`	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 7	**show standby** [**all**] [**brief**] 例： Router# show standby	（任意）HSRP に関する情報を表示します。 • このコマンドを実行すると、各グループの情報が表示されます。**all** オプションを付けると、検出されたグループおよび **standby ip** コマンドが設定されていないグループが表示されます。
ステップ 8	**show standby** *type number* [*group-number* | **all**] [**brief**] 例： Router# show standby ethernet 0	（任意）特定のグループまたはインターフェイスの HSRP 関連の情報が表示されます。

インターフェイスでの HSRP の初期化の遅延

standby delay コマンドを使用して、インターフェイスのリロード後や起動後の HSRP の初期化を遅延します。この設定を行うと、インターフェイス起動イベントの後にインターフェイスやルータの状態が安定する時間を確保して、HSRP のステートが不安定になるのを防ぐことができます。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip address** *ip-address mask*
5. **standby delay minimum** *min-seconds* **reload** *reload-seconds*
6. **standby** [*group-number*] **ip** [*ip-address* [**secondary**]]
7. **end**
8. **show standby delay** [*type number*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： Router> enable	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： Router# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* 例： Router(config)# interface Ethernet0/1	インターフェイス タイプを設定し、インターフェイス コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	**ip address** *ip-address mask* 例： `Router(config-if)# ip address 10.0.0.1 255.255.255.0`	インターフェイスの IP アドレスを指定します。
ステップ 5	**standby delay minimum** *min-seconds* **reload** *reload-seconds* 例： `Router(config-if)# standby delay minimum 30 reload 60`	（任意）HSRP グループの初期化までの遅延時間を設定します。 • *min-seconds* の値は、インターフェイスの起動後に HSRP グループの初期化を遅延する最小時間（秒単位）です。この最小遅延時間は、インターフェイスの以降のイベントのすべてに適用されます。 • *reload-seconds* の値は、ルータのリロード後に遅延する時間です。この遅延時間は、ルータがリロードした後の最初のインターフェイス起動イベントにのみ適用されます。 **（注）** *min-seconds* および *reload-seconds* の値は、それぞれ 30 と 60 に設定することを推奨します。
ステップ 6	**standby** [*group-number*] **ip** [*ip-address* [**secondary**]] 例： `Router(config-if)# standby 1 ip 10.0.0.3 255.255.255.0`	HSRP をアクティブにします。
ステップ 7	**end** 例： `Router(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 8	**show standby delay** [*type number*] 例： `Router# show standby delay`	（任意）HSRP の遅延時間に関する情報を表示します。

トラブルシューティングのヒント

standby timers コマンドをミリ秒単位で設定する場合や、スイッチの VLAN インターフェイスで HSRP を設定する場合は、**standby delay minimum reload** コマンドを使用することを推奨します。

HSRP のプライオリティとプリエンプションの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip address** *ip-address mask*
5. **standby** [*group-number*] **priority** *priority*
6. **standby** [*group-number*] **preempt** [**delay** {**minimum** *delay* | **reload** *delay* | **sync** *delay*}]
7. **standby** [*group-number*] **ip** [*ip-address* [**secondary**]]
8. **end**
9. **show standby** [**all**] [**brief**]
10. **show standby** *type number* [*group-number* | **all**] [**brief**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* 例： `Router(config)# interface Ethernet0/1`	インターフェイス タイプを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ip address** *ip-address mask* 例： `Router(config-if)# ip address 10.0.0.1 255.255.255.0`	インターフェイスの IP アドレスを指定します。
ステップ 5	**standby** [*group-number*] **priority** *priority* 例： `Router(config-if)# standby 1 priority 110`	HSRP のプライオリティを設定します。 • デフォルトのプライオリティは 100 です。

	コマンドまたはアクション	目的
ステップ 6	**standby** [*group-number*] **preempt** [**delay** {**minimum** *delay* | **reload** *delay* | **sync** *delay*}] **例：** `Router(config-if)# standby 1 preempt delay minimum 380`	HSRP のプリエンプションとプリエンプション遅延を設定します。 • デフォルトの遅延時間は 0 秒です。つまり、ルータは最優位になれる場合、すぐに最優位になります。デフォルトでは、後で起動したルータはスタンバイ ルータになります。
ステップ 7	**standby** [*group-number*] **ip** [*ip-address* [**secondary**]] **例：** `Router(config-if)# standby 1 ip 10.0.0.3 255.255.255.0`	HSRP をアクティブにします。
ステップ 8	**end** **例：** `Router(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 9	**show standby** [**all**] [**brief**] **例：** `Router# show standby`	（任意）HSRP に関する情報を表示します。 • このコマンドを実行すると、各グループの情報が表示されます。**all** オプションを付けると、検出されたグループおよび **standby ip** コマンドが設定されていないグループが表示されます。
ステップ 10	**show standby** *type number* [*group-number* | **all**] [**brief**] **例：** `Router# show standby ethernet 0/1`	（任意）特定のグループまたはインターフェイスの HSRP 関連の情報が表示されます。

HSRP のオブジェクト トラッキングの設定

ここでは、オブジェクトをトラッキングし、そのステートに基づいて HSRP のプライオリティを変更するように HSRP を設定する作業を行います。

トラッキング対象の各オブジェクトは、トラッキング CLI で指定した一意の番号で識別されます。クライアント プロセスは、この番号を使用して特定のオブジェクトを追跡します。

オブジェクト トラッキングの詳細については、『Configuring Enhanced Object Tracking』を参照してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **track** *object-number* **interface** *type number* {**line-protocol** | **ip routing**}
4. **exit**
5. **interface** *type number*
6. **standby** [*group-number*] **track** *object-number* [**decrement** *priority-decrement*]
7. **standby** [*group-number*] **track** *object-number* **shutdown**
8. **standby** [*group-number*] **ip** [*ip-address* [**secondary**]]
9. **end**
10. **show track** [*object-number* | **brief**] [**interface** [**brief**] | **ip route** [**brief**] | **resolution** | **timers**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**track** *object-number* **interface** *type number* {**line-protocol** | **ip routing**} **例：** `Router(config)# track 100 interface serial2/0 line-protocol`	インターフェイスをトラッキングされるように設定し、トラッキング 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	**exit** **例：** `Router(config-track)# exit`	グローバル コンフィギュレーション モードに戻ります。

	コマンドまたはアクション	目的
ステップ 5	**interface** *type number* 例： `Router(config)# interface ethernet 2`	インターフェイス タイプを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 6	**standby** [*group-number*] **track** *object-number* [**decrement** *priority-decrement*] 例： `Router(config-if)# standby 1 track 100 decrement 20`	オブジェクトをトラッキングし、そのステートに基づいてホット スタンバイのプライオリティを変更するように HSRP を設定します。 • デフォルトでは、トラッキング対象のオブジェクトがダウンすると、ルータのプライオリティは 10 だけ引き下げられます。デフォルトの動作を変更するには、キーワードと引数の組み合わせの **decrement** *priority-decrement* を使用します。 • トラッキング対象の複数のオブジェクトがダウンした場合、*priority-decrement* の値が設定されていれば、設定されているプライオリティの減分値が累積されます。トラッキング対象のオブジェクトがダウンした場合、どのオブジェクトにもプライオリティの減分値が設定されていなければ、デフォルトの減分値は 10 で、累積されます。
ステップ 7	**standby** [*group-number*] **track** *object-number* **shutdown** 例： `Router(config-if)# standby 1 track 100 shutdown`	（任意）オブジェクトをトラッキングし、トラッキング対象のオブジェクトがダウンしたときに HSRP グループをディセーブルにするように HSRP を設定します。 • トラッキング対象のオブジェクトがダウンしたときにルータの HSRP グループをディセーブルにするには、**shutdown** キーワードを使用します。
ステップ 8	**standby** [*group-number*] **ip** [*ip-address* [**secondary**]] 例： `Router(config-if)# standby 1 ip 10.10.10.0`	HSRP をアクティブにします。 • デフォルトのグループ番号は 0 です。グループ番号の範囲は、HSRP バージョン 1 の場合は 0 ～ 255 で、HSRP バージョン 2 の場合は 0 ～ 4095 です。
ステップ 9	**end** 例： `Router(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 10	**show track** [*object-number* | **brief**] [**interface** [**brief**]| **ip route** [**brief**]| **resolution** | **timers**] 例： `Router# show track 100 interface`	トラッキング情報を表示します。

キー ストリングを使用した HSRP MD5 認証の設定

制約事項

HSRP グループにテキスト認証と MD5 認証を併用することはできません。MD5 認証が設定されている場合、受信側のルータの MD5 認証がイネーブルになっていれば、HSRP Hello メッセージのテキスト認証フィールドは転送時にすべてゼロに設定され、受信時に無視されます。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip address** *ip-address mask* [**secondary**]
5. **standby** [*group-number*] **priority** *priority*
6. **standby** [*group-number*] **preempt** [**delay** {**minimum** *delay* | **reload** *delay* | **sync** *delay*}]
7. **standby** [*group-number*] **authentication md5 key-string** [**0** | **7**] *key* [**timeout** *seconds*]
8. **standby** [*group-number*] **ip** [*ip-address* [**secondary**]]
9. 通信するルータごとにステップ 1 ～ 8 を繰り返します。
10. **end**
11. **show standby**

手順の詳細

	コマンド	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* 例： `Router(config)# interface Ethernet0/1`	インターフェイス タイプを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ip address** *ip-address mask* [**secondary**] 例： `Router(config-if)# ip address 10.0.0.1 255.255.255.0`	インターフェイスのプライマリ IP アドレスまたはセカンダリ IP アドレスを指定します。

	コマンド	目的
ステップ 5	**standby** [*group-number*] **priority** *priority* 例： `Router(config-if)# standby 1 priority 110`	HSRP のプライオリティを設定します。
ステップ 6	**standby** [*group-number*] **preempt** [**delay** {**minimum** *delay* | **reload** *delay* | **sync** *delay*}] 例： `Router(config-if)# standby 1 preempt`	HSRP のプリエンプションを設定します。
ステップ 7	**standby** [*group-number*] **authentication md5 key-string** [**0** | **7**] *key* [**timeout** *seconds*] 例： `Router(config-if)# standby 1 authentication md5 key-string d00b4r987654321a timeout 30`	HSRP MD5 認証の認証文字列を設定します。 • *key* 引数には最大 64 文字を設定できます。16 文字以上を使用することを推奨します。 • *key* 引数にはプレフィクスを指定しません。**0** を指定すると、キーは暗号化されないことを示します。 • **7** を指定するとキーは暗号化されます。**service password-encryption** グローバル コンフィギュレーション コマンドがイネーブルになっていると、key-string 認証キーは自動的に暗号化されます。 • タイムアウト値は、古いキー ストリングが受け入れられ、新しいキーを使用してグループ内のすべてのルータを設定できる時間です。
ステップ 8	**standby** [*group-number*] **ip** [*ip-address* [**secondary**]] 例： `Router(config-if)# standby 1 ip 10.0.0.3`	HSRP をアクティブにします。
ステップ 9	通信するルータごとにステップ 1 ～ 8 を繰り返します。	—
ステップ 10	**end** 例： `Router(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 11	**show standby** 例： `Router# show standby`	（任意）HSRP に関する情報を表示します。 • このコマンドを使用して、設定を確認します。キー ストリングまたはキー チェーンが表示されます（設定されている場合）。

トラブルシューティングのヒント

あるグループのルータのキー ストリングを変更する場合、アクティブ ルータを最後に変更して、HSRP ステートが変化しないようにします。アクティブ ルータのキー ストリングの変更は、アクティブでないルータの後、インターフェイス コンフィギュレーション コマンド **standby timers** によって指定されているホールド時間 1 回分の時間が経過する前に行われなければなりません。この手順により、アクティブでないルータでアクティブ ルータのタイムアウトが発生することがなくなります。

キー チェーンを使用した HSRP MD5 認証の設定

キー チェーンを使用すると、キー チェーンの設定に基づき、場合に応じて異なるキー ストリングを使用できます。HSRP は適切なキー チェーンを照会し、特定のキー チェーンに対して現在アクティブになっているキーとキー ID を取得します。

手順の概要

1. **enable**
2. **configure terminal**
3. **key chain** *name-of-chain*
4. **key** *key-id*
5. **key-string** *string*
6. **exit**
7. **interface** *type number*
8. **ip address** *ip-address mask* [**secondary**]
9. **standby** [*group-number*] **priority** *priority*
10. **standby** [*group-number*] **preempt** [**delay** {**minimum** *delay* | **reload** *delay* | **sync** *delay*}]
11. **standby** [*group-number*] **authentication md5 key-chain** *key-chain-name*
12. **standby** [*group-number*] **ip** [*ip-address* [**secondary**]]
13. 通信するルータごとにステップ 1 ～ 12 を繰り返します。
14. **end**
15. **show standby**

手順の詳細

	コマンド	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**key chain** *name-of-chain* 例： `Router(config)# key chain hsrp1`	ルーティング プロトコルの認証をイネーブルにし、認証キーのグループを識別します。
ステップ 4	**key** *key-id* 例： `Router(config-keychain)# key 100`	キー チェーンの認証キーを識別します。 • *key-id* は、数値で指定する必要があります。

	コマンド	目的
ステップ 5	**key-string** *string* 例： Router(config-keychain-key) # key-string mno172	キーの認証文字列を指定します。 • *string* には、1 ～ 80 文字の大文字と小文字の英数字を指定できます。ただし、最初の文字を数値にすることはできません。
ステップ 6	**exit** 例： Router(config-keychain-key) # exit	グローバル コンフィギュレーション モードに戻ります。
ステップ 7	**interface** *type number* 例： Router(config)# interface Ethernet0/1	インターフェイス タイプを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 8	**ip address** *ip-address mask* [**secondary**] 例： Router(config-if)# ip address 10.21.8.32 255.255.255.0	インターフェイスのプライマリ IP アドレスまたはセカンダリ IP アドレスを指定します。
ステップ 9	**standby** [*group-number*] **priority** *priority* 例： Router(config-if)# standby 1 priority 110	HSRP のプライオリティを設定します。
ステップ 10	**standby** [*group-number*] **preempt** [**delay** {**minimum** *delay* | **reload** *delay* | **sync** *delay*}] 例： Router(config-if)# standby 1 preempt	HSRP のプリエンプションを設定します。
ステップ 11	**standby** [*group-number*] **aut** **hentication md5** **key-chain** *key-chain-name* 例： Router(config-if)# standby 1 authentication md5 key-chain hsrp1	HSRP MD5 認証の認証 MD5 キー チェーンを設定します。 • キー チェーン名は、ステップ 3 で指定した名前と一致する必要があります。
ステップ 12	**standby** [*group-number*] **ip** [*ip-address* [**secondary**]] 例： Router(config-if)# standby 1 ip 10.21.8.12	HSRP をアクティブにします。

	コマンド	目的
ステップ 13	通信するルータごとにステップ 1 ～ 12 を繰り返します。	—
ステップ 14	**end** **例：** `Router(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 15	**show standby** **例：** `Router# show standby`	（任意）HSRP に関する情報を表示します。 • このコマンドを使用して、設定を確認します。キー ストリングまたはキー チェーンが表示されます（設定されている場合）。

HSRP MD5 認証のトラブルシューティング

ここでは、HSRP MD5 認証が正しく機能しない場合に行う作業を説明します。

手順の概要

1. **enable**
2. **debug standby errors**

手順の詳細

	コマンド	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**debug standby errors** **例：** `Router# debug standby errors`	HSRP 関連のエラー メッセージを表示します。 • エラー メッセージは、認証に失敗したパケットごとに表示されるため、このコマンドを使用するときは注意してください。 • 2 台のルータで認証が実行されないときに表示されるエラー メッセージの例については、「例」を参照してください。

例

次の例では、ルータ A には MD5 テキスト文字列認証が設定されていますが、ルータ B にはデフォルトのテキスト認証が設定されています。

```
Router# debug standby errors

A:Jun 16 12:14:50.337:HSRP:Et0/1 Grp 0 Auth failed for Hello pkt from 10.21.0.5, MD5
confgd but no tlv
B:Jun 16 12:16:34.287:HSRP:Et0/1 Grp 0 Auth failed for Hello pkt from 10.21.0.4, Text auth failed
```

次の例では、ルータ A とルータ B の両方に別々の MD5 認証文字列が設定されています。

```
Router# debug standby errors

A:Jun 16 12:19:26.335:HSRP:Et0/1 Grp 0 Auth failed for Hello pkt from 10.21.0.5, MD5 auth failed
B:Jun 16 12:18:46.280:HSRP:Et0/1 Grp 0 Auth failed for Hello pkt from 10.21.0.4, MD5 auth failed
```

HSRP テキスト認証の設定

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip address** *ip-address mask* [**secondary**]
5. **standby** [*group-number*] **priority** *priority*
6. **standby** [*group-number*] **preempt** [**delay** {**minimum** *delay* | **reload** *delay* | **sync** *delay*}]
7. **standby** [*group-number*] **authentication text** *string*
8. **standby** [*group-number*] **ip** [*ip-address* [**secondary**]]
9. 通信するルータごとにステップ 1 ～ 8 を繰り返します。
10. **end**
11. **show standby**

手順の詳細

	コマンド	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードなど、高位の権限レベルをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* 例： `Router(config)# interface Ethernet0/1`	インターフェイス タイプを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ip address** *ip-address mask* [**secondary**] 例： `Router(config-if)# ip address 10.0.0.1 255.255.255.0`	インターフェイスのプライマリ IP アドレスまたはセカンダリ IP アドレスを指定します。
ステップ 5	**standby** [*group-number*] **priority** *priority* 例： `Router(config-if)# standby 1 priority 110`	HSRP のプライオリティを設定します。

	コマンド	目的
ステップ 6	**standby** [*group-number*] **preempt** [**delay** {**minimum** *delay* | **reload** *delay* | **sync** *delay*}] **例：** `Router(config-if)# standby 1 preempt`	HSRP のプリエンプションを設定します。
ステップ 7	**standby** [*group-number*] **authentication text** *string* **例：** `Router(config-if)# standby 1 authentication text authentication1`	HSRP テキスト認証の認証文字列を設定します。 • デフォルトの文字列は「cisco」です。
ステップ 8	**standby** [*group-number*] **ip** [*ip-address* [**secondary**]] **例：** `Router(config-if)# standby 1 ip 10.0.0.3`	HSRP をアクティブにします。
ステップ 9	通信するルータごとにステップ 1 ～ 8 を繰り返します。	—
ステップ 10	**end** **例：** `Router(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 11	**show standby** **例：** `Router# show standby`	（任意）HSRP に関する情報を表示します。 • このコマンドを使用して、設定を確認します。キー ストリングまたはキー チェーンが表示されます（設定されている場合）。

HSRP タイマーの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip address** *ip-address mask* [**secondary**]
5. **standby** [*group-number*] **timers** [**msec**] *hellotime* [**msec**] *holdtime*
6. **standby** [*group-number*] **ip** [*ip-address* [**secondary**]]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* 例： `Router(config)# interface Ethernet0/1`	インターフェイス タイプを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ip address** *ip-address mask* [**secondary**] 例： `Router(config-if)# ip address 10.0.0.1 255.255.255.0`	インターフェイスのプライマリ IP アドレスまたはセカンダリ IP アドレスを指定します。
ステップ 5	**standby mac-refresh** *seconds* 例： `Router(config-if)# standby mac-refresh 100`	HSRP が FDDI で動作している場合に、MAC キャッシュをリフレッシュするためにパケットが送信される間隔を変更します。 • このコマンドは、FDDI で動作している HSRP にのみ適用されます。
ステップ 6	**standby** [*group-number*] **ip** [*ip-address* [**secondary**]] 例： `Router(config-if)# standby 1 ip 10.0.0.3`	HSRP をアクティブにします。

トラブルシューティングのヒント

hellotime と holdtime の最小値は、それぞれ 250 ミリ秒、800 ミリ秒に設定することを推奨します。

standby delay コマンドを使用すると、HSRP が初期化される前に、インターフェイスを完全に起動することが可能です。

HSRP MAC リフレッシュ インターバルの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip address** *ip-address mask* [**secondary**]
5. **standby mac-refresh** *seconds*
6. **standby** [*group-number*] **ip** [*ip-address* [**secondary**]]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* 例： `Router(config)# interface Ethernet0/1`	インターフェイス タイプを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ip address** *ip-address mask* [**secondary**] 例： `Router(config-if)# ip address 10.0.0.1 255.255.255.0`	インターフェイスのプライマリ IP アドレスまたはセカンダリ IP アドレスを指定します。
ステップ 5	**standby mac-refresh** *seconds* 例： `Router(config-if)# standby mac-refresh 100`	HSRP が FDDI で動作している場合に、MAC キャッシュをリフレッシュするためにパケットが送信される間隔を変更します。 • このコマンドは、FDDI で動作している HSRP にのみ適用されます。
ステップ 6	**standby** [*group-number*] **ip** [*ip-address* [**secondary**]] 例： `Router(config-if)# standby 1 ip 10.0.0.3`	HSRP をアクティブにします。

ロード バランシング用の複数の HSRP グループの設定

ここでは、ロード バランシングのために複数の HSRP グループを設定する作業を行います。

HSRP グループを複数にすると、ネットワークで冗長性を確保し、ロード シェアリングを実現できるほか、冗長ルータを余すところなく活用できるようになります。各ルータは、1 つの HSRP グループにトラフィックをアクティブに転送する一方、別のグループに対してスタンバイ ステートやリスン ステートになることができます。

2 台のルータを使用している場合、ルータ A はグループ 1 に対してアクティブと設定され、グループ 2 に対してスタンバイと設定されます。また、ルータ B はグループ 1 に対してスタンバイになり、グループ 2 に対してアクティブになります。LAN 上のホストの半数はグループ 1 の仮想 IP アドレスを使用して設定され、残りの半数はグループ 2 の仮想 IP アドレスを使用して設定されます。図および設定例については、「例：ロード バランシング用の複数の HSRP」（P.59）を参照してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip address** *ip-address mask* [**secondary**]
5. **standby** [*group-number*] **priority** *priority*
6. **standby** [*group-number*] **preempt** [**delay** {**minimum** *delay* | **reload** *delay* | **sync** *delay*}]
7. **standby** [*group-number*] **ip** [*ip-address* [**secondary**]]
8. 同じルータでステップ 5 ～ 7 を繰り返して、別のスタンバイ グループのルータ アトリビュートを設定します。
9. **exit**
10. もう 1 つのルータで、ステップ 3 ～ 9 を繰り返して HSRP を設定します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* 例： `Router(config)# interface Ethernet0/1`	インターフェイス タイプを設定し、インターフェイス コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	**ip address** *ip-address mask* [**secondary**] **例：** `Router(config-if)# ip address 10.0.0.1 255.255.255.0`	インターフェイスのプライマリ IP アドレスまたはセカンダリ IP アドレスを指定します。
ステップ 5	**standby** [*group-number*] **priority** *priority* **例：** `Router(config-if)# standby 1 priority 110`	HSRP のプライオリティを設定します。
ステップ 6	**standby** [*group-number*] **preempt** [**delay** {**minimum** *delay* | **reload** *delay* | **sync** *delay*}] **例：** `Router(config-if)# standby 1 preempt`	HSRP のプリエンプションを設定します。
ステップ 7	**standby** [*group-number*] **ip** [*ip-address* [**secondary**]] **例：** `Router(config-if)# standby 1 ip 10.0.0.3`	HSRP をアクティブにします。
ステップ 8	同じルータでステップ 5 ～ 7 を繰り返して、別のスタンバイ グループのルータ アトリビュートを設定します。	たとえば、ルータ A をグループ 1 のアクティブ ルータとして設定するとともに、別のプライオリティおよびプリエンプションの値を使用して別の HSRP グループのアクティブ ルータまたはスタンバイ ルータとして設定することができます。
ステップ 9	**exit** **例：** `Router(config-if)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 10	もう 1 つのルータでステップ 3 ～ 9 を繰り返します。	もう 1 つのルータで複数の HSRP を設定し、ロード バランシングをイネーブルにします。

HSRP 複数グループ最適化による CPU およびネットワークのパフォーマンスの向上

前の項の「「ロード バランシング用の複数の HSRP グループの設定」」の手順を行って HSRP マスター グループを設定してください。

ここでは、複数の HSRP クライアント グループを設定する作業を行います。

standby follow コマンドでは、別の HSRP グループのスレーブになるように HSRP グループを設定します。

HSRP クライアント グループがマスター HSRP に追従するときは短時間のランダムな遅延が発生するので、すべてのクライアント グループが同時に変化することはありません。

アクティブなクライアント グループは FDDI の MAC リフレッシュ メカニズムを使用して、マスター グループよりも長い間隔で hello パケットを送信します。デフォルトの間隔は 10 秒ですが、最大で 255 秒に設定することができます。

制約事項

- クライアント グループまたはスレーブ グループは、マスター グループと同じ物理インターフェイス上に存在していなければなりません。
- クライアント グループは、追従しているグループからステートを取得します。このため、クライアント グループは自身のタイマー設定、プライオリティ設定、プリエンプション設定を使用しません。これらの設定がクライアント グループに設定されている場合は、警告が表示されます。

```
Router(config-if)# standby 1 priority 110
%Warning: This setting has no effect while following another group.

Router(config-if)# standby 1 timers 5 15
% Warning: This setting has no effect while following another group.

Router(config-if)# standby 1 preempt delay minimum 300
% Warning: This setting has no effect while following another group.
```

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip address** *ip-address mask* [**secondary**]
5. **standby** *group-number* **follow** *group-name*
6. **exit**
7. ステップ 3 ～ 6 を繰り返して、さらに HSRP クライアント グループを設定します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* **例：** `Router(config)# interface Ethernet0/1`	インターフェイス タイプを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ip address** *ip-address mask* [**secondary**] **例：** `Router(config-if)# ip address 10.0.0.1 255.255.255.0`	インターフェイスのプライマリ IP アドレスまたはセカンダリ IP アドレスを指定します。
ステップ 5	**standby** *group-number* **follow** *group-name* **例：** `Router(config-if)# standby 1 follow HSRP1`	HSRP グループをクライアント グループとして設定します。
ステップ 6	**exit** **例：** `Router(config-if)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 7	ステップ 3 ～ 6 を繰り返して、さらに HSRP クライアント グループを設定します。	複数の HSRP クライアント グループを設定します。

HSRP の ICMP リダイレクト サポートのイネーブル化

デフォルトでは、ICMP リダイレクト メッセージの HSRP フィルタリングは、HSRP が実行されているルータでイネーブルになっています。ここでは、この機能がディセーブルになっている場合に、ルータでこの機能を再度イネーブルにする作業を行います。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **standby redirect** [**timers** *advertisement holddown*] [**unknown**]
5. **end**
6. **show standby redirect** [*ip-address*] [*interface-type interface-number*] [**active**] [**passive**] [**timers**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* 例： `Router(config)# interface Ethernet0/1`	インターフェイス タイプを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**standby redirect** [**timers** *advertisement holddown*] [**unknown**] 例： `Router(config-if)# standby redirect`	ICMP リダイレクト メッセージの HSRP フィルタリングをイネーブルにします。 • このコマンドは、グローバル コンフィギュレーション モードで使用することもできます。この場合、ICMP リダイレクト メッセージの HSRP フィルタリングが、HSRP 用に設定されているすべてのインターフェイスでイネーブルになります。
ステップ 5	**end** 例： `Router(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show standby redirect** [*ip-address*] [*interface-type interface-number*] [**active**] [**passive**] [**timers**] 例： `Router# show standby redirect`	（任意）HSRP を使用して設定されているインターフェイスの ICMP リダイレクト関連の情報を表示します。

HSRP 仮想 MAC アドレスまたは BIA MAC アドレスの設定

制約事項

standby use-bia コマンドと **standby mac-address** コマンドを同じ設定で使用することはできません。これらのコマンドは相互に排他的な関係にあります。

standby use-bia コマンドには次の欠点があります。

- あるルータがアクティブになると、その仮想 IP アドレスが別の MAC アドレスに移行されます。この新しいアクティブ ルータは、gratuitous ARP 応答を送信しますが、すべてのホスト実装で gratuitous ARP が正しく処理されるとは限りません。
- **standby use-bia** コマンドを設定すると、プロキシ ARP を使用できなくなります。ルータで障害が発生してプロキシ ARP データベースが失われても、スタンバイ ルータはそれに対応できなくなります。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip address** *ip-address mask* [**secondary**]
5. **standby** [*group-number*] **mac-address** *mac-address*
   または
   standby use-bia [**scope interface**]
6. **standby** [*group-number*] **ip** [*ip-address* [**secondary**]]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* 例： `Router(config)# interface Ethernet0/1`	インターフェイス タイプを設定し、インターフェイス コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	**ip address** *ip-address mask* [**secondary**] 例： `Router(config-if)# ip address 172.16.6.5 255.255.255.0`	インターフェイスの IP アドレスを設定します。
ステップ 5	**standby** [*group-number*] **mac-address** *mac-address* または **standby use-bia** [**scope interface**] 例： `Router(config-if)# standby 1 mac-address 5000.1000.1060` または 例： `Router(config-if)# standby use-bia`	HSRP の仮想 MAC アドレスを指定します。 • このコマンドは、トークン リング インターフェイスでは使用できません。 または 仮想 MAC アドレスとしてインターフェイスのバーンドイン アドレスを使用するように HSRP を設定します。 • **scope interface** キーワードでは、コマンドの設定対象が、メジャー インターフェイスではなく、コマンドを入力したサブインターフェイスに限定されるように指定されます。
ステップ 6	**standby** [*group-number*] **ip** [*ip-address* [**secondary**]] 例： `Router(config-if)# standby 1 ip 172.16.6.100`	HSRP をアクティブにします。

HSRP グループへの IP 冗長性クライアントのリンク

ここでは、IP 冗長性クライアントを HSRP グループにリンクする作業を行います。

HSRP により、IP ルーティングのステートレスな冗長性が実現されます。HSRP は、単独ではそれ自身のステートを管理することしかできません。HSRP グループに IP 冗長性クライアントをリンクすると、HSRP がクライアント アプリケーションにサービスを提供できるようになるため、このクライアント アプリケーションがステートフル フェールオーバーを実装できます。

IP 冗長性クライアントは、HSRP を使用して、グループのステートに応じてサービスやリソースを提供または抑制する他の Cisco IOS プロセスまたはアプリケーションです。

HSRP グループのデフォルトの名前は **hsrp**-*interface-group* であるため、グループ名の指定は省略可能です。たとえば、Ethernet0/0 のグループ 1 のデフォルトの名前は「hsrp-Et0/0-1」です。

前提条件

クライアント アプリケーションでは、**standby name** コマンドで設定したものと同じ名前を最初に指定する必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip address** *ip-address mask*
5. **standby** [*group-number*] **name** [*redundancy-name*]
6. **standby** [*group-number*] **ip** [*ip-address* [**secondary**]]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* 例： `Router(config)# interface Ethernet0/1`	インターフェイス タイプを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ip address** *ip-address mask* 例： `Router(config-if)# ip address 10.0.0.1 255.255.255.0`	インターフェイスの IP アドレスを指定します。
ステップ 5	**standby** [*group-number*] **name** [*redundancy-name*] 例： `Router(config-if)# standby 1 name HSRP-1`	スタンバイ グループの名前を設定します。 • HSRP グループのデフォルトの名前は **hsrp**-*interface-group* であるため、グループ名の指定は省略可能です。
ステップ 6	**standby** [*group-number*] **ip** [*ip-address* [**secondary**]] 例： `Router(config-if)# standby 1 ip 10.0.0.11`	HSRP をアクティブにします。

HSRP バージョン 2 への変更

HSRP バージョン 2 は、今後の機能拡張に備え、HSRP バージョン 1 よりも機能を拡張するために導入されました。HSRP バージョン 2 のパケット形式は、バージョン 1 とは異なります。

制約事項

- HSRP バージョン 2 は、LAN エミュレーションを実行している ATM インターフェイスでは使用できません。
- HSRP バージョン 2 は HSRP バージョン 1 と相互運用できません。バージョン 1 とバージョン 2 は相互に排他的な関係であるため、この両方を 1 つのインターフェイスで動作させることはできません。ただし、同じルータの別々の物理インターフェイスで、この別々のバージョンを実行することは可能です。バージョン 1 で許可されているグループ番号の範囲（0 ～ 255）よりも上のグループが設定されている場合、バージョン 2 からバージョン 1 に変更することはできません。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip address** *ip-address mask*
5. **standby version** {**1** | **2**}
6. **standby** [*group-number*] **ip** [*ip-address* [**secondary**]]
7. **end**
8. **show standby**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* 例： `Router(config)# interface vlan 400`	インターフェイス タイプを設定し、インターフェイス コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	**ip address** *ip-address mask* **例：** `Router(config-if)# ip address 10.10.28.1 255.255.255.0`	インターフェイスの IP アドレスを設定します。
ステップ 5	**standby version** {**1** | **2**} **例：** `Router(config-if)# standby version 2`	HSRP のバージョンを変更します。
ステップ 6	**standby** [*group-number*] **ip** [*ip-address* [**secondary**]] **例：** `Router(config-if)# standby 400 ip 10.10.28.5`	HSRP をアクティブにします。 • HSRP バージョン 2 のグループ番号範囲は 0 ～ 4095 に拡張されています。HSRP バージョン 1 のグループ番号範囲は 0 ～ 255 です。
ステップ 7	**end** **例：** `Router(config-if)# end`	現在の設定セッションを終了し、特権 EXEC モードに戻ります。
ステップ 8	**show standby** **例：** `Router# show standby`	（任意）HSRP に関する情報を表示します。 • HSRP バージョン 2 関連の情報が表示されます（設定されている場合）。

SSO 対応 HSRP のイネーブル化

この機能は、冗長モードが SSO に設定されている場合にデフォルトでイネーブルになっています。ここでは、SSO に対応するように HSRP を再度イネーブルにする作業を行います（ディセーブルになっている場合）。

（注） SSO が他の接続のトラフィック フローを保持しているときに HSRP トラフィックを冗長デバイスにスイッチする必要がある LAN セグメントがある場合は、**no standby sso** コマンドを使用して SSO HSRP をディセーブルにすることができます。

手順の概要

1. **enable**
2. **configure terminal**
3. **redundancy**
4. **mode sso**
5. **exit**
6. **no standby sso**
7. **standby sso**
8. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**redundancy** 例： `Router(config)# redundancy`	冗長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	**mode sso** 例： `Router(config-red)# mode sso`	SSO に対する動作の冗長モードをイネーブルにします。 • このステップを実行すると、HSRP 用に設定されているインターフェイスで HSRP の動作が SSO に対応した状態になり、スタンバイ RP が自動的にリセットされます。
ステップ 5	**exit** 例： `Router(config-red)# exit`	冗長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	**no standby sso** 例： `Router(config)# no standby sso`	すべての HSRP グループの HSRP SSO モードをディセーブルにします。
ステップ 7	**standby sso** 例： `Router(config)# standby sso`	SSO HSRP 機能をイネーブルにします（ディセーブルになっている場合）。
ステップ 8	**end** 例： `Router(config)# end`	現在の設定セッションを終了し、特権 EXEC モードに戻ります。

SSO 対応 HSRP の検証

HSRP の SSO 動作を検証またはデバッグするためには、次の手順をアクティブ RP コンソールで行います。

手順の概要

1. **show standby**
2. **debug standby events ha**

手順の詳細

ステップ 1 **show standby**

show standby コマンドを実行すると、スタンバイ RP のステートが表示されます。次に例を示します。

```
Router# show standby

GigabitEthernet3/25 - Group 1
State is Init (standby RP, peer state is Active)
Virtual IP address is 10.0.0.1
Active virtual MAC address is unknown
Local virtual MAC address is 0000.0c07.ac01 (v1 default)
Hello time 3 sec, hold time 10 sec
Preemption disabled
Active router is unknown
Standby router is unknown
Priority 100 (default 100)
Group name is "hsrp-Gi3/25-1" (default)
```

ステップ 2 **debug standby events ha**

debug standby events ha コマンドを実行すると、アクティブ RP とスタンバイ RP が表示されます。次に例を示します。

```
Router# debug standby events ha

!Active RP
```

```
*Sep 1 09:46:19.788 UTC: HSRP: Gi3/25 Grp 1 HA send sync state Listen
*Sep 1 09:46:31.435 UTC: HSRP: Gi3/25 Grp 1 HA send sync state Speak
*Sep 1 09:46:40.940 UTC: HSRP: Gi3/25 Grp 1 HA send sync state Standby
*Sep 1 09:46:41.724 UTC: HSRP: Gi3/25 Grp 1 HA send sync state Active

Standby RP

*Sep 1 09:46:19.143 UTC: STBY: HSRP: Gi3/25 Grp 1 RF sync state Unknown -> Init
*Sep 1 09:46:20.167 UTC: STBY: HSRP: Gi3/25 Grp 1 RF sync state Init -> Listen
*Sep 1 09:46:30.812 UTC: STBY: HSRP: Gi3/25 Grp 1 RF sync state Listen -> Speak
*Sep 1 09:46:41.315 UTC: STBY: HSRP: Gi3/25 Grp 1 RF sync state Speak -> Standby
*Sep 1 09:46:42.103 UTC: STBY: HSRP: Gi3/25 Grp 1 RF sync state Standby -> Active
```

HSRP MIB トラップのイネーブル化

手順の概要

1. **enable**
2. **configure terminal**
3. **snmp-server enable traps hsrp**
4. **snmp-server host** *host community-string* **hsrp**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**snmp-server enable traps hsrp** 例： `Router(config)# snmp-server enable traps hsrp`	SNMP トラップ、SNMP インフォーム、HSRP 通知をルータが送信できるようにします。
ステップ 4	**snmp-server host** *host community-string* **hsrp** 例： `Router(config)# snmp-server host myhost.comp.com public hsrp`	SNMP 通知動作の受信者と、HSRP 通知がホストに送信されることを指定します。

インターフェイスでの BFD セッション パラメータの設定

ここでは、BFD セッションのベースライン パラメータをインターフェイスで設定して、インターフェイスで BFD を設定する作業を行います。この手順のステップは、BFD ネイバーに BFD セッションを実行する各インターフェイスで行ってください。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **bfd interval** *milliseconds* **min_rx** *milliseconds* **multiplier** *interval-multiplier*
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* 例： `Router(config)# interface FastEthernet 6/0`	インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**bfd interval** *milliseconds* **min_rx** *milliseconds* **multiplier** *interval-multiplier* 例： `Router(config-if)# bfd interval 50 min_rx 50 multiplier 5`	インターフェイスで BFD をイネーブルにします。
ステップ 5	**end** 例： `Router(config-if)# end`	インターフェイス コンフィギュレーション モードを終了します。

HSRP BFD ピアリングの設定

ここでは、HSRP BFD ピアリングをイネーブルにする作業を行います。この手順のステップは、HSRP ピアに BFD セッションを実行する各インターフェイスで行ってください。

HSRP はデフォルトで BFD ピアリングをサポートしています。HSRP BFD ピアリングは、手動でディセーブルになっている場合、ルータ レベルで再度イネーブルにして、すべてのインターフェイスの BFD サポートをまとめてイネーブル化したり、インターフェイス レベルでインターフェイスごとに再度イネーブルにしたりすることができます。

前提条件

- 参加中のすべてのルータで HSRP が実行されている。
- Cisco Express Forwarding（CEF; シスコ エクスプレス フォワーディング）がイネーブルになっている。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip cef** [**distributed**]
4. **interface** *type number*
5. **ip address** *ip-address mask*
6. **standby** [*group-number*] **ip** [*ip-address* [**secondary**]]
7. **standby bfd**
8. **exit**
9. **standby bfd all-interfaces**
10. **exit**
11. **show standby** [**neighbors**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip cef** [**distributed**] 例： `Router(config)# ip cef`	CEF または分散 CEF をイネーブルにします。

	コマンドまたはアクション	目的
ステップ 4	**interface** *type number* 例： `Router(config)# interface FastEthernet 6/0`	インターフェイス コンフィギュレーション モードを開始します。
ステップ 5	**ip address** *ip-address mask* 例： `Router(config-if)# ip address 10.0.0.11 255.255.255.0`	インターフェイスの IP アドレスを設定します。
ステップ 6	**standby** [*group-number*] **ip** [*ip-address* [**secondary**]] 例： `Router(config-if)# standby 1 ip 10.0.0.11`	HSRP をアクティブにします。
ステップ 7	**standby bfd** 例： `Router(config-if)# standby bfd`	（任意）インターフェイスで HSRP の BFD サポートをイネーブルにします。
ステップ 8	**exit** 例： `Router(config-if)# exit`	インターフェイス 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	**standby bfd all-interfaces** 例： `Router(config)# standby bfd all-interfaces`	（任意）すべてのインターフェイスで HSRP の BFD サポートをイネーブルにします。
ステップ 10	**exit** 例： `Router(config)# exit`	グローバル コンフィギュレーション モードを終了します。
ステップ 11	**show standby** [**neighbors**] 例： `Router# show standby neighbors`	（任意）HSRP の BFD サポートに関する情報を表示します。

HSRP BFD ピアリングの検証

HSRP BFD ピアリングを検証するには、次のコマンドを必要に応じて実行します。

手順の概要

1. **show standby**
2. **show standby neighbors** [*type number*]
3. **show bfd neighbor** [**details**]

手順の詳細

ステップ 1 **show standby**

show standby コマンドを実行すると、HSRP に関する情報が表示されます。

```
Router# show standby

FastEthernet2/0 - Group 1
  State is Active
    2 state changes, last state change 00:08:06
  Virtual IP address is 10.0.0.11
  Active virtual MAC address is 0000.0c07.ac01
    Local virtual MAC address is 0000.0c07.ac01 (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 2.772 secs
  Preemption enabled
  Active router is local
  Standby router is 10.0.0.2, priority 90 (expires in 8.268 sec)
    BFD enabled !
  Priority 110 (configured 110)
    Group name is "hsrp-Fa2/0-1" (default)
```

ステップ 2 **show standby neighbors** [*type number*]

show standby neighbors コマンドを実行すると、インターフェイスの HSRP ピア ルータに関する情報が表示されます。

```
Router1# show standby neighbors

HSRP neighbors on FastEthernet2/0
    10.1.0.22
    No active groups
    Standby groups: 1
    BFD enabled !

Router2# show standby neighbors

HSRP neighbors on FastEthernet2/0
    10.0.0.2
    Active groups: 1
    No standby groups
    BFD enabled !
```

ステップ 3 **show bfd neighbors** [**details**]

show bfd neighbors コマンドを実行すると、現在の Bidirectional Forwarding Detection（BFD; 双方向フォワーディング検出）の隣接関係が 1 行ずつ一覧表示されます。**details** キーワードを付けると、各ネイバーの BFD プロトコルのパラメータとタイマーが表示されます。

```
Router# show bfd neighbors details

OurAddr       NeighAddr     LD/RD  RH/RS   Holdown(mult)  State     Int
10.0.0.2      10.0.0.1       5/0    Down      0    (0 )   Down      Fa2/0
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 1000000, MinRxInt: 1000000, Multiplier: 3
Received MinRxInt: 0, Received Multiplier: 0
Holdown (hits): 0(0), Hello (hits): 1000(55)
Rx Count: 0, Rx Interval (ms) min/max/avg: 0/0/0 last: 3314120 ms ago
Tx Count: 55, Tx Interval (ms) min/max/avg: 760/1000/872 last: 412 ms ago
Registered protocols: HSRP !
Last packet: Version: 1            - Diagnostic: 0
             State bit: AdminDown  - Demand bit: 0
             Poll bit: 0           - Final bit: 0
             Multiplier: 0         - Length: 0
             My Discr.: 0          - Your Discr.: 0
             Min tx interval: 0    - Min rx interval: 0
             Min Echo interval: 0
```

HSRP gratuitous ARP の設定

ここでは、ARP キャッシュのエントリが正しいことを確認し、1 つまたは複数のアクティブ HSRP グループから gratuitous ARP パケットを定期的に送信するように HSRP を設定する作業を行います。HSRP は、デフォルトでは HSRP グループのステートが Active に変化したときに、そのグループから gratuitous ARP パケットを 3 個送信します。最初の 1 個はグループがアクティブになったときに送信しますが、残りの 2 個が送信されるのは 2 秒後と 4 秒後です。

手順の概要

1. **enable**
2. **standby send arp** [*interface-type interface-number* [*group-number*]]
3. **configure terminal**
4. **interface** *type number*
5. **standby arp gratuitous** [**count** *number*] [**interval** *seconds*]
6. **end**
7. **show standby arp gratuitous** [*type number*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**standby send arp** [*interface-type interface-number* [*group-number*]] **例：** `Router# standby send arp Ethernet1/1 1`	（任意）アクティブ HSRP グループごとに 1 つの gratuitous ARP パケットを送信するように HSRP を設定します。

	コマンドまたはアクション	目的
ステップ 3	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 4	**interface** *type number* 例： `Router(config)# interface Ethernet1/1`	インターフェイス タイプを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 5	**standby arp gratuitous** [**count** *number*] [**interval** *seconds*] 例： `Router(config-if)# standby arp gratuitous count 3 interval 4`	アクティブ HSRP グループによって送信される gratuitous ARP パケットの数と送信頻度を設定します。
ステップ 6	**end** 例： `Router(config-if)# end`	（任意）特権 EXEC モードに戻ります。
ステップ 7	**show standby arp gratuitous** [*type number*] 例： `Router# show standby arp gratuitous ethernet1/1`	（任意）HSRP によって送信される gratuitous ARP パケットの数と、設定されている送信間隔を表示します。

例

次のサンプルは、**show standby arp gratuitous** コマンドからの出力です。

```
Router# show standby arp gratuitous ethernet1/1

HSRP Gratuitous ARP
Interface          Interval  Count
Ethernet1/1 4         3
```

HSRP の設定例

例：HSRP のプライオリティとプリエンプション

次の例では、ルータ A は、ルータ B よりもプライオリティが高いためにグループ 1 のアクティブ ルータになっているほか、グループ 2 のスタンバイ ルータになっています。ルータ B は、グループ 2 のアクティブ ルータおよびグループ 1 のスタンバイ ルータになるように設定されています。

ルータ A の設定

```
Router(config)# interface Ethernet0/0
Router(config-if)# ip address 10.1.0.21 255.255.0.0
Router(config-if)# standby 1 priority 110
Router(config-if)# standby 1 preempt
Router(config-if)# standby 1 ip 10.1.0.1
Router(config-if)# standby 2 priority 95
Router(config-if)# standby 2 preempt
Router(config-if)# standby 2 ip 10.1.0.2
```

ルータ B の設定

```
Router(config)# interface Ethernet0/0
Router(config-if)# ip address 10.1.0.22 255.255.0.0
Router(config-if)# standby 1 preempt
Router(config-if)# standby 1 priority 105
Router(config-if)# standby 1 ip 10.1.0.1
Router(config-if)# standby 2 priority 110
Router(config-if)# standby 2 preempt
Router(config-if)# standby 2 ip 10.1.0.2
```

例：HSRP オブジェクト トラッキング

次の例では、トラッキング プロセスはシリアル インターフェイス 1/0 の IP ルーティング機能を追跡するように設定されています。イーサネット インターフェイス 0/0 の HSRP は、シリアル インターフェイス 1/0 の IP ルーティング ステートに何らかの変更が生じた場合には通知されるように、トラッキング プロセスに登録します。シリアル インターフェイス 1/0 の IP ステートがダウンになると、その HSRP グループのプライオリティが 10 だけ引き下げられます。

両方のシリアル インターフェイスが動作している場合は、ルータ A はルータ B よりもプライオリティが高いので、ルータ A が HSRP アクティブ ルータになります。ただし、ルータ A のシリアル インターフェイス 1/0 の IP ルーティングに障害が発生すると、HSRP グループのプライオリティが引き下げられてルータ B がアクティブ ルータとして処理を引き継ぐため、ホストに対するデフォルトの仮想ゲートウェイ サービスはサブネット 10.1.0.0 で継続されます。

ルータ A の設定

```
Router(config)# track 100 interface serial1/0 ip routing
Router(config-track)# exit
Router(config)# interface Ethernet0/0
Router(config-if)# ip address 10.1.0.21 255.255.0.0
Router(config-if)# standby 1 preempt
Router(config-if)# standby 1 priority 110
Router(config-if)# standby 1 track 100 decrement 10
Router(config-if)# standby 1 ip 10.1.0.1
```

ルータ B の設定

```
Router(config)# track 100 interface serial1/0 ip routing
Router(config-track)# exit
Router(config)# interface Ethernet0/0
Router(config-if)# ip address 10.1.0.22 255.255.0.0
Router(config-if)# standby 1 preempt
Router(config-if)# standby 1 priority 105
Router(config-if)# standby 1 track 100 decrement 10
Router(config-if)# standby 1 ip 10.1.0.1
```

例：HSRP グループ シャットダウン

次の例では、トラッキング プロセスはシリアル インターフェイス 1/0 の IP ルーティング機能を追跡するように設定されています。イーサネット インターフェイス 0/0 の HSRP は、シリアル インターフェイス 1/0 の IP ルーティング ステートに何らかの変更が生じた場合には通知されるように、トラッキング プロセスに登録します。シリアル インターフェイス 1/0 の IP ステートがダウンになると、HSRP グループはディセーブルになります。

両方のシリアル インターフェイスが動作している場合は、ルータ A はルータ B よりもプライオリティが高いので、ルータ A が HSRP アクティブ ルータになります。ただし、ルータ A のシリアル インターフェイス 1/0 の IP ルーティングに障害が発生すると、HSRP グループがディセーブルになってルータ B がアクティブ ルータとして処理を引き継ぐため、ホストに対するデフォルトの仮想ゲートウェイ サービスはサブネット 10.1.0.0 で継続されます。

ルータ A の設定

```
Router(config)# track 100 interface serial1/0 ip routing
Router(config-track)# exit
Router(config)# interface Ethernet0/0
Router(config-if)# ip address 10.1.0.21 255.255.0.0
Router(config-if)# standby 1 ip 10.1.0.1
Router(config-if)# standby 1 preempt
```

```
Router(config-if)# standby 1 priority 110
Router(config-if)# standby 1 track 100 shutdown
```

ルータ B の設定

```
Router(config)# track 100 interface serial1/0 ip routing
Router(config-track)# exit
Router(config)# interface Ethernet0/0
Router(config-if)# ip address 10.1.0.22 255.255.0.0
Router(config-if)# standby 1 ip 10.1.0.1
Router(config-if)# standby 1 preempt
Router(config-if)# standby 1 priority 105
Router(config-if)# standby 1 track 100 shutdown
```

あるオブジェクトが HSRP グループによってすでにトラッキングされている場合、HSRP グループ シャットダウン機能を使用するようにこのトラッキング設定を変更することはできません。先に、**no standby track** コマンドを使用してトラッキング設定を解除し、**shutdown** キーワードとともに **standby track** コマンドを使用してトラッキング設定を再度設定する必要があります。

次の例は、HSRP グループ シャットダウン機能が追加されるようにトラッキング対象のオブジェクトの設定を変更する方法を示しています。

```
Router(config-if)# no standby 1 track 101 decrement 10
Router(config-if)# standby 1 track 101 shutdown
```

例：キー ストリングを使用した HSRP MD5 認証

次に、キー ストリングを使用して HSRP MD5 認証を設定する例を示します。

```
Router(config)# interface Ethernet0/1
Router(config-if)# standby 1 priority 110
Router(config-if)# standby 1 preempt
Router(config-if)# standby 1 authentication md5 key-string 54321098452103ab timeout 30
Router(config-if)# standby 1 ip 10.21.0.10
```

例：キー チェーンを使用した HSRP MD5 認証

次の例では、特定のキー チェーンに対して現在アクティブになっているキーとキー ID を取得するため、HSRP にはキー チェーン「hsrp1」が必要です。

```
Router(config)# key chain hsrp1
Router(config-keychain)# key 1
Router(config-keychain-key)# key-string 54321098452103ab
Router(config-keychain-key)# exit
Router(config)# interface Ethernet0/1
Router(config-if)# standby 1 priority 110
Router(config-if)# standby 1 preempt
Router(config-if)# standby 1 authentication md5 key-chain hsrp1
Router(config-if)# standby 1 ip 10.21.0.10
```

例：キー ストリングとキー チェーンを使用した HSRP MD5 認証

キー ストリング認証のキー ID は常にゼロです。キー チェーンのキー ID がゼロに設定されている場合、次のように設定できます。

ルータ 1

```
Router(config)# key chain hsrp1
```

```
Router(config-keychain)# key 0
Router(config-keychain-key)# key-string 54321098452103ab
Router(config-keychain-key)# exit
Router(config)# interface Ethernet0/1

Router(config-if)# standby 1 authentication md5 key-chain hsrp1
Router(config-if)# standby 1 ip 10.21.0.10
```

ルータ 2

```
Router(config)# interface Ethernet0/1
Router(config-if)# standby 1 authentication md5 key-string 54321098452103ab
Router(config-if)# standby 1 ip 10.21.0.10
```

例：HSRP テキスト認証

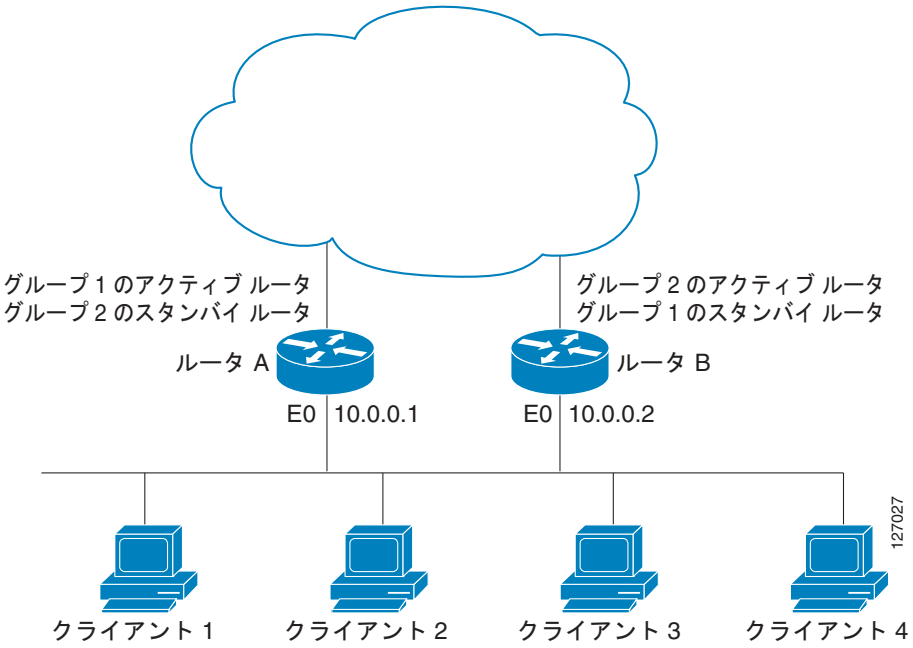
次の例は、テキスト文字列を使用して HSRP テキスト認証を設定する方法を示しています。

```
Router(config)# interface Ethernet0/1
Router(config-if)# standby 1 priority 110
Router(config-if)# standby 1 preempt
Router(config-if)# standby 1 authentication text company2
Router(config-if)# standby 1 ip 10.21.0.10
```

例：ロード バランシング用の複数の HSRP

ロード シェアリングを設定するときは、HSRP または複数の HSRP グループを使用できます。図 4 では、クライアントの半数はルータ A 用に設定され、残りの半数はルータ B 用に設定されています。ルータ A とルータ B の設定が組み合わされて、2 つのホット スタンバイ グループが確立されています。グループ 1 では、ルータ A に最も高いプライオリティが割り当てられているため、ルータ A がデフォルトのアクティブ ルータであり、ルータ B がスタンバイ ルータです。グループ 2 では、ルータ B に最も高いプライオリティが割り当てられているため、ルータ B がデフォルトのアクティブ ルータであり、ルータ A がスタンバイ ルータです。通常の動作中は、2 つのルータに IP トラフィックの負荷が共有されます。どちらかのルータが使用不能になると、もう一方のルータがアクティブになり、使用不能になったルータのパケット転送機能を引き継ぎます。ルータが停止し、後で復帰した場合に、プリエンプションを実行してロード シェアリング状態に戻すために、インターフェイス コンフィギュレーション コマンド **standby preempt** が必要です。

図 4　　HSRP ロード シェアリングの例



次の例は、プライオリティが 110 で、グループ 1 のアクティブ ルータとして設定されているルータ A と、プライオリティが 110 で、グループ 2 のアクティブ ルータとして設定されているルータ B を示しています。デフォルトのプライオリティ レベルは 100 です。グループ 1 で使用されている仮想 IP アドレスは 10.0.0.3 で、グループ 2 で使用されている仮想 IP アドレスは 10.0.0.4 です。

ルータ A の設定

```
Router(config)# hostname RouterA
RouterA(config)# interface ethernet 0
RouterA(config-if)# ip address 10.0.0.1 255.255.255.0
RouterA(config-if)# standby 1 ip 10.0.0.3
RouterA(config-if)# standby 1 priority 110
RouterA(config-if)# standby 1 preempt
RouterA(config-if)# standby 2 preempt
RouterA(config-if)# standby 2 ip 10.0.0.4
```

ルータ B の設定

```
Router(config)# hostname RouterB
RouterB(config)# interface ethernet 0
RouterB(config-if)# ip address 10.0.0.2 255.255.255.0
RouterB(config-if)# standby 1 ip 10.0.0.3
RouterB(config-if)# standby 1 preempt
RouterB(config-if)# standby 2 priority 110
RouterB(config-if)# standby 2 preempt
RouterB(config-if)# standby 2 ip 10.0.0.4
```

例：HSRP 複数グループ最適化を使用した CPU およびネットワークのパフォーマンスの向上

次の例は、HSRP クライアントおよびマスター グループを設定する方法を示しています。

```
Router(config)# interface Ethernet1/0
Router(config-if)# no shutdown
Router(config-if)# standby mac-refresh 30
! Client Hello message interval
!
Router(config)# interface Ethernet1/0.2
Router(config-if)# no shutdown
Router(config-if)# encapsulation dot1Q 2
Router(config-if)# ip vrf forwarding VRF2
Router(config-if)# ip address 10.0.0.100 255.255.0.0
Router(config-if)# standby 1 ip 10.0.0.254
Router(config-if)# standby 1 priority 110
Router(config-if)# standby 1 preempt
Router(config-if)# standby 1 name HSRP1
!Server group
!
Router(config)# interface Ethernet1/0.3
Router(config-if)# no shutdown
Router(config-if)# encapsulation dot1Q 3
Router(config-if)# ip vrf forwarding VRF3
Router(config-if)# ip address 10.0.0.100 255.255.0.0
Router(config-if)# standby 2 ip 10.0.0.254
Router(config-if)# standby 2 follow HSRP1
! Client group
!
Router(config)# interface Ethernet1/0.4
Router(config-if)# no shutdown
Router(config-if)# encapsulation dot1Q 4
Router(config-if)# ip vrf forwarding VRF4
Router(config-if)# ip address 10.0.0.100 255.255.0.0
Router(config-if)# standby 2 ip 10.0.0.254
Router(config-if)# standby 2 follow HSRP1
! Client group
```

例：ICMP リダイレクト メッセージの HSRP サポート

次の設定例は、ICMP リダイレクト メッセージのフィルタリングが可能な 2 つの HSRP グループです。

ルータ A の設定：グループ 1 に対してはアクティブでグループ 2 に対してはスタンバイ

```
RouterA(config)# interface Ethernet1
RouterA(config-if)# ip address 10.0.0.10 255.0.0.0
RouterA(config-if)# standby redirect
RouterA(config-if)# standby 1 priority 120
RouterA(config-if)# standby 1 preempt delay minimum 20
RouterA(config-if)# standby 1 ip 10.0.0.1
RouterA(config-if)# standby 2 priority 105
RouterA(config-if)# standby 2 preempt delay minimum 20
RouterA(config-if)# standby 2 ip 10.0.0.2
```

ルータ B の設定：グループ 1 に対してはスタンバイでグループ 2 に対してはアクティブ

```
RouterB(config)# interface Ethernet1
RouterB(config-if)# ip address 10.0.0.11 255.0.0.0
RouterB(config-if)# standby redirect
```

```
RouterB(config-if)# standby 1 priority 105
RouterB(config-if)# standby 1 preempt delay minimum 20
RouterB(config-if)# standby 1 ip 10.0.0.1
RouterB(config-if)# standby 2 priority 120
RouterB(config-if)# standby 2 preempt delay minimum 20
RouterB(config-if)# standby 2 ip 10.0.0.2
```

例：HSRP 仮想 MAC アドレスと BIA MAC アドレス

APPN ネットワークでは、エンドノードは隣接するネットワーク ノードの MAC アドレスを使用して設定されていることがほとんどです。次の例では、エンドノードが 4000.1000.1060 を使用するように設定されている場合、HSRP グループ 1 は同じ MAC アドレスを使用するように設定されます。

```
Router(config)# interface Ethernet0/2
Router(config-if)# ip address 10.0.0.1
Router(config-if)# standby 1 mac-address 4000.1000.1060
Router(config-if)# standby 1 ip 10.0.0.11
```

次の例では、トークン リング インターフェイス 3/0 のバーンドイン アドレスは、仮想 IP アドレスにマッピングされる仮想 MAC アドレスになります。

```
Router(config)# interface token3/0
Router(config-if)# standby use-bia
```

（注） **standby use-bia** コマンドと **standby mac-address** コマンドを同じ設定で使用することはできません。

例：HSRP グループへの IP 冗長性クライアントのリンク

次の例は、HSRP のスタティック NAT 設定サポートを示しています。NAT クライアント アプリケーションは、**standby name** コマンドで指定される名前の相互関係によって HSRP にリンクされます。また、2 台のルータが HSRP アクティブ ルータと HSRP スタンバイ ルータとして動作しているほか、インターフェイス内の NAT は HSRP が使用可能になっており、「group1」という名前のグループに属するように設定されています。

アクティブ ルータの設定

```
Router(config)# interface BVI10
Router(config-if)# ip address 192.168.5.54 255.255.255.255.0
Router(config-if)# no ip redirects
Router(config-if)# ip nat inside
Router(config-if)# standby 10 ip 192.168.5.30
Router(config-if)# standby 10 priority 110
Router(config-if)# standby 10 preempt
Router(config-if)# standby 10 name group1
Router(config-if)# standby 10 track Ethernet2/1
!
!
Router(config)# ip default-gateway 10.0.18.126
Router(config)# ip nat inside source static 192.168.5.33 10.10.10.5 redundancy group1
Router(config)# ip classless
Router(config)# ip route 10.10.10.0 255.255.255.0 Ethernet2/1
Router(config)# ip route 172.22.33.0 255.255.255.0 Ethernet2/1
Router(config)# no ip http server
```

スタンバイ ルータの設定

```
Router(config)# interface BVI10
Router(config-if)# ip address 192.168.5.56 255.255.255.255.0
```

```
Router(config-if)# no ip redirects
Router(config-if)# ip nat inside
Router(config-if)# standby 10 priority 95
Router(config-if)# standby 10 preempt
Router(config-if)# standby 10 name group1
Router(config-if)# standby 10 ip 192.168.5.30
Router(config-if)# standby 10 track Ethernet3/1
Router(config-if)# exit
Router(config)# ip default-gateway 10.0.18.126
Router(config)# ip nat inside source static 192.168.5.33 3.3.3.5 redundancy group1
Router(config)# ip classless
Router(config)# ip route 10.0.32.231 255.255.255 Ethernet3/1
Router(config)# ip route 10.10.10.0 255.255.255.0 Ethernet3/1
Router(config)# no ip http server
```

例：HSRP バージョン 2

次の例は、グループ番号が 350 のインターフェイスで HSRP バージョン 2 を設定する方法を示しています。

```
Router(config)# interface vlan350
Router(config-if)# standby version 2
Router(config-if)# standby 350 priority 110
Router(config-if)# standby 350 preempt
Router(config-if)# standby 350 timers 5 15
Router(config-if)# standby 350 ip 172.20.100.10
```

例：SSO HSRP

次の例は、冗長モードを SSO に設定する方法を示しています。このモードがイネーブルになっていると、HSRP は自動的に SSO に対応します。

```
Router(config)# redundancy
Router(config-red)# mode sso
```

no standby sso コマンドを使用して SSO HSRP をディセーブルにしている場合は、**standby sso** コマンドをグローバル コンフィギュレーション モードで使用して SSO HSRP を再度イネーブルにすることができます。

例：HSRP MIB トラップ

次の例は、HSRP を 2 台のルータで設定し、HSRP MIB トラップのサポート機能をイネーブルにする方法を示しています。多くの環境と同様に、1 台のルータがアクティブ ルータとして優先されます。あるルータにアクティブ ルータとしての優先度を設定するには、他のルータよりも高いプライオリティ レベルでそのルータを設定し、プリエンプションをイネーブルにします。次の例では、アクティブ ルータはプライマリ ルータと呼ばれ、2 番目のルータはバックアップ ルータと呼ばれます。

ルータ A

```
RouterA(config)# interface Ethernet1
RouterA(config-if)# ip address 10.1.1.1 255.255.0.0
RouterA(config-if)# standby priority 200
RouterA(config-if)# standby preempt
RouterA(config-if)# standby ip 10.1.1.3
RouterA(config-if)# exit
RouterA(config)# snmp-server enable traps hsrp
RouterA(config)#snmp-server host yourhost.cisco.com public hsrp
```

ルータ B

```
RouterB(config)# interface Ethernet1
RouterB(config-if)# ip address 10.1.1.2 255.255.0.0
RouterB(config-if)# standby priority 101
RouterB(config-if)# standby ip 10.1.1.3
RouterB(config-if)# exit
RouterB(config)# snmp-server enable traps hsrp
RouterB(config)# snmp-server host myhost.cisco.com public hsrp
```

例：HSRP BFD ピアリング

HSRP は、HSRP グループ メンバーのヘルス モニタリング システムの一部として BFD をサポートしています。BFD がないと、HSRP はマルチプロセス システムの 1 つのプロセスとして動作するため、ミリ秒の hello タイマーやホールド タイマーを使用して大量のグループに対応できるように適切なタイミングでスケジュールされることが保証されません。BFD は疑似プリエンプティブ プロセスとして動作するため、必要なときに実行されることが保証されます。複数の HSRP グループに早期フェールオーバー通知を実行できるのは、2 台のルータ間の 1 つの BFD セッションだけです。

次の例では、**standby bfd** コマンドと **standby bfd all-interfaces** コマンドは表示されません。**bfd interval** コマンドを使用して、BFD がルータまたはインターフェイスで設定されているときは、HSRP の BFD サポートはデフォルトでイネーブルになっています。**standby bfd** コマンドと **standby bfd all-interfaces** コマンドが必要なのは、ルータまたはインターフェイスで BFD が手動でディセーブルになっている場合だけです。

ルータ A

```
RouterA(config)# ip cef
RouterA(config)# interface FastEthernet2/0
RouterA(config-if)#  no shutdown
RouterA(config-if)# ip address 10.0.0.2 255.0.0.0
RouterA(config-if)# ip router-cache cef
RouterA(config-if)# bfd interval 200 min_rx 200 multiplier 3
RouterA(config-if)# standby 1 ip 10.0.0.11
RouterA(config-if)# standby 1 preempt
RouterA(config-if)# standby 1 priority 110
RouterA(config-if)# standby 2 ip 10.0.0.12
RouterA(config-if)# standby 2 preempt
RouterA(config-if)# standby 2 priority 110
```

ルータ B

```
RouterB(config)# interface FastEthernet2/0
RouterB(config-if)# ip address 10.1.0.22 255.255.0.0
RouterB(config-if)# no shutdown
RouterB(config-if)# bfd interval 200 min_rx 200 multiplier 3
RouterB(config-if)# standby 1 ip 10.0.0.11
RouterB(config-if)# standby 1 preempt
RouterB(config-if)# standby 1 priority 90
RouterB(config-if)# standby 2 ip 10.0.0.12
RouterB(config-if)# standby 2 preempt
RouterB(config-if)# standby 2 priority 80
```

例：HSRP Gratuitous ARP

次の例は、ARP キャッシュのエントリが正しいことを確認し、インターフェイスの HSRP グループがアクティブ ステートに変化したときに 4 秒間隔で gratuitous ARP パケットを 3 個送信するように HSRP を設定する方法を示しています。

```
Router> enable
Router# standby send arp Ethernet1/1 1
Router# configure terminal
Router(config)# interface Ethernet1/1
Router(config-if)# standby arp gratuitous count 3 interval 4
Router(config-if)# end
Router# show standby arp gratuitous ethernet1/1

HSRP Gratuitous ARP
Interface   Interval   Count
Ethernet1/1 4           3
```

その他の参考資料

関連資料

内容	参照先
Cisco IOS コマンド	『*Cisco IOS Master Commands List, All Releases*』
BFD	「*Bidirectional Forwarding Detection* 」モジュール
GLBP	「*Configuring GLBP*」モジュール
HSRP コマンド：complete コマンド構文、コマンド モード、コマンド履歴、デフォルト設定、使用に関する注意事項および例	『*Cisco IOS IP Application Services Command Reference*』
HSRP と IPSec	「*IPsec VPN High Availability Enhancements*」モジュールの「Hot Standby Routing Protocol and IPSec」
HSRP と IPv6	「*Configuring First Hop Redundancy Protocols in IPv6*」モジュール
ISSU	• 『*Cisco IOS In Service Software Upgrade Process*』 • 『*Catalyst 4500 Series Switch Cisco IOS Software* Configuration Guide』（リリース 12.2(31)SGA）の「Configuring the Cisco IOS In Service Software Upgrade Process」モジュール
オブジェクト トラッキング	「Configuring Enhanced Object Tracking」モジュール
HSRP のトラブルシューティング	• 『*Understanding and Troubleshooting HSRP Problems in Catalyst Switch Networks*』 • 『*Hot Standby Router Protocol: Frequently Asked Questions*』
VRRP	「Configuring VRRP」モジュール

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-HSRP-MIB CISCO-HSRP-EXT-MIB	選択されたプラットフォーム、シスコ ソフトウェア リリース、およびフィーチャ セットの MIB を検索してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
RFC 792	「*Internet Control Message Protocol*」
RFC 1828	「*IP Authentication Using Keyed MD5*」
RFC 2281	「*Cisco Hot Standby Router Protocol*」

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 ・テクニカル サポートを受ける ・ソフトウェアをダウンロードする ・セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける ・ツールおよびリソースへアクセスする - Product Alert の受信登録 - Field Notice の受信登録 - Bug Toolkit を使用した既知の問題の検索 ・Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する ・トレーニング リソースへアクセスする ・TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

HSRP の機能情報

表 1 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。

プラットフォーム サポートとソフトウェア イメージ サポートに関する情報を入手するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator を使用すると、特定のソフトウェア リリース、フィーチャ セット、またはプラットフォームをサポートするソフトウェア イメージを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

表 1　　HSRP の機能情報

機能名	リリース	機能情報
FHRP - HSRP BFD ピアリング	12.4(11)T	FHRP - HSRP BFD ピアリング機能により、HSRP グループ メンバーのヘルス モニタリング システムで BFD を使用できるようになりました。以前は、グループ メンバーのモニタリングには、かなり大規模で、生成とチェックに CPU メモリを消費する HSRP マルチキャスト メッセージだけが利用されていました。単一のインターフェイスが大量のグループをホストするアーキテクチャでは、CPU メモリの消費量と処理のオーバーヘッドが少ないプロトコルが必要です。BFD によって、この問題が解消されているほか、CPU にあまり負担をかけずに 1 秒未満のヘルス モニタリング（ミリ秒単位の障害検出）が実現されています。 この機能に関する詳細については、次の各項を参照してください。 • 「HSRP の BFD ピアリング」（P.18） • 「インターフェイスでの BFD セッション パラメータの設定」（P.50） • 「HSRP BFD ピアリングの設定」（P.51） • 「HSRP BFD ピアリングの検証」（P.53） • 「例：HSRP BFD ピアリング」（P.64） この機能によって導入または修正されたコマンドは、**debug standby events neighbor**、**show standby**、**show standby neighbors**、**standby bfd**、**standby bfd all-interfaces** です。

表 1　HSRP の機能情報 （続き）

機能名	リリース	機能情報
FHRP - HSRP グループ シャットダウン	12.4(9)T 12.2(33)SRC 12.2(33)SXI 15.0(1)S	FHRP - HSRP グループ シャットダウン機能を使用すると、トラッキング対象のオブジェクトがダウンしたときに、HSRP グループのプライオリティを下げるのではなく、ディセーブルな状態になる（ステートが Init になる）ように HSRP グループを設定することができます。 この機能に関する詳細については、次の各項を参照してください。 • 「HSRP グループ シャットダウン」（P.15） • 「HSRP のオブジェクト トラッキングの設定」（P.26） • 「例：HSRP グループ シャットダウン」（P.57） **standby track** および **show standby** の各コマンドがこの機能によって修正されました。
FHRP - HSRP - MIB	12.0(3)T 12.0(12)S	FHRP - HSRP - MIB 機能により、CISCO - HRSP - MIB がサポートされています。
FHRP - HSRP 複数グループ最適化	12.4(6)T 12.2(33)SRB 12.2(33)SXI 15.0(1)S	FHRP - HSRP 複数グループ最適化機能により、サブインターフェイスで設定されている複数の HSRP グループのネゴシエーションとメンテナンス方法が改善されました。アクティブ ルータとスタンバイ ルータを選出するために物理インターフェイスに必要なのは、1 つの HSRP グループだけです。このグループがマスター グループと呼ばれます。他の HSRP グループは、各サブインターフェイスに作成されたり、グループ名によってマスター グループとリンクされたりします。リンクされた HSRP グループは、*クライアント グループ*または*スレーブ グループ*と呼ばれます。 この機能に関する詳細については、次の各項を参照してください。 • 「HSRP 複数グループ最適化」（P.16） • 「HSRP 複数グループ最適化による CPU およびネットワークのパフォーマンスの向上」（P.39） • 「例：HSRP 複数グループ最適化を使用した CPU およびネットワークのパフォーマンスの向上」（P.61） **standby follow** および **show standby** の各コマンドがこの機能によって導入または修正されました。
FHRP - HSRP の IPv6 サポート	12.4(4)T 12.2(33)SRB 12.2(33)SXI	IPv6 のサポートが追加されました。 詳細については、『*Cisco IOS IPv6 Configuration Guide*』の「Configuring First Hop Redundancy Protocols in IPv6」モジュールを参照してください。
HSRP：グローバル IPv6 アドレス	12.2(33)SXI4	グローバル IPv6 の HSRP サポートが追加されました。 詳細については、『*Cisco IOS IPv6 Configuration Guide*』の「Configuring First Hop Redundancy Protocols in IPv6」モジュールを参照してください。

表 1　HSRP の機能情報 （続き）

機能名	リリース	機能情報
HSRP gratuitous ARP	12.2(33)SXI	HSRP gratuitous ARP 機能により、HSRP は ARP キャッシュ内のエントリが正しいことを確認し、1 つまたは複数のアクティブ HSRP グループから gratuitous ARP パケットを定期的に送信するように設定されます。 この機能に関する詳細については、次の各項を参照してください。 • 「HSRP gratuitous ARP」（P.11） • 「HSRP gratuitous ARP の設定」（P.54） • 「例：HSRP Gratuitous ARP」（P.65） **show standby arp gratuitous**、**standby arp gratuitous**、**standby send arp** の各コマンドがこの機能によって導入されました。 **show standby** および **debug standby events** の各コマンドがこの機能によって修正されました。
HSRP - ISSU	Cisco IOS XE 3.1.0SG 12.2(31)SGA 12.2(33)SRB1 15.0(1)S	HSRP - In-Service Software Upgrade（ISSU; インサービス ソフトウェア アップグレード）機能により、HSRP で ISSU がサポートされています。 In-Service Software Upgrade（ISSU; インサービス ソフトウェア アップグレード）プロセスにより、パケット転送を続行しながら、Cisco IOS ソフトウェアをアップデートまたは修正することができます。ほとんどのネットワークでは、予定されているソフトウェア アップグレードがダウンタイムの大きな原因になっています。ISSU を使用すると、パケット転送を続行しながら Cisco IOS ソフトウェアを修正できるので、ネットワークの可用性が向上し、予定されているソフトウェア アップグレードによるダウンタイムを短縮することができます。このマニュアルでは、ISSU の概念が説明されているほか、ISSU をシステムで実行するのに必要な手順が説明されています。 この機能については、次の項に説明があります。 • 「HSRP - ISSU」（P.17） この機能の詳細については、『*Cisco IOS In Service Software Upgrade Process*』を参照してください。 この機能により、新規追加または変更されたコマンドはありません。

表 1　HSRP の機能情報 （続き）

機能名	リリース	機能情報
HSRP MD5 認証	Cisco IOS XE 3.1.0SG 12.3(2)T 12.2(25)S 12.2(33)SRA 12.2(33)SXH 15.0(1)S	HSRP MD5 認証機能が導入される前、HSRP は単純なプレーン テキスト文字列でプロトコル パケットを認証していました。HSRP MD5 認証機能は、マルチキャスト HSRP プロトコル パケットの HSRP 部分の MD5 ダイジェストを生成するように拡張されています。この機能により、セキュリティが強化され、HSRP スプーフィング ソフトウェアの脅威に対する保護が得られます。 この機能に関する詳細については、次の各項を参照してください。 • 「HSRP MD5 認証」（P.9） • 「キー ストリングを使用した HSRP MD5 認証の設定」（P.28） • 「キー チェーンを使用した HSRP MD5 認証の設定」（P.30） • 「HSRP MD5 認証のトラブルシューティング」（P.32） • 「例：キー ストリングを使用した HSRP MD5 認証」（P.58） • 「例：キー チェーンを使用した HSRP MD5 認証」（P.58） • 「例：キー ストリングとキー チェーンを使用した HSRP MD5 認証」（P.58） **show standby** および **standby authentication** の各コマンドがこの機能によって導入または修正されました。
HSRP の ICMP リダイレクト サポート	12.1(3)T 15.0(1)S	HSRP の ICMP リダイレクト サポート機能により、HSRP を使用して設定されているインターフェイスで ICMP リダイレクトが可能になっています。 この機能に関する詳細については、次の各項を参照してください。 • 「HSRP の ICMP リダイレクト サポート」（P.12） • 「HSRP の ICMP リダイレクト サポートのイネーブル化」（P.41） • 「例：ICMP リダイレクト メッセージの HSRP サポート」（P.61） この機能によって導入または修正されたコマンドは、 **debug standby event**、**debug standby events icmp**、**show standby**、**standby redirects** です。

表 1　HSRP の機能情報 （続き）

機能名	リリース	機能情報
HSRP の MPLS VPN サポート	12.0(23)S、12.0(17)ST、12.2(28)SB、12.2(17b)SXA、12.2(8)T 15.0(1)S	HSRP の Multiprotocol Label Switching（MPLS; マルチプロトコル ラベル スイッチング）Virtual Private Network（VPN; バーチャル プライベート ネットワーク）インターフェイス サポートが役に立つのは、次のいずれかの状態で 2 つの Provider Edge（PE; プロバイダー エッジ）ルータ間でイーサネット LAN が接続されている場合です。 この機能については、次の項に説明があります。 • 「HSRP の MPLS VPN サポート」（P.16） この機能により、新規追加または変更されたコマンドはありません。
HSRP バージョン 2	Cisco IOS XE 3.1.0SG 12.3(4)T 12.2(25)S 15.0(1)S	HSRP バージョン 2 機能は、今後の機能拡張に備え、HSRP バージョン 1 よりも機能を拡張するために導入されました。HSRP バージョン 2 のパケット形式は、バージョン 1 とは異なります。 この機能に関する詳細については、次の各項を参照してください。 • 「HSRP バージョン 2 の設計」（P.4） • 「HSRP バージョン 2 への変更」（P.45） • 「例：HSRP バージョン 2」（P.63） **show standby**、**standby ip**、**standby version** の各コマンドがこの機能によって導入または修正されました。
SSO - HSRP	Cisco IOS XE 3.1.0SG 12.2(25)S 12.2(33)SRA 12.2(33)SXH 15.0(1)S	SSO - HSRP 機能により、冗長 RP のあるルータが SSO 用に設定されているときの HSRP の動作が変更されました。ある RP がアクティブで、もう一方の RP がスタンバイになっているとき、アクティブ RP に障害が発生すると、SSO は処理を引き継ぐスタンバイ RP をイネーブルにします。 この機能に関する詳細については、次の各項を参照してください。 • 「SSO HSRP」（P.17） • 「デュアル ルート プロセッサの SSO とシスコ ノンストップ フォワーディング」（P.17） • 「HSRP と SSO の協調動作」（P.18） • 「SSO 対応 HSRP のイネーブル化」（P.47） • 「SSO 対応 HSRP の検証」（P.48） • 「例：SSO HSRP」（P.63） **debug standby events** および **standby sso** の各コマンドがこの機能によって導入または修正されました。

用語集

ARP：Address Resolution Protocol（ARP; アドレス解決プロトコル）。ARP は IP ルーティングで必要な機能です。ARP は、ホストのハードウェア アドレスをホストの既知の IP アドレスから検出します。このハードウェア アドレスは Media Access Control（MAC; メディア アクセス制御）アドレスとも呼ばれます。ARP が保持するキャッシュ（テーブル）では、MAC アドレスが IP アドレスにマッピングされています。ARP は IP が動作しているすべての Cisco IOS システムの一部です。

BFD：Bidirectional Forwarding Detection（双方向フォワーディング検出）。これは、カプセル化、トポロジ、ルーティング プロトコルの転送パスの障害を高速に検出するように設定された検出プロトコルです。また、転送パス障害を高速で検出するだけでなく、一貫した障害検出方式をネットワーク管理者が使用できるようにします。

HSRP：Hot Standby Router Protocol（ホット スタンバイ ルータ プロトコル）。これによって、ネットワークの可用性が高まるほか、透過的にネットワーク トポロジを変更できます。HSRP は、HSRP アドレスに送信されるすべてのパケットを処理するメイン ルータのあるルータ グループを作成します。メイン ルータは、グループの他のルータによってモニタされます。メイン ルータに障害が発生すると、これらのスタンバイ HSRP ルータのいずれかが、メイン ルータとしての地位と HSRP グループ アドレスを継承します。

ISSU：In Service Software Upgrade（インサービス ソフトウェア アップグレード）。パケット転送の実行中に Cisco IOS ソフトウェアの更新や変更を可能にするプロセス。ほとんどのネットワークでは、予定されているソフトウェア アップグレードがダウンタイムの大きな原因になっています。ISSU を使用すると、パケット転送を続行しながら Cisco IOS ソフトウェアを修正できるので、ネットワークの可用性が向上し、予定されているソフトウェア アップグレードによるダウンタイムを短縮することができます。

NSF：Nonstop Forwarding（ノンストップ フォワーディング）。機能停止状態からの回復処理を行っているルータに対してトラフィックの転送を継続するルータの機能。また、障害からの回復中であるルータは、自身に送信されたトラフィックをピアによって正しく転送することができます。

RF：Redundancy Facility（冗長ファシリティ）。ステートがアクティブおよびスタンバイであるクライアントに進捗およびイベントを通知するのに使用される、構造化された機能インターフェイスです。

RP：Route Processor（ルート プロセッサ）。シャーシの中央制御装置の総称です。一般に、プラットフォーム固有の用語が使用されます（Cisco 7500 では RSP、Cisco 10000 では PRE、Cisco 7600 では SUP+MSFC など）。

RPR：Route Processor Redundancy（ルート プロセッサ冗長性）。RPR は、High System Availability（HSA）機能に代替方法を提供します。HSA を使用すると、システムはアクティブ RP が機能を停止したときにスタンバイ RP をリセットして使用できます。RPR を活用すると、アクティブ RP に致命的なエラーが発生したときにアクティブ RP とスタンバイ RP の間で迅速なスイッチオーバーが行われるため、不測のダウンタイムを減らすことができます。

RPR+：RPR の拡張。スタンバイ RP が完全に初期化されます。

SSO：Stateful Switchover（ステートフル スイッチオーバー）。SSO とは、アプリケーションや機能が、定義されているステートをアクティブ RP とスタンバイ RP との間で維持できる Cisco IOS ソフトウェアの実装を指しています。スイッチオーバーが発生しても、転送処理とセッションが維持されます。NSF と SSO を組み合わせると、RP に障害が発生してもネットワークに影響がおよぶことがありません。

アクティブ RP：アクティブ RP は、システムの制御やネットワーク サービスの提供を行うほか、ルーティング プロトコルを実行したり、システム管理インターフェイスを表示したりします。

アクティブ ルータ：仮想ルータにパケットを現在転送している HSRP グループのプライマリ ルータ。

クライアント グループ：サブインターフェイスに作成され、グループ名でマスター グループにリンクされる HSRP グループ。

スイッチオーバー：システム制御とルーティング プロトコルの実行がアクティブ RP からスタンバイ RP に移行するイベント。スイッチオーバーは、手動操作によって、またはハードウェア/ソフトウェアの機能停止によって発生します。スイッチオーバーには、個々のユニットのシステム制御とパケット転送を組み合わせるシステムでのパケット転送機能の移行が含まれることがあります。

スタンバイ RP：バックアップ RP。

スタンバイ グループ：HSRP に参加しているルータのうち、共同で仮想ルータをエミュレートする一連のルータ。

スタンバイ ルータ：HSRP グループのバックアップ ルータ。

仮想 IP アドレス：HSRP グループに設定されるデフォルト ゲートウェイの IP アドレス。

仮想 MAC アドレス：イーサネットおよび FDDI で、HSRP が設定されるときに自動的に生成される MAC アドレス。使用される標準の仮想 MAC アドレスは、0000.0C07.ACxy です。この xy は 16 進数のグループ番号です。機能アドレスはトークン リングに使用されます。HSRP バージョン 2 では、仮想 MAC アドレスが異なります。

マスター グループ：アクティブ ルータとスタンバイ ルータを選出するために物理インターフェイスに必要な HSRP グループ。

IRDP の設定

ICMP Router Discovery Protocol（IRDP）を使用すると、IPv4 ホストが他の（ローカルではない）IP ネットワークに対する IPv4 接続を提供するルータを特定できるようになります。この章で説明する IPv4 アドレッシング コマンドの詳細については、『*Cisco IOS IP Application Services Command Reference*』を参照してください。この章で説明するその他のコマンドについて詳細が記載されている資料を探すには、コマンド リファレンス マスター インデックス、またはオンライン検索を使用してください。

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、「IRDP の機能情報」（P.7）を参照してください。

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

この章の構成

IRDP について

IRDP の概要

ICMP Router Discovery Protocol（IRDP）を使用すると、ホストが、他のネットワーク上にある IP ベースのデバイスに到達するためにゲートウェイとして使用できるルータを特定できるようになります。IRDP を実行しているデバイスがルータとして動作する場合、ルータ検出パケットを生成します。IRDP を実行しているデバイスがホストとして動作する場合、ルータ検出パケットを受信します。Cisco IRDP の実装は、RFC 1256（http://www.ietf.org/rfc/rfc1256.txt）に概説されているルータ ディスカバリ プロトコルに完全に適合しています。

IRDP の設定方法

IRDP の設定

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **no shutdown**
5. **ip address** *ip-address mask*
6. **ip irdp**
7. **ip irdp multicast**
8. **ip irdp holdtime** *seconds*
9. **ip irdp maxadvertinterval** *seconds*
10. **ip irdp minadvertinterval** *seconds*
11. **ip irdp preference** *number*
12. **ip irdp address** *address number*
13. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**interface** *type number* 例： `Router(config)# interface fastethernet 0/0`	インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**no shutdown** 例： `Router(config-if)# no shutdown`	インターフェイスをアクティブ（イネーブル）にします。
ステップ 5	**ip address** *ip-address mask* 例： `Router(config-if)# ip address 172.16.16.1 255.255.240.0`	インターフェイスの IP アドレスを設定します。
ステップ 6	**ip irdp** 例： `Router(config-if)# ip irdp`	インターフェイスで IRDP をイネーブルにします。
ステップ 7	**ip irdp multicast** 例： `Router(config-if)# ip irdp multicast`	（任意）指定のインターフェイス上にある全システムのマルチキャスト アドレス（224.0.0.1）に IRDP アドバタイズメントを送信します。
ステップ 8	**ip irdp holdtime** *seconds* 例： `Router(config-if)# ip irdp holdtime 120`	（任意）アドバタイズメントが有効である IRDP 期間を設定します。
ステップ 9	**ip irdp maxadvertinterval** *seconds* 例： `Router(config-if)# ip irdp maxadvertinterval 60`	（任意）アドバタイズメントの IRDP 最大間隔を設定します。
ステップ 10	**ip irdp minadvertinterval** *seconds* 例： `Router(config-if)# ip irdp minadvertinterval 10`	（任意）アドバタイズメントの IRDP 最小間隔を設定します。
ステップ 11	**ip irdp preference** *number* 例： `Router(config-if)# ip irdp preference 900`	（任意）デバイスの IRDP プリファレンス レベルを設定します。

	コマンドまたはアクション	目的
ステップ 12	**ip irdp address** *address number* **例：** `Router(config-if)# ip irdp address 192.168.10.2 90`	（任意）プロキシ アドバタイズを行うための IRDP アドレスとプリファレンスを設定します。
ステップ 13	**end** **例：** `Router(config-if)# end`	現在のコンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

IRDP の設定例

例：IRDP の設定

次に、ルータ上で IRDP を設定する方法の例を示します。

```
Router(config)# interface fastethernet 0/1
Router(config-if)# no shutdown
Router(config-if)# ip address 172.16.10.1 255.255.255.0
Router(config-if)# ip irdp
Router(config-if)# ip irdp multicast
Router(config-if)# ip irdp holdtime 120
Router(config-if)# ip irdp maxadvertinterval 60
Router(config-if)# ip irdp minadvertinterval 10
Router(config-if)# ip irdp preference 900
Router(config-if)# ip irdp address 192.168.10.2 90
```

その他の参考資料

関連資料

内容	参照先
Cisco IOS コマンド	『*Cisco IOS Master Commands List, All Releases*』
IP アプリケーション サービス コマンド	『*Cisco IOS IP Application Services Command Reference*』

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
この機能がサポートする新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	—

RFC

RFC	タイトル
RFC 1256	『ICMP Router Discovery Messages』 http://www.ietf.org/rfc/rfc1256.txt

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 ・テクニカル サポートを受ける ・ソフトウェアをダウンロードする ・セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける ・ツールおよびリソースへアクセスする - Product Alert の受信登録 - Field Notice の受信登録 - Bug Toolkit を使用した既知の問題の検索 ・Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する ・トレーニング リソースへアクセスする ・TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

IRDP の機能情報

表 1 に、この章に記載されている機能を示します。

プラットフォーム サポートとソフトウェア イメージ サポートに関する情報を入手するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator を使用すると、特定のソフトウェア リリース、フィーチャ セット、またはプラットフォームをサポートするソフトウェア イメージを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 表 1 に、特定のソフトウェア リリース トレイン内の機能に対するサポートが導入されたソフトウェア リリースだけを示します。特に断りのないかぎり、そのソフトウェア リリース トレイン以降のリリースでもその機能がサポートされます。

表 1　　IRDP の機能情報

機能名	リリース	機能情報
ICMP Router Discovery Protocol	10.0 12.2(33)SRA	ICMP Router Discovery Protocol（IRDP）を使用すると、IPv4 ホストが他の（ローカルではない）IP ネットワークに対する IPv4 接続を提供するルータを特定できるようになります。 コマンド **ip irdp** が導入または変更されました。

VRRP の設定

Virtual Router Redundancy Protocol（VRRP; 仮想ルータ冗長プロトコル）は、LAN 上の VRRP ルータに対し、1 台または複数台の仮想ルータの役割をダイナミックに割り当てる選択プロトコルです。この場合、マルチアクセス リンク上にある何台かのルータが同じ仮想 IP アドレスを使用できるようにします。VRRP ルータは、LAN に接続されている 1 台以上の他のルータと連動して VRRP プロトコルを実行するように設定されます。VRRP 設定では、1 台のルータが仮想ルータ マスターとして選定され、他のルータは仮想ルータ マスターが機能を停止した場合のバックアップとして動作します。

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、「VRRP の機能情報」（P.27）を参照してください。

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

この章の構成

VRRP の制約事項

- VRRP は、マルチアクセス、マルチキャスト、またはブロードキャストに対応したイーサネット LAN 上で使用できるように設計されています。VRRP は既存のダイナミック プロトコルの代替にはなりません。
- VRRP は、イーサネット、ファスト イーサネット、Bridge Group Virtual Interface（BVI）、およびギガビット イーサネット インターフェイス、Multiprotocol Label Switching（MPLS; マルチプロトコル ラベル スイッチング）Virtual Private Network（VPN; バーチャル プライベート ネットワーク）、VRF を認識する MPLS VPN、および VLAN 上でサポートされます。
- BVI インターフェイスの初期化に関連して転送遅延が発生するため、VRRP アドバタイズ タイマーの時間は BVI インターフェイスでの転送遅延時間と同じにするか、または長く設定する必要があります。このように設定することで、最近初期化された BVI インターフェイス上にある VRRP ルータが無条件にマスター ロールを引き継ぐことがなくなります。BVI インターフェイスでの転送遅延を設定するには、**bridge forward-time** コマンドを使用します。VRRP アドバタイズメント タイマーを設定するには、**vrrp timers advertise** コマンドを使用します。
- Enhanced Object Tracking（EOT; 拡張オブジェクト トラッキング）はステートフル スイッチオーバー（SSO）を認識しないため、SSO モードで VRRP と併用することはできません。

VRRP について

VRRP の動作

LAN クライアントが特定のリモート宛先に対してファーストホップとなるルータを決定する場合、いくつかの方法があります。クライアントは、ダイナミック プロセスまたはスタティック設定を使用できます。次に、ダイナミックなルータ検出の例を示します。

- プロキシ ARP：クライアントは Address Resolution Protocol（ARP; アドレス解決プロトコル）を使用して到達先の宛先を取得します。ルータは自分の MAC アドレスを使用して ARP 要求に応答します。
- ルーティング プロトコル：クライアントは、（たとえば、Routing Information Protocol（RIP）からの）ダイナミック ルーティング プロトコル アップデートをリスンし、独自にルーティング テーブルを作成します。

- IRDP（ICMP Router Discovery Protocol）クライアント：このクライアントは Internet Control Message Protocol（ICMP; インターネット制御メッセージ プロトコル）ルータ検出クライアントを実行します。

ダイナミック ディスカバリ プロトコルの欠点として、LAN クライアントで多少の設定が必要となることと、処理のオーバーヘッドが生じることが挙げられます。また、ルータが機能を停止した場合、他のルータへの切り替えを行うプロセスに時間がかかることがあります。

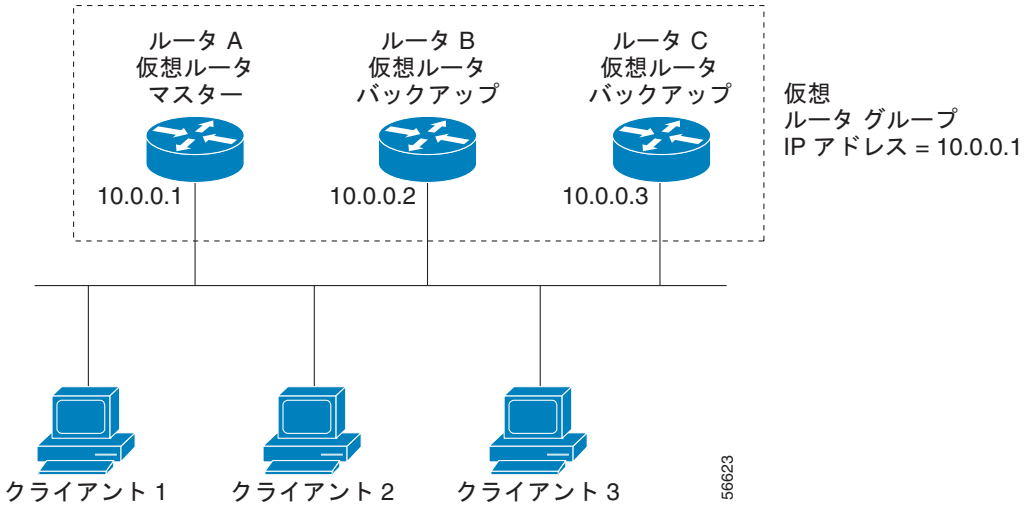
ダイナミック ディスカバリ プロトコルの代替方法として、クライアント上でデフォルト ルータをスタティックに設定する方法があります。このアプローチでは、クライアントの設定と処理は簡略化されますが、単一障害点が生じます。デフォルト ゲートウェイが機能を停止すると、LAN クライアントが通信できるのはローカル IP ネットワーク セグメントだけに制限され、残りのネットワークからは切断されます。

VRRP を使用すると、スタティックな設定の問題は解消されます。VRRP は、ルータのグループを使用して単一の*仮想ルータ*を形成します。これにより、仮想ルータをデフォルト ゲートウェイとして使用するように、LAN クライアントを設定できます。ルータのグループを表す仮想ルータは、「VRRP グループ」とも呼ばれます。

VRRP は、イーサネット、ファスト イーサネット、BVI、およびギガビット イーサネット インターフェイス、MPLS VPN、VRF を認識する MPLS VPN、および VLAN 上でサポートされます。

図 1 に、VRRP が設定された LAN トポロジを示します。この例では、ルータ A、B、および C は仮想ルータで構成される *VRRP ルータ*（VRRP を実行するルータ）です。仮想ルータの IP アドレスは、ルータ A のイーサネット インターフェイスに設定されたアドレス（10.0.0.1）と同じです。

図 1　　VRRP の基本トポロジ

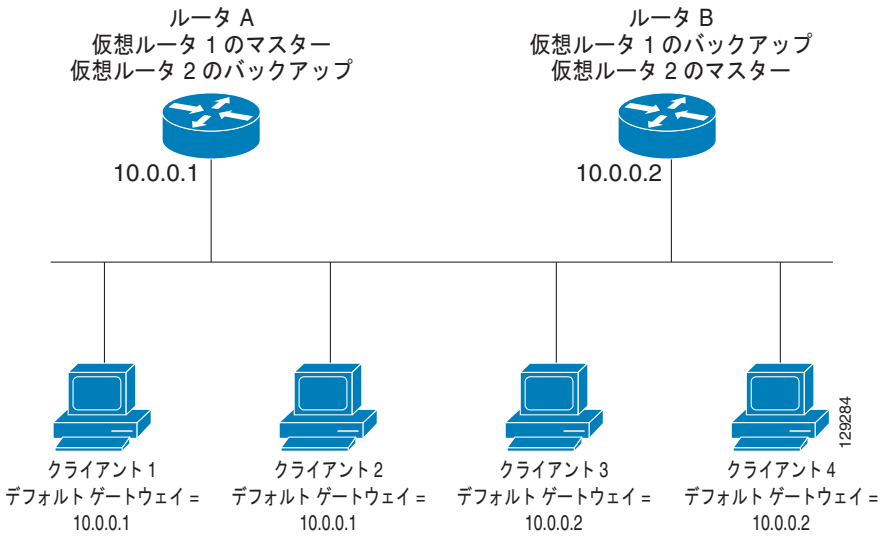


仮想ルータはルータ A の物理イーサネット インターフェイスの IP アドレスを使用するため、ルータ A は*仮想ルータ マスター*のロールを担い、「*IP アドレス所有者*」とも呼ばれます。ルータ A は、仮想ルータ マスターとして、仮想ルータの IP アドレスを管理し、この IP アドレスに送信されたパケットの転送を行います。クライアント 1 ～ 3 はデフォルト ゲートウェイ IP アドレス（10.0.0.1）を使用して設定されます。

ルータ B とルータ C は*仮想ルータ バックアップ*として機能します。仮想ルータ マスターが機能を停止すると、高いプライオリティに設定されているルータが仮想ルータ マスターとなり、LAN ホストには継続してサービスが提供されます。ルータ A が回復すると、ルータ A が再び仮想ルータ マスターになります。VRRP ルータが果たすロールと、仮想ルータ マスターが機能を停止したときにどのようなことが起こるかについての詳細は、このマニュアル内の「VRRP ルータ プライオリティとプリエンプション」を参照してください。

図 2 に示す LAN トポロジでは、ルータ A とルータ B がクライアント 1 ～ 4 のトラフィックを共有し、ルータ A とルータ B がいずれかのルータが機能を停止したときに相互に仮想ルータ バックアップとして機能するように VRRP が設定されています。

図 2　ロード シェアリングと冗長化が設定された VRRP トポロジ



このトポロジでは、2 つの仮想ルータが設定されています（詳細については、このマニュアルの「複数の仮想ルータのサポート」を参照してください）。仮想ルータ 1 では、ルータ A が IP アドレス 10.0.0.1 の所有者で、仮想ルータ マスターになっています。ルータ B はルータ A に対する仮想ルータ バックアップです。クライアント 1 と クライアント 2 はデフォルト ゲートウェイ IP アドレス（10.0.0.1）を使用して設定されています。

仮想ルータ 2 では、ルータ B が IP アドレス 10.0.0.2 の所有者で、仮想ルータ マスターになっています。ルータ A はルータ B に対する仮想ルータ バックアップです。クライアント 3 と クライアント 4 はデフォルト ゲートウェイ IP アドレス（10.0.0.2）を使用して設定されています。

VRRP の利点

冗長性

VRRP により、複数のルータをデフォルト ゲートウェイ ルータとして設定できるようになり、ネットワークに単一障害点が生じる可能性を低減できます。

ロード シェアリング

LAN クライアントとの間のトラフィックを複数のルータで共有するように VRRP を設定できるため、利用可能なルータ間でより均等にトラフィックの負荷を分散できます。

複数の仮想ルータ

プラットフォームが複数の MAC アドレスをサポートする場合、VRRP はルータの物理インターフェイス上で最大 255 の仮想ルータ（VRRP グループ）をサポートします。複数の仮想ルータをサポートすることで、LAN トポロジ内で冗長化とロード シェアリングを実装できます。

複数の IP アドレス

仮想ルータは、セカンダリ IP アドレスを含め複数の IP アドレスを管理できます。そのため、イーサネット インターフェイスに複数のサブネットを設定した場合、サブネットごとに VRRP を設定できます。

プリエンプション

VRRP の冗長性スキームにより、仮想ルータ バックアップのプリエンプトが可能になり、より高いプライオリティが設定された仮想ルータ バックアップが、機能を停止した仮想ルータ マスターを引き継ぐようにできます。

認証

VRRP の Message Digest 5（MD5; メッセージ ダイジェスト 5）アルゴリズム認証は、VRRP スプーフィング ソフトウェアから保護し、業界標準の MD5 アルゴリズムを使用して、信頼性とセキュリティを高めます。

アドバタイズメント プロトコル

VRRP は専用の Internet Assigned Numbers Authority（IANA）標準マルチキャスト アドレス（224.0.0.18）を使用して VRRP アドバタイズメントを行います。このアドレッシング方式により、マルチキャストにサービスを提供しなければならないルータの数を最小限に抑え、テスト装置がセグメントの VRRP パケットを正確に特定できるようになります。IANA は VRRP に IP プロトコル番号 112 を割り当てました。

VRRP オブジェクト トラッキング

VRRP オブジェクト トラッキングにより、インターフェイスや IP ルート ステートなどの追跡対象オブジェクトのステータスに応じて VRRP プライオリティを変更することで、最適な VRRP ルータがグループの仮想ルータ マスターになります。

複数の仮想ルータのサポート

ルータの物理インターフェイスには、最大 255 の仮想ルータを設定できます。ルータ インターフェイスがサポートできる実際の仮想ルータの数は、次の要因によって決定されます。

- ルータの処理機能
- ルータのメモリ機能
- 複数の MAC アドレスのルータ インターフェイス サポート

1 つのルータ インターフェイス上に複数の仮想ルータが設定されているトポロジでは、インターフェイスは 1 つの仮想ルータにはマスターとして動作し、1 つまたは複数の仮想ルータにはバックアップとして動作することができます。

VRRP ルータ プライオリティとプリエンプション

VRRP 冗長性スキームの重要な一面に、ルータ プライオリティがあります。プライオリティにより、各 VRRP ルータが果たすロールと、仮想ルータ マスターが機能を停止したときにどのようなことが起こるかが決定されます。

ある VRRP ルータが仮想ルータの IP アドレスと物理インターフェイスの IP アドレスを所有している場合、このルータが仮想ルータ マスターとして機能します。

VRRP ルータが仮想ルータ バックアップとして機能するかどうかや、仮想ルータ マスターが機能を停止した場合に仮想ルータ マスターを引き継ぐ順序も、プライオリティによって決定されます。**vrrp priority** コマンドを使用して 1 ～ 254 の値を設定し、各仮想ルータ バックアップのプライオリティを設定できます。

たとえば、ルータ A（LAN トポロジの仮想ルータ マスター）が機能を停止した場合、選択プロセスが行われ、仮想ルータ バックアップ B と C のどちらが引き継ぐかが決定されます。ルータ B とルータ C がそれぞれ プライオリティ 101 と 100 に設定されている場合、プライオリティの高いルータ B が仮想ルータ マスターになります。ルータ B とルータ C が両方ともプライオリティ 100 に設定されている場合、IP アドレスが高い方の仮想ルータ バックアップが選択されて仮想ルータ マスターになります。

デフォルトでは、プリエンプティブ スキームはイネーブルになっています。この場合、仮想ルータ マスターになるように選択されている仮想ルータ バックアップの中で、より高いプライオリティが設定されている仮想ルータ バックアップが仮想ルータ マスターになります。このプリエンプティブ スキームをディセーブルにするには、**no vrrp preempt** コマンドを使用します。プリエンプションがディセーブルになっている場合は、元の仮想ルータ マスターが回復して再びマスターになるまで、仮想ルータ マスターになるように選択されている仮想ルータ バックアップがマスターのロールを果たします。

VRRP アドバタイズメント

仮想ルータ マスターは、同じグループ内の他の VRRP ルータに VRRP アドバタイズメントを送信します。アドバタイズメントでは、仮想ルータ マスターのプライオリティとステートを伝えます。VRRP アドバタイズメントは IP パケットにカプセル化され、VRRP グループに割り当てられた IP バージョン 4 マルチキャスト アドレスに送信されます。アドバタイズメントは、デフォルトで 1 秒に 1 回送信されますが、この間隔は設定可能です。

RFC 3768 と同様に VRRP プロトコルもミリ秒タイマーをサポートしていませんが、Cisco ルータを使用すれば、ミリ秒タイマーを設定することができます。ミリ秒タイマー値は、プライマリ ルータとバックアップ ルータの両方に手動で設定する必要があります。バックアップ ルータ上の **show vrrp** コマンド出力に表示されるマスター アドバタイズメント値は、常に、1 秒です。これは、バックアップ ルータ上のパケットでミリ秒値が受け入れられないためです。

ミリ秒タイマーは、絶対に必要な場合以外は使用しないようにし、使用する場合は慎重な検討とテストが必要です。ミリ秒値は順境の下でしか機能しません。そのため、ミリ秒タイマー値の使用は、VRRP の動作をシスコ デバイスに限定することに注意する必要があります。

VRRP オブジェクト トラッキング

オブジェクト トラッキングは、インターフェイス ライン プロトコルのステートなど、追跡対象オブジェクトの作成、モニタ、削除を管理する独立したプロセスです。Hot Standby Router Protocol（HSRP; ホット スタンバイ ルータ プロトコル）、Gateway Load Balancing Protocol（GLBP; ゲートウェイ ロード バランシング プロトコル）、そして VRRP のようなクライアントは、追跡対象オブジェクトを登録し、オブジェクトのステートが変更されたときにアクションを実行できます。

各追跡対象オブジェクトには、トラッキング CLI（コマンドライン インターフェイス）で指定される一意の番号があります。VRRP などのクライアント プロセスは、この番号を使用して特定のオブジェクトを追跡します。

トラッキング プロセスは、追跡対象オブジェクトを定期的にポーリングし、値に変化がないかどうかを確認します。追跡対象オブジェクトに変化があれば登録されているクライアント プロセスに通知します。ただちに通知する場合と、指定された時間遅延後に通知する場合があります。オブジェクトの値は、アップまたはダウンとして報告されます。

VRRP オブジェクト トラッキングにより、VRRP はトラッキング プロセスで追跡可能なすべてのオブジェクトにアクセスします。トラッキング プロセスでは、インターフェイス ライン プロトコルのステート、IP ルートのステート、ルートの到達可能性など、オブジェクトを個別に追跡する機能が提供されます。

VRRP はトラッキング プロセスに対するインターフェイスを提供します。VRRP グループごとに、VRRP ルータのプライオリティに影響を及ぼす可能性のある複数のオブジェクトを追跡できます。追跡対象のオブジェクト番号を指定すると、そのオブジェクトに何らかの変更が生じた場合に VRRP によって通知されます。VRRP は、追跡対象オブジェクトのステートに基づいて、仮想ルータのプライオリティを増加（または減少）させます。

オブジェクト トラッキングが VRRP ルータのプライオリティに及ぼす影響

オブジェクト トラッキングが設定されている場合に、追跡対象のオブジェクトがダウンすると、デバイスのプライオリティはダイナミックに変化します。トラッキング プロセスは、追跡対象オブジェクトを定期的にポーリングし、値に変化がないかどうかを確認します。追跡対象オブジェクトに変化があれば VRRP に通知します。ただちに通知する場合と、指定された時間遅延後に通知する場合があります。オブジェクトの値は、アップまたはダウンとして報告されます。トラッキング可能なオブジェクトには、インターフェイスのライン プロトコル ステートや IP ルートの到達可能性などがあります。指定したオブジェクトがダウンすると、VRRP プライオリティが引き下げられます。その場合、**vrrp preempt** コマンドが設定されていると、より高いプライオリティが設定された VRRP ルータが仮想ルータ マスターになります。オブジェクト トラッキングの詳細については、「VRRP オブジェクト トラッキング」を参照してください。

VRRP 認証

VRRP は、認証されていない VRRP プロトコル メッセージを無視します。デフォルトの認証タイプはテキスト認証です。

VRRP テキスト認証、単純な MD5 キー ストリングを使用した認証、または MD5 キー チェーンを使用した認証を設定することができます。

MD5 認証は、代替となるプレーン テキスト認証スキームよりも高いセキュリティを実現します。MD5 認証を使用すると、各 VRRP グループ メンバが秘密キーを使用して、発信パケットの一部であるキー付き MD5 ハッシュを生成できます。着信パケットのキー付きハッシュが生成されると、生成されたハッシュと着信パケット内のハッシュが一致しない場合、そのパケットは無視されます。

MD5 ハッシュのキーは、キー ストリングを使用して設定内で直接指定することも、キー チェーンを通して間接的に指定することもできます。

ルータは、VRRP グループと認証の設定が異なるルータから着信した VRRP パケットは無視します。VRRP には、次の 3 つの認証スキームがあります。

- 認証なし
- プレーン テキスト認証
- MD5 認証

VRRP パケットは、次の場合はいずれも拒否されます。

- ルータと着信パケットの認証スキームが異なる。
- ルータと着信パケットの MD5 ダイジェストが異なる。
- ルータと着信パケットのテキスト認証文字列が異なる。

ISSU と VRRP

VRRP は In Service Software Upgrade（ISSU; インサービス ソフトウェア アップグレード）をサポートします。In Service Software Upgrade（ISSU）を使用すると、アクティブおよびスタンバイの Route Processor（RP; ルート プロセッサ）またはラインカード上で異なるバージョンの Cisco IOS ソフトウェアが実行されている場合でも、ハイアベイラビリティ（HA）システムをステートフル スイッチオーバー（SSO）モードで実行できるようになります。

ISSU は、サポートされる Cisco IOS リリースから別のリリースへアップグレードまたはダウングレードする機能を提供します。この場合、パケット転送は継続して行われ、セッションは維持されるため、予定されるシステムの停止時間を短くすることができます。アップグレードまたはダウングレードする機能は、アクティブ RP およびスタンバイ RP 上で異なるバージョンのソフトウェアを実行することで実現します。これにより、RP 間でステート情報を維持する時間が短くなります。この機能により、システムをアップグレード対象（またはダウングレード対象）のソフトウェアを実行するセカンダリ RP に切り替えることができ、セッションを切断することなく、またパケットの損失も最小限に抑えながら、継続してパケットを転送できます。この機能は、デフォルトでイネーブルにされています。

ISSU の詳細については、次の URL に掲載されている『*Cisco IOS In Service Software Upgrade Process*』を参照してください。

http://www.cisco.com/en/US/docs/ios/ha/configuration/guide/ha-inserv_updg.html

7600 シリーズ ルータでの ISSU の詳細については、次の URL に掲載されている『*ISSU and eFSU on Cisco 7600 Series Routers*』を参照してください。

http://www.cisco.com/en/US/partner/products/hw/routers/ps368/products_configuration_guide_chapter09186a00807f1c85.html

SSO と VRRP

SSO VRRP 機能が導入されたため、VRRP はステートフル スイッチオーバー（SSO）を認識するようになりました。VRRP は、ルータがセカンダリ RP にフェールオーバーしたことを検出し、グループの現在の状態を継続することができます。

SSO は、デュアル RP をサポートするネットワーキングデバイス（通常はエッジ デバイス）で機能します。1 台の RP をアクティブ プロセッサとして設定し、他の RP をスタンバイ プロセッサとして設定することで、RP 冗長化を実現します。また、RP 間の重要なステート情報を同期するため、ネットワーク ステート情報は RP 間でダイナミックに維持されます。

VRRP が SSO を認識する前に、RP が冗長化されたルータに VRRP を展開した場合、アクティブ RP とスタンバイ RP 間のロールがスイッチオーバーされると、ルータの GLBP グループ メンバとしてのアクティビティは破棄され、ルータはリロードされた場合と同様にグループに再び参加することになります。SSO VRRP 機能により、スイッチオーバーが行われても、GLBP は継続してグループ メンバとしてのアクティビティを継続できます。冗長化された RP 間の VRRP ステート情報は維持されるため、スタンバイ RP はスイッチオーバーの実行中も実行後も VRRP 内で引き続きルータのアクティビティを実行できます。

この機能は、デフォルトでイネーブルにされています。この機能をディセーブルにするには、グローバル コンフィギュレーション モードで **no vrrp sso** コマンドを使用します。

詳細については、次の URL に掲載されている『*Stateful Switchover*』を参照してください。

http://www.cisco.com/en/US/docs/ios/ha/configuration/guide/ha-stfl_swovr.html

VRRP の設定方法

ここでは、次の各手順について説明します。

VRRP のカスタマイズ

VRRP の動作のカスタマイズはオプションです。VRRP グループをイネーブルにするとすぐに、そのグループは動作を開始することに注意してください。VRRP をカスタマイズする前に VRRP グループをイネーブルにすると、ルータがグループの制御を引き継ぎ、機能のカスタマイズを完了する前に仮想ルータ マスターになることがあります。このため、VRRP をカスタマイズする場合には、カスタマイズを行ってから VRRP をイネーブルにすることを推奨します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip address** *ip-address mask*
5. **vrrp** *group* **description** *text*
6. **vrrp** *group* **priority** *level*
7. **vrrp** *group* **preempt** [**delay minimum** *seconds*]
8. **vrrp** *group* **timers advertise** [**msec**] *interval*
9. **vrrp** *group* **timers learn**
10. **no vrrp sso**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* **例：** `Router(config)# interface ethernet 0`	インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ip address** *ip-address mask* **例：** `Router(config-if)# ip address 172.16.6.5 255.255.255.0`	インターフェイスの IP アドレスを設定します。
ステップ 5	**vrrp** *group* **description** *text* **例：** `Router(config-if)# vrrp 10 description working-group`	VRRP グループに説明テキストを割り当てます。
ステップ 6	**vrrp** *group* **priority** *level* **例：** `Router(config-if)# vrrp 10 priority 110`	VRRP グループ内のルータのプライオリティ レベルを設定します。 • デフォルトのプライオリティは 100 です。
ステップ 7	**vrrp** *group* **preempt** [**delay minimum** *seconds*] **例：** `Router(config-if)# vrrp 10 preempt delay minimum 380`	現在の仮想ルータ マスターよりも高いプライオリティが設定されている場合、VRRP グループの仮想ルータ マスターとして引き継ぐルータを指定します。 • デフォルトの遅延時間は 0 秒です。 • このコマンドの設定にかかわらず、IP アドレスの所有者であるルータがプリエンプトします。
ステップ 8	**vrrp** *group* **timers advertise** [**msec**] *interval* **例：** `Router(config-if)# vrrp 10 timers advertise 110`	VRRP グループの仮想ルータ マスターが行う、連続したアドバタイズ インターバルを設定します。 • 間隔の単位は、**msec** キーワードが指定された場合を除き、「秒」です。デフォルトの *interval* 値は 1 秒です。 **（注）** VRRP グループ内のすべてのルータが同じタイマー値を使用する必要があります。同じタイマー値が設定されていないと、VRRP グループ内のルータが相互通信せず、正しく設定されていないルータのステートがマスターに変わります。

	コマンドまたはアクション	目的
ステップ 9	**vrrp** *group* **timers learn** 例： `Router(config-if)# vrrp 10 timers learn`	ルータが VRRP グループの仮想ルータ バックアップとして動作している場合、仮想ルータ マスターのアドバタイズ インターバルを学習するようにルータを設定します。
ステップ 10	**no vrrp sso** 例： `Router(config)# no vrrp sso`	（任意）SSO の VRRP サポートをディセーブルにします。SSO の VRRP サポートはデフォルトでイネーブルになっています。

VRRP のイネーブル化

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip address** *ip-address mask*
5. **vrrp** *group* **ip** *ip-address* [**secondary**]
6. **end**
7. **show vrrp** [**brief** | *group*]
8. **show vrrp interface** *type number* [**brief**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* 例： `Router(config)# interface ethernet 0`	インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ip address** *ip-address mask* 例： `Router(config-if)# ip address 172.16.6.5 255.255.255.0`	インターフェイスの IP アドレスを設定します。

	コマンドまたはアクション	目的
ステップ 5	**vrrp** *group* **ip** *ip-address* [**secondary**] **例：** `Router(config-if)# vrrp 10 ip 172.16.6.1`	インターフェイスの VRRP をイネーブルにします。 • プライマリ IP アドレスを指定した後、**secondary** キーワードを指定して **vrrp ip** コマンドをもう一度使用すれば、このグループでサポートする追加の IP アドレスを指定できます。 **（注）** VRRP グループ内のすべてのルータには、同じプライマリ アドレスと、仮想ルータで一致するセカンダリ アドレスのリストを設定する必要があります。プライマリ アドレスまたはセカンダリ アドレスに異なるアドレスを設定すると、VRRP グループ内のルータが相互通信せず、正しく設定されていないルータのステートがマスターに変わります。
ステップ 6	**end** **例：** `Router(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 7	`Router# show vrrp [brief | group]` **例：** `Router# show vrrp 10`	（任意）ルータのいずれかまたはすべての VRRP グループについて、簡易または詳細なステータスを表示します。
ステップ 8	`Router# show vrrp interface type number [brief]` **例：** `Router# show vrrp interface ethernet 0`	（任意）指定インターフェイスの VRRP グループおよびそのステータスを表示します。

インターフェイスでの VRRP のディセーブル化

インターフェイスで VRRP をディセーブルにすると、プロトコルをディセーブルにできますが、設定は維持されます。この機能は、VRRP MIB、RFC 2787「*Definitions of Managed Objects for the Virtual Router Redundancy Protocol*」の導入とともに追加されました。

Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）管理ツールを使用して、インターフェイスでの VRRP をイネーブルまたはディセーブルに設定できます。SNMP 管理機能により、**vrrp shutdown** コマンドが導入され、SNMP を使用して設定されたステートが VRRP の CLI を通して表示されるようになりました。

show running-config コマンドを入力すると、VRRP グループが設定されているかどうか、およびイネーブルとディセーブルのどちらに設定されているかをすぐに確認できます。これは、MIB 内でイネーブルされるのと同じ機能です。

このコマンドを **no** 形式で使用すると、MIB 内で実行される同じ動作がイネーブルになります。SNMP インターフェイスを使用して **vrrp shutdown** コマンドを指定した場合、Cisco IOS CLI を使って **no vrrp shutdown** コマンドを入力すると、VRRP グループが再びイネーブルになります。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip address** *ip-address mask*
5. **vrrp** *group* **shutdown**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* 例： `Router(config)# interface ethernet 0`	インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ip address** *ip-address mask* 例： `Router(config-if)# ip address 172.16.6.5 255.255.255.0`	インターフェイスの IP アドレスを設定します。
ステップ 5	**vrrp** *group* **shutdown** 例： `Router(config-if)# vrrp 10 shutdown`	インターフェイスの VRRP をディセーブルにします。 • コマンドがルータに表示されるようになります。 **（注）** 設定を維持した状態で、1 つの VRRP グループをディセーブルにし、別の VRRP グループをイネーブルにできます。

VRRP オブジェクト トラッキングの設定

制約事項

VRRP グループが IP アドレス所有者である場合、そのプライオリティは 255 に固定され、オブジェクト トラッキングで減じることはできません。

手順の概要

1. **enable**
2. **configure terminal**
3. **track** *object-number* **interface** *type number* {**line-protocol** | **ip routing**}
4. **interface** *type number*
5. **vrrp** *group* **ip** *ip-address*
6. **vrrp** *group* **priority** *level*
7. **vrrp** *group* **track** *object-number* [**decrement** *priority*]
8. **end**
9. **show track** [*object-number*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**track** *object-number* **interface** *type number* {**line-protocol** | **ip routing**} 例： `Router(config)# track 2 interface serial 6 line-protocol`	インターフェイスを追跡し、インターフェイスのステートに変更が生じると VRRP グループのプライオリティに影響するように設定します。 • このコマンドを使って、**vrrp track** コマンドで使用されるインターフェイスおよび対応するオブジェクト番号を設定します。 • **line-protocol** キーワードは、インターフェイスがアップしているかどうかを追跡します。**ip routing** キーワードを指定すると、インターフェイス上で IP ルーティングがイネーブルになっていて、アクティブになっていることも確認します。 • **track IP route** コマンドを使用して、IP ルートまたはメトリック タイプのオブジェクトの到達可能性を追跡することもできます。
ステップ 4	**interface** *type number* 例： `Router(config)# interface Ethernet 2`	インターフェイス コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 5	**vrrp** *group* **ip** *ip-address* 例： `Router(config-if)# vrrp 1 ip 10.0.1.20`	インターフェイス上で VRRP をイネーブルにし、仮想ルータのプライマリ IP アドレスを指定します。
ステップ 6	**vrrp** *group* **priority** *level* 例： `Router(config-if)# vrrp 1 priority 120`	VRRP グループ内のルータのプライオリティ レベルを設定します。
ステップ 7	**vrrp** *group* **track** *object-number* [**decrement** *priority*] 例： `Router(config-if)# vrrp 1 track 2 decrement 15`	オブジェクトを追跡するように VRRP を設定します。
ステップ 8	**end** 例： `Router(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 9	**show track** [*object-number*] 例： `Router# show track 1`	トラッキング情報を表示します。

キー ストリングを使用した VRRP MD5 認証の設定

制約事項

RFC 2338 方式を実装したベンダーとの相互運用性は、有効ではありません。

どのような場合でも、テキスト認証を MD5 認証と組み合わせて VRRP グループに使用することはできません。MD5 認証が設定されている場合、VRRP hello メッセージのテキスト認証のフィールドはすべてゼロ（0）に設定されて送信され、受信時には無視されます（受信側のルータでも MD5 認証が有効になっている場合）。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip address** *ip-address mask* [**secondary**]
5. **vrrp** *group* **priority** *priority*
6. **vrrp** *group* **authentication md5 key-string** [**0** | **7**] *key-string* [**timeout** *seconds*]
7. **vrrp** *group* **ip** [*ip-address* [**secondary**]]

8. 通信を行う各ルータ上でステップ 1 ～ 7 を繰り返します。
9. **end**

手順の詳細

	コマンド	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* **例：** `Router(config)# interface Ethernet0/1`	インターフェイス タイプを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ip address** *ip-address mask* [**secondary**] **例：** `Router(config-if)# ip address 10.0.0.1 255.255.255.0`	インターフェイスのプライマリ IP アドレスまたはセカンダリ IP アドレスを指定します。
ステップ 5	**vrrp** *group* **priority** *priority* **例：** `Router(config-if)# vrrp 1 priority 110`	VRRP プライオリティを設定します。
ステップ 6	**vrrp** *group* **authentication md5 key-string** [**0** | **7**] *key-string* [**timeout** *seconds*] **例：** `Router(config-if)# vrrp 1 authentication md5 key-string d00b4r987654321a timeout 30`	VRRP MD5 認証の認証文字列を設定します。 • *key* 引数には最大 64 文字を設定できます。16 文字以上を使用することを推奨します。 • *key* 引数にはプレフィクスを指定しません。**0** を指定すると、キーは暗号化されないことを示します。 • **7** を指定するとキーは暗号化されます。**service password-encryption** グローバル コンフィギュレーション コマンドがイネーブルになっていると、key-string 認証キーは自動的に暗号化されます。 • タイムアウト値は、古いキー ストリングが受け入れられ、新しいキーを使用してグループ内のすべてのルータを設定できる時間です。 **（注）** VRRP グループ内のすべてのルータは、同じ認証文字列を使用して設定する必要があります。同じ認証文字列が設定されていないと、VRRP グループ内のルータが相互通信せず、正しく設定されていないいずれかのルータのステートがマスターに変わります。

	コマンド	目的
ステップ 7	**vrrp** *group* **ip** [*ip-address* [**secondary**]] 例： `Router(config-if)# vrrp 1 ip 10.0.0.3`	インターフェイス上で VRRP をイネーブルにし、仮想ルータのプライマリ IP アドレスを指定します。
ステップ 8	通信を行う各ルータ上でステップ 1 ～ 7 を繰り返します。	—
ステップ 9	**end** 例： `Router(config-if)# end`	特権 EXEC モードに戻ります。

キー チェーンを使用した VRRP MD5 認証の設定

キー チェーンを使用して VRRP MD5 認証を設定するには、次の手順を実行します。キー チェーンを使用すると、キー チェーンの設定に基づき、場合に応じて異なるキー ストリングを使用できます。VRRP は適切なキー チェーンを照会し、特定のキー チェーンに対して現在アクティブになっているキーとキー ID を取得します。

制約事項

RFC 2338 方式を実装したベンダーとの相互運用性は、有効ではありません。

どのような場合でも、テキスト認証を MD5 認証と組み合わせて VRRP グループに使用することはできません。MD5 認証が設定されている場合、VRRP hello メッセージのテキスト認証のフィールドはすべてゼロ（0）に設定されて送信され、受信時には無視されます（受信側のルータでも MD5 認証が有効になっている場合）。

手順の概要

1. **enable**
2. **configure terminal**
3. **key chain** *name-of-chain*
4. **key** *key-id*
5. **key-string** *string*
6. **exit**
7. **interface** *type number*
8. **ip address** *ip-address mask* [**secondary**]
9. **vrrp** *group* **priority** *priority*
10. **vrrp** *group* **authentication md5 key-chain** *key-chain*
11. **vrrp** *group* **ip** [*ip-address* [**secondary**]]
12. 通信を行う各ルータ上でステップ 1 ～ 11 を繰り返します。
13. **end**

手順の詳細

	コマンド	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**key chain** *name-of-chain* 例： `Router(config)# key chain vrrp1`	ルーティング プロトコルの認証をイネーブルにし、認証キーのグループを識別します。
ステップ 4	**key** *key-id* 例： `Router(config-keychain)# key 100`	キー チェーンの認証キーを識別します。 • *key-id* は、数値で指定する必要があります。
ステップ 5	**key-string** *string* 例： `Router(config-keychain-key)# key-string mno172`	キーの認証文字列を指定します。 • *string* には、1 ～ 80 文字の大文字と小文字の英数字を指定できます。ただし、最初の文字を数値にすることはできません。
ステップ 6	**exit** 例： `Router(config-keychain-key)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 7	**interface** *type number* 例： `Router(config)# interface Ethernet0/1`	インターフェイス タイプを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 8	**ip address** *ip-address mask* [**secondary**] 例： `Router(config-if)# ip address 10.21.8.32 255.255.255.0`	インターフェイスのプライマリ IP アドレスまたはセカンダリ IP アドレスを指定します。
ステップ 9	**vrrp** *group* **priority** *priority* 例： `Router(config-if)# vrrp 1 priority 110`	VRRP プライオリティを設定します。

	コマンド	目的
ステップ 10	**vrrp** *group* **authentication md5 key-chain** *key-chain* 例： `Router(config-if)# vrrp 1 authentication md5 key-chain vrrp1`	VRRP MD5 認証の認証 MD5 キー チェーンを設定します。 • キー チェーン名は、ステップ 3 で指定した名前と一致する必要があります。 **（注）** VRRP グループ内のすべてのルータは、同じ認証文字列を使用して設定する必要があります。同じ認証文字列が設定されていないと、VRRP グループ内のルータが相互通信せず、正しく設定されていないいずれかのルータのステートがマスターに変わります。
ステップ 11	**vrrp** *group* **ip** [*ip-address* [**secondary**]] 例： `Router(config-if)# vrrp 1 ip 10.21.8.12`	インターフェイス上で VRRP をイネーブルにし、仮想ルータのプライマリ IP アドレスを指定します。
ステップ 12	通信を行う各ルータ上でステップ 1 ～ 11 を繰り返します。	—
ステップ 13	**end** 例： `Router(config-if)# end`	特権 EXEC モードに戻ります。

VRRP MD5 認証設定の確認

手順の概要

1. **show vrrp**
2. **debug vrrp authentication**

手順の詳細

ステップ 1 **show vrrp**

このコマンドを使用して、認証が正しく設定されていることを確認します。

```
Router# show vrrp

Ethernet0/1 - Group 1
State is Master
Virtual IP address is 10.21.0.10
Virtual MAC address is 0000.5e00.0101
Advertisement interval is 1.000 sec
Preemption is enabled
 min delay is 0.000 sec
Priority is 100
  Authentication MD5, key-string, timeout 30 secs
Master Router is 10.21.0.1 (local), priority is 100
Master Advertisement interval is 1.000 sec
Master Down interval is 3.609 sec
```

出力には、MD5 認証が設定されていることと、f00d4s キー ストリングが使用されていることが表示されます。タイムアウト値は 30 秒に設定されます。

ステップ 2　debug vrrp authentication

このコマンドを使用して、両方のルータに認証が設定されていること、各 ルータの MD5 キー ID が同じであること、各 ルータの MD5 キー ストリングが同じであることを確認します。

```
Router1#: debug vrrp authentication

VRRP: Sent: 21016401FE050000AC1801FE0000000000000000
VRRP: HshC: B861CBF1B9026130DD34AED849BEC8A1

VRRP: Rcvd: 21016401FE050000AC1801FE0000000000000000
VRRP: HshC: B861CBF1B9026130DD34AED849BEC8A1
VRRP: HshR: C5E193C6D84533FDC750F85FCFB051E1
VRRP: Grp 1 Adv from 172.24.1.2 has failed MD5 auth

Router2#: debug vrrp authentication

VRRP: Sent: 21016401FE050000AC1801FE0000000000000000
VRRP: HshC: C5E193C6D84533FDC750F85FCFB051E1

VRRP: Rcvd: 21016401FE050000AC1801FE0000000000000000
VRRP: HshC: C5E193C6D84533FDC750F85FCFB051E1
VRRP: HshR: B861CBF1B9026130DD34AED849BEC8A1
VRRP: Grp 1 Adv from 172.24.1.1 has failed MD5 auth
```

VRRP テキスト認証の設定

制約事項

RFC 2338 方式を実装したベンダーとの相互運用性は、有効ではありません。

どのような場合でも、テキスト認証を MD5 認証と組み合わせて VRRP グループに使用することはできません。MD5 認証が設定されている場合、VRRP hello メッセージのテキスト認証のフィールドはすべてゼロ（0）に設定されて送信され、受信時には無視されます（受信側のルータでも MD5 認証が有効になっている場合）。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip address** *ip-address mask* [**secondary**]
5. **vrrp** *group* **authentication text** *text-string*
6. **vrrp** *group* **ip** *ip-address*
7. 通信を行う各ルータ上でステップ 1 ～ 6 を繰り返します。
8. **end**

手順の詳細

	コマンド	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードなど、高位の権限レベルをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* **例：** `Router(config)# interface Ethernet0/1`	インターフェイス タイプを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ip address** *ip-address mask* [**secondary**] **例：** `Router(config-if)# ip address 10.0.0.1 255.255.255.0`	インターフェイスのプライマリ IP アドレスまたはセカンダリ IP アドレスを指定します。
ステップ 5	**vrrp** *group* **authentication text** *text-string* **例：** `Router(config-if)# vrrp 1 authentication text textstring1`	グループ内の他のルータから受信した VRRP パケットを認証します。 • 認証を設定する場合、VRRP グループ内のすべてのルータで同じ認証文字列を使用する必要があります。 • デフォルトの文字列は「cisco」です。 **（注）** VRRP グループ内のすべてのルータは、同じ認証文字列を使用して設定する必要があります。同じ認証文字列が設定されていないと、VRRP グループ内のルータが相互通信せず、正しく設定されていないいずれかのルータのステートがマスターに変わります。
ステップ 6	**vrrp** *group* **ip** *ip-address* **例：** `Router(config-if)# vrrp 1 ip 10.0.1.20`	インターフェイス上で VRRP をイネーブルにし、仮想ルータのプライマリ IP アドレスを指定します。
ステップ 7	通信を行う各ルータ上でステップ 1 ～ 6 を繰り返します。	—
ステップ 8	**end** **例：** `Router(config-if)# end`	特権 EXEC モードに戻ります。

SNMP VRRP 通知を送信するようにルータをイネーブル化

VRRP MIB は、SNMP GET 操作をサポートします。この操作により、ネットワーク デバイスがネットワーク管理ステーションからネットワークの VRRP グループについてのレポートを受け取ることができるようになります。

VRRP MIB トラップ サポートを有効にする操作は、CLI から行います。そして、MIB を使用してレポートを取得します。あるルータがマスターまたはバックアップ ルータになると、トラップがネットワーク管理ステーションに通知します。CLI からエントリを設定すると、直ちに、MIB でのそのグループの RowStatus がアクティブ ステートになります。

手順の概要

1. **enable**
2. **configure terminal**
3. **snmp-server enable traps vrrp**
4. **snmp-server host** *host community-string* **vrrp**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**snmp-server enable traps vrrp** 例： `Router(config)# snmp-server enable traps vrrp`	SNMP VRRP 通知（トラップおよび応答要求）を送信するように、ルータを設定します。
ステップ 4	**snmp-server host** *host community-string* **vrrp** 例： `Router(config)# snmp-server host myhost.comp.com public vrrp`	SNMP 通知動作の指定

VRRP の設定例

ここでは、次の設定例について説明します。

例：VRRP の設定

次の例では、ルータ A とルータ B はそれぞれ 3 つの VRRP グループに属しています。

各グループには次のプロパティが設定されています。

- グループ 1：
  - 仮想 IP アドレスは 10.1.0.10 です。
  - ルータ A は、プライオリティが 120 のときにこのグループのマスターになります。
  - アドバタイズ インターバルは 3 秒です。
  - プリエンプションはイネーブルになっています。
- グループ 5：
  - ルータ B は、プライオリティが 200 のときにこのグループのマスターになります。
  - アドバタイズ インターバルは 30 秒です。
  - プリエンプションはイネーブルになっています。
- グループ 100：
  - ルータ A は、より高い IP アドレス（10.1.0.2）が設定されているため、最初にこのグループのマスターになります。
  - アドバタイズ インターバルはデフォルトで 1 秒に設定されます。
  - プリエンプションはディセーブルになっています。

ルータ A

```
RouterA(config)# interface ethernet 1/0
RouterA(config-if)# ip address 10.1.0.2 255.0.0.0
RouterA(config-if)# vrrp 1 priority 120
RouterA(config-if)# vrrp 1 authentication cisco
RouterA(config-if)# vrrp 1 timers advertise 3
RouterA(config-if)# vrrp 1 timers learn
RouterA(config-if)# vrrp 1 ip 10.1.0.10
RouterA(config-if)# vrrp 5 priority 100
RouterA(config-if)# vrrp 5 timers advertise 30
RouterA(config-if)# vrrp 5 timers learn
RouterA(config-if)# vrrp 5 ip 10.1.0.50
RouterA(config-if)# vrrp 100 timers learn
```

```
RouterA(config-if)# no vrrp 100 preempt
RouterA(config-if)# vrrp 100 ip 10.1.0.100
RouterA(config-if)# no shutdown
```

ルータ B

```
RouterB(config)# interface ethernet 1/0
RouterB(config-if)# ip address 10.1.0.1 255.0.0.0
RouterB(config-if)# vrrp 1 priority 100
RouterB(config-if)# vrrp 1 authentication cisco
RouterB(config-if)# vrrp 1 timers advertise 3
RouterB(config-if)# vrrp 1 timers learn
RouterB(config-if)# vrrp 1 ip 10.1.0.10
RouterB(config-if)# vrrp 5 priority 200
RouterB(config-if)# vrrp 5 timers advertise 30
RouterB(config-if)# vrrp 5 timers learn
RouterB(config-if)# vrrp 5 ip 10.1.0.50
RouterB(config-if)# vrrp 100 timers learn
RouterB(config-if)# no vrrp 100 preempt
RouterB(config-if)# vrrp 100 ip 10.1.0.100
RouterB(config-if)# no shutdown
```

例：VRRP オブジェクト トラッキング

次の例では、トラッキング プロセスはシリアル インターフェイス 0/1 上でライン プロトコルのステートを追跡するように設定されています。イーサネット インターフェイス 1/0 の VRRP は、シリアル インターフェイス 0/1 のライン プロトコル ステートに何らかの変更が生じた場合には通知されるように、トラッキング プロセスに登録します。シリアル インターフェイス 0/1 のライン プロトコル ステートがダウンになると、VRRP グループのプライオリティは 15 減じられます。

```
Router(config)# track 1 interface Serial0/1 line-protocol
Router(config-track)# exit
Router(config)# interface Ethernet1/0
Router(config-if)# ip address 10.0.0.2 255.0.0.0
Router(config-if)# vrrp 1 ip 10.0.0.3
Router(config-if)# vrrp 1 priority 120
Router(config-if)# vrrp 1 track 1 decrement 15
```

例：VRRP オブジェクト トラッキングの確認

次に、「例：VRRP オブジェクト トラッキング」で説明した設定を確認する例を示します。

```
Router# show vrrp

Ethernet1/0 - Group 1
  State is Master
  Virtual IP address is 10.0.0.3
  Virtual MAC address is 0000.5e00.0101
  Advertisement interval is 1.000 sec
  Preemption is enabled
   min delay is 0.000 sec
  Priority is 105
   Track object 1 state Down decrement 15
  Master Router is 10.0.0.2 (local), priority is 105
  Master Advertisement interval is 1.000 sec
  Master Down interval is 3.531 sec
```

```
Router# show track

Track 1
  Interface Serial0/1 line-protocol
  Line protocol is Down (hw down)
   1 change, last change 00:06:53
  Tracked by:
   VRRP Ethernet1/0 1
```

例：キー ストリングを使用した VRRP MD5 認証の設定

次に、キー ストリングを使用して MD5 認証を設定し、タイムアウトを 30 秒に設定する例を示します。

```
Router(config)# interface Ethernet0/1
Router(config-if)# description ed1-cat5a-7/10
Router(config-if)# vrrp 1 ip 10.21.0.10
Router(config-if)# vrrp 1 priority 110
Router(config-if)# vrrp 1 authentication md5 key-string f00c4s timeout 30
Router(config-if)# exit
```

例：キー チェーンを使用した VRRP MD5 認証の設定

次に、キー チェーンを使用して MD5 認証を設定する例を示します。

```
Router(config)# key chain vrrp1
Router(config-keychain)# key 1
Router(config-keychain-key)# key-string f00c4s
Router(config-keychain-key)# exit
Router(config)#interface ethernet0/1
Router(config-if)# description ed1-cat5a-7/10
Router(config-if)# vrrp 1 priority 110
Router(config-if)# vrrp 1 authentication md5 key-chain vrrp1
Router(config-if)# vrrp 1 ip 10.21.0.10
```

この例では、VRRP はキー チェーンを照会し、特定のキー チェーンに対して現在アクティブになっているキーとキー ID を取得します。

例：VRRP テキスト認証

次に、テキスト ストリングを使用して VRRP テキスト認証を設定する例を示します。

```
Router(config)# interface fastethernet 0/0
Router(config-if)# ip address 10.21.8.32 255.255.255.0
Router(config-if)# vrrp 10 authentication text stringxyz
Router(config-if)# vrrp 10 ip 10.21.8.10
```

例：インターフェイス上での VRRP グループのディセーブル化

次に、イーサネット インターフェイス 0/2 上ではグループ 2 の VRRP を維持しながら、イーサネット インターフェイス 0/1 上にある 1 つの VRRP グループをディセーブルにする例を示します。

```
Router(config)# interface ethernet0/1
Router(config-if)# ip address 10.24.1.1 255.255.255.0
Router(config-if)# vrrp 1 ip 10.24.1.254
Router(config-if)# vrrp 1 shutdown
```

```
Router(config-if)# exit
Router(config)# interface ethernet0/2
Router(config-if)# ip address 10.168.42.1 255.255.255.0
Router(config-if)# vrrp 2 ip 10.168.42.254
```

例：VRRP MIB トラップ

次に、VRRP MIB トラップ サポート機能をイネーブルにする例を示します。

```
Router(config)# snmp-server enable traps vrrp
Router(config)# snmp-server host 10.1.1.0 community abc vrrp
```

その他の参考資料

関連資料

内容	参照先
VRRP コマンド：コマンド構文、コマンド モード、コマンド履歴、デフォルト設定、使用に関する注意事項および例	『*Cisco IOS IP Application Services Command Reference*』
キー チェーンおよびキー管理用コマンド：コマンド構文の詳細、コマンド モード、コマンド履歴、デフォルト設定、使用に関する注意事項、および例	『*Cisco IOS IP Routing : RIP Command Reference*』
オブジェクト トラッキング	「Configuring Enhanced Object Tracking」モジュール
HSRP	「Configuring HSRP」モジュール
GLBP	「Configuring GLBP」モジュール

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
この機能がサポートする新しい MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択されたプラットフォーム、シスコ ソフトウェア リリース、およびフィーチャ セットの MIB を検索してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
RFC 2338	「*Virtual Router Redundancy Protocol*」
RFC 3768	「*Virtual Router Redundancy Protocol（VRRP）*」

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 ・テクニカル サポートを受ける ・ソフトウェアをダウンロードする ・セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける ・ツールおよびリソースへアクセスする - Product Alert の受信登録 - Field Notice の受信登録 - Bug Toolkit を使用した既知の問題の検索 ・Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する ・トレーニング リソースへアクセスする ・TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

VRRP の機能情報

表 1 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。

プラットフォーム サポートとソフトウェア イメージ サポートに関する情報を入手するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator を使用すると、特定のソフトウェア リリース、フィーチャ セット、またはプラットフォームをサポートするソフトウェア イメージを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 表 1 に、特定のソフトウェア リリース トレイン内の機能に対するサポートが導入されたソフトウェア リリースだけを示します。特に断りのないかぎり、そのソフトウェア リリース トレイン以降のリリースでもその機能がサポートされます。

表 1　VRRP の機能情報

機能名	リリース	機能設定情報
FHRP—VRF-Aware VRRP	12.2(15)T 12.0(18)ST 12.2(31)SG 12.2(17d)SXB	FHRP—VRF-Aware VRRP 機能により、VRF-Aware MPLS VPN による VRRP サポートが追加されます。
FHRP—VRRP 拡張	12.3(14)T	FHRP—VRRP 拡張機能により、次のサポートが追加されます。 • MD5 認証：VRRP に設定されているルータに追加されます。HSRP と同様に、RFC 2338 に規定されている方法よりも簡単な方法を使用した、ピアの認証方法を提供します。 • Bridged Virtual Interface（BVI）：BVI に VRRP を設定する機能を追加します。この機能は、BVI に既存の HSRP サポートに類似しています。 この機能に関する詳細については、次の各項を参照してください。 • 「VRRP の制約事項」（P.2） • 「VRRP 認証」（P.7） • 「キー ストリングを使用した VRRP MD5 認証の設定」（P.15） • 「キー チェーンを使用した VRRP MD5 認証の設定」（P.17） • 「VRRP MD5 認証設定の確認」（P.19） • 「例：キー ストリングを使用した VRRP MD5 認証の設定」（P.25） • 「例：キー チェーンを使用した VRRP MD5 認証の設定」（P.25） コマンド **debug vrrp authentication** がこの機能により導入されました。 **vrrp authentication** および **show vrrp** の各コマンドがこの機能により変更されました。

表 1　VRRP の機能情報 （続き）

機能名	リリース	機能設定情報
ISSU と VRRP	12.2(33)SRC	VRRP は In Service Software Upgrade（ISSU; インサービス ソフトウェア アップグレード）をサポートします。ISSU を使用すると、アクティブおよびスタンバイの Route Processor（RP; ルート プロセッサ）またはライン カード上で異なるバージョンの Cisco IOS ソフトウェアが実行されている場合でも、ハイアベイラビリティ（HA）システムをステートフル スイッチオーバー（SSO）モードで実行できるようになります。 この機能は、ソフトウェア アップグレード中に予定されたシステム停止中も同じレベルの HA 機能を提供します。不測のシステム停止が発生した場合も、SSO を使用できます。つまり、システムをセカンダリ RP に切り替えることができ、セッションを切断することなく、またパケットの損失も最小限に抑えながら、継続してパケットを転送できます。 この機能は、デフォルトでイネーブルにされています。 この機能に関する詳細については、次の各項を参照してください。 • 「ISSU と VRRP」（P.8） この機能により、新規追加または変更されたコマンドはありません。
SSO と VRRP	12.2(33)SRC 12.2(33)SXI	VRRP が SSO を認識するようになりました。VRRP は、ルータがセカンダリ RP にフェールオーバーしたことを検出し、VRRP グループの現在の状態を継続することができます。 この機能は、デフォルトでイネーブルにされています。 この機能に関する詳細については、次の各項を参照してください。 • 「SSO と VRRP」（P.8） • 「VRRP のカスタマイズ」（P.9） **debug vrrp ha**、**vrrp sso**、**show vrrp** の各コマンドが、この機能により導入または変更されました。

表 1　VRRP の機能情報 （続き）

機能名	リリース	機能設定情報
Virtual Router Redundancy Protocol	Cisco IOS XE 3.1.0SG 12.2(13)T 12.2(14)S 15.0(1)S	VRRP は、ルータのグループを使用して単一の仮想ルータを形成し、冗長性を実現します。これにより、仮想ルータをデフォルト ゲートウェイとして使用するように、LAN クライアントを設定できます。ルータのグループを表す仮想ルータは、「VRRP グループ」とも呼ばれます。 この機能に関する詳細については、すべての項に記載しています。 この機能により次のコマンドが導入されました。**debug vrrp all**、**debug vrrp error**、**debug vrrp events**、**debug vrrp packets**、**debug vrrp state**、**show vrrp**、**show vrrp interface**、**vrrp authentication**、**vrrp description**、**vrrp ip**、**vrrp preempt**、**vrrp priority**、**vrrp timers advertise**、**vrrp timers learn**
VRRP オブジェクト トラッキング	12.3(2)T 12.2(25)S	VRRP オブジェクト トラッキング機能により VRRP の機能が拡張され、ルータ内の特定のオブジェクトを追跡して VRRP グループの仮想ルータのプライオリティ レベルを変更できるようになりました。 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。 • 「VRRP オブジェクト トラッキング」（P.6） • 「VRRP オブジェクト トラッキングの設定」（P.14） コマンド **vrrp track** がこの機能により導入されました。 コマンド **show track** がこの機能により変更されました。
VRRP MIB—RFC 2787	12.3(11)T	VRRP MIB—RFC 2787 機能により、SNMP ベースのネットワーク管理で使用できるように MIB の機能が強化されました。VRRP を使用するルータの設定、モニタ、および制御をサポートするようになりました。 この機能に関する詳細については、次の各項を参照してください。 • 「インターフェイスでの VRRP のディセーブル化」（P.12） • 「SNMP VRRP 通知を送信するようにルータをイネーブル化」（P.22） コマンド **vrrp shutdown** がこの機能により導入されました。 **snmp-server enable traps** および **snmp-server host** の各コマンドがこの機能により変更されました。

用語集

VRRP ルータ：VRRP を実行しているルータ。

仮想 IP アドレス所有者：仮想ルータの IP アドレスを所有する VRRP ルータ。仮想ルータ アドレスを物理インターフェイス アドレスとして持っているルータが所有者になります。

仮想ルータ：1 つのグループを形成する 1 台または複数台の VRRP ルータ。仮想ルータは、LAN クライアントのデフォルト ゲートウェイ ルータとして動作します。「VRRP グループ」とも呼ばれます。

仮想ルータ バックアップ：仮想ルータ マスターが機能を停止したときにパケット転送のロールを引き受けることのできる 1 台または複数台の VRRP ルータ。

仮想ルータ マスター：仮想ルータの IP アドレスに送信されるパケットの転送を現在行っている VRRP ルータ。通常、仮想ルータ マスターは IP アドレス所有者としても機能します。

UDP

IPv4 ブロードキャスト パケット処理の設定

この章では、IPv4 ブロードキャスト パケットとは何か、どのようなときに使用するか、IPv4 ブロードキャスト パケットの処理が適切でない場合のデフォルトの動作についてルータの設定をカスタマイズする方法について説明します。

（注） また、ルータによる IPv4 ブロードキャスト パケット処理のカスタマイズが必要になる一般的なシナリオも取り上げます。たとえば、Dynamic Host Configuration Protocol（DHCP）トラフィックの UDP 転送によって、DHCP クライアントによって送信されるブロードキャスト パケットが、クライアントと同じネットワーク セグメント上にない DHCP サーバに確実に到達するように設定する方法を説明します。この章では、設定作業と例についても示します。このマニュアルでは、「IP アドレス」を「IP」と表記します。これは「IP」を示すものではありません。

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、「IP ブロードキャスト パケット処理の機能情報」（P.27）を参照してください。

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

この章の構成

IPv4 ブロードキャスト パケット処理について

IP ユニキャスト アドレス

IP ユニキャスト アドレスはブロードキャスト アドレスではありません。ユニキャスト宛先 IP アドレスが設定されたパケットは、特定の IP ホストに送信されます。たとえば、172.16.1.1/32 などです。ユニキャスト パケットの送信先ホストは、パケットを受信して処理します。「ユニキャスト」という用語は、IP ブロードキャスト トラフィックのタイプとともに使用されることが多いため、ここに、このマニュアルでの意味を定義します。たとえば、ネットワーク管理者がネットワーク上のルータのアップグレードを検討する場合、ユニキャスト、マルチキャスト、およびブロードキャスト トラフィックの量を考慮しなければなりません。このタイプのトラフィックは、ルータのパフォーマンスに対してそれぞれ異なる影響を及ぼします。

IP ブロードキャスト アドレス

IP ブロードキャスト パケットは、宛先 IP ブロードキャスト アドレス 255.255.255.255（または、場合によっては IP ブロードキャスト アドレス 000.000.000.000 が使用されることがあります）に送信されます。ブロードキャスト 宛先 IP アドレス 255.255.255.255 と 000.000.000.000 は、パケットをネットワーク上の IP 対応の各デバイスに送信するときに使用されます。

（注） 宛先 IP アドレスとしてブロードキャスト IP アドレスを使用するパケットは、「ブロードキャスト パケット」と呼ばれます。

ルータがデフォルトで IP ブロードキャスト パケットを転送した場合、IP 対応の各インターフェイスを通してパケットを転送する必要があります。IP 宛先アドレス（255.255.255.255）は、ルータの IP 対応の各インターフェイスを通して到達可能と見なされるためです。IP に対応したすべてのインターフェイス経由で IP ブロードキャスト パケットを転送すると、ブロードキャスト ストーム（高レベルのブロードキャスト トラフィックが原因のネットワーク過負荷）の状態になります。ルータが、ブロー

ドキャスト IP 宛先アドレスを使用して、すべての IP 対応インターフェイスにパケットを転送した場合に発生する IP パケット ブロードキャスト ストームを回避するには、ルータのデフォルト動作でブロードキャスト パケットを転送*しない*ようにします。このことは、レイヤ 3 でのルーティング IP トラフィックとレイヤ 2 のブリッジングとの決定的な相違点です。レイヤ 2 ブリッジは、デフォルトで各インターフェイスを通して IP ブロードキャスト トラフィックを転送します。これはフォワーディング ステートで実行され、スケーラビリティの面で問題が発生します。

（注） このマニュアルでは、IP トラフィックのルーティングと ブリッジングの相違についての詳細な説明は行いません。IP トラフィックのルーティングと ブリッジングの詳細については、他の資料を参照してください。参照先については、「関連資料」（P.25）をご覧ください。

TCP/IP プロトコルでは、ネットワーク セグメント上のすべてのホストと通信したり、ネットワーク セグメントの特定のホストの IP アドレスを特定したりするために、IP ブロードキャスト アドレスを使用することがあります。次に例を示します。

- Routing Information Protocol（RIP）バージョン 1 は IP ブロードキャスト アドレスを使用してルーティング テーブル情報を送信します。これにより、ネットワーク セグメント上で RIP バージョン 1 を実行している他のホストが更新を受信して処理できます。
- Address Resolution Protocol（ARP; アドレス解決プロトコル）は、特定のレイヤ 3 IP アドレスを所有するホストのレイヤ 2 MAC アドレスを決定するために使用されます。ARP は、ローカル ネットワーク上で IP ブロードキャスト パケット（レイヤ 2 ブロードキャスト フレームでもあります）を送信します。ローカル ネットワーク上のすべてのホストは ARP ブロードキャスト パケットを受信します。このパケットがレイヤ 2 ブロードキャスト フレームとして送信されるためです。ローカル ネットワーク上のすべてのホストは ARP パケットを処理します。このパケットが IP ブロードキャスト アドレスに送信されるためです。ARP パケットのデータ領域に示されている IP アドレスを所有するホストだけが、ARP ブロードキャスト パケットに応答します。

IP 誘導ブロードキャスト アドレス

IP 誘導ブロードキャストは、リモート ネットワーク上のすべてのホストに到達するために使用されます。IP ネットワーク アドレスが認識されている場合にのみデータをリモート IP ホストに送信する必要のあるルータは、IP 誘導ブロードキャストを使用してリモート ホストに到達します。たとえば、ホスト（IP アドレスは 192.168.100.1）から宛先 IP アドレス（172.16.255.255）に送信された誘導ブロードキャストは、172.16.0.0 のアドレス空間（IP アドレスが 172.16.0.0 から始まるホスト）内にあるホストにのみ到達します。

IP 誘導ブロードキャスト パケットは、ターゲット サブネットに到達するまで、ネットワーク経由でユニキャスト パケットとしてルーティングされます。到達すると、レイヤ 2 ブロードキャスト フレーム（MAC アドレス FFFF.FFFF.FFFF）に変換されます。IP アドレッシング アーキテクチャの特性により、チェーンの最後のルータ（ターゲット サブネットに直接接続されているルータ）のみが最終的に誘導ブロードキャストを特定します。たとえば、アドレス空間 172.16.0.0/16 内の IP アドレス（172.16.1.1/16 など）を使用してネットワークに接続しているインターフェイスを使うルータだけが、172.16.255.255 に送信されたパケットが誘導ブロードキャストであることを確認し、これをレイヤ 2 ブロードキャストに変換します。変換されたブロードキャストは、ローカル ネットワーク上のすべてのホストによって受信されます。ネットワーク上のその他のルータ（172.16.0.0/16 ネットワークに接続されていないルータ）は、パケットを特定の IP ホスト向けであるかのように扱い、172.16.255.255 宛てにパケットを転送します。

リモート ネットワーク上のすべてのホストは、レイヤ 2 ブロードキャスト フレームに変換された後、IP 誘導ブロードキャストを受信します。理想的には、意図された宛先ホストだけが、IP 誘導ブロードキャストを完全に処理して応答すべきです。ただし、IP 誘導ブロードキャストが悪意のある目的で使用される可能性があります。たとえば、一般的な Smurf Denial of Service（DoS; サービス拒否）攻撃

やその攻撃から派生したもので IP 誘導ブロードキャストが使用されます。「smurf」攻撃では、攻撃者は攻撃対象であるデバイスの送信元 IP アドレスを使用して Internet Control Message Protocol（ICMP; インターネット制御メッセージ プロトコル）エコー 要求（ping）を誘導ブロードキャスト アドレスに送信します。通常、企業のネットワーク内部にあるホスト（Web サーバ）などがターゲットとなります。ICMP エコー 要求が企業のネットワーク内の IP 誘導ブロードキャスト アドレスに送信されます。これに起因して、ターゲット サブネット上のすべてのホストが攻撃対象のデバイスに ICMP エコー応答を送信します。このような要求の連続ストリームを送信することによって、攻撃者は、より大量の応答ストリームを作成して、攻撃対象のホストを混乱させることができます。DoS 攻撃で IP 誘導ブロードキャストがどのように使用されるのかについての詳細は、インターネットで「IP 誘導ブロードキャスト」、「サービス拒否」、「smurf 攻撃」などを検索してください。

ルータが誘導ブロードキャストを転送し、誘導ブロードキャストを要求するアプリケーションの数を減少させるというセキュリティ上の問題が予測されるため、IP 誘導ブロードキャストは Cisco IOS Release 12.0 以降のリリースではデフォルトでディセーブルに設定されています。IP 誘導ブロードキャストのサポートが必要なネットワークでは、IP 誘導ブロードキャストからレイヤ 2 ブロードキャストへの変換を行うインターフェイス上で **ip directed-broadcast** コマンドを使用して、この機能をイネーブルにできます。たとえば、ルータがファスト イーサネット インターフェイス 0/0 上で、ファスト イーサネット インターフェイス 0/1 に割り当てられているネットワーク アドレスへの IP 誘導ブロードキャストを受信している場合、IP 誘導ブロードキャストをレイヤ 2 ブロードキャストに変換して インターフェイス Fastethernet 0/1 に出力するには、ファスト イーサネット インターフェイス 0/1 で **ip directed-broadcast** コマンドを設定します。IP 誘導ブロードキャストのレイヤ 2 ブロードキャストへの変換を制御するアクセス リストを指定できます。アクセス リストを指定すると、そのリストで許可されている IP パケットだけが誘導ブロードキャストからレイヤ 2 ブロードキャストに変換されます。たとえば、ネットワーク内の IP 誘導ブロードキャストの正規の送信元 IP アドレスが 192.168.10.2 であるとわかっている場合、192.168.10.2 からのトラフィックを許可する拡張 IP アクセス リストを作成し、**ip directed-broadcast** *access-list* コマンドを使用してこのアクセス リストを割り当てることができます。

IP 誘導ブロードキャスト

IP 誘導ブロードキャストはデフォルトでドロップされます。IP 誘導ブロードキャストをドロップすると、DoS 攻撃のリスクが軽減します。

ブロードキャストが物理ブロードキャストになっているインターフェイスで、IP 誘導ブロードキャストの転送を有効にすることができます。IP 誘導ブロードキャストの送信先である IP ネットワークに接続されたインターフェイスで、誘導 IP ブロードキャスト パケットをレイヤ 2 ブロードキャスト フレームに変換できます。たとえば、IP 宛先アドレスが 172.16.10.255 の IP 誘導ブロードキャストをレイヤ 2 ブロードキャスト フレームに変換する必要がある場合、変換は、IP ネットワーク 172.16.10.0/24 に接続されているインターフェイス上で行うことができます。

転送する誘導ブロードキャストを制御するアクセス リストを指定できます。アクセス リストを指定すると、そのリストで許可されている IP パケットだけが誘導ブロードキャストから物理ブロードキャストに変換されます。

Cisco IOS Release 12.0 以降のリリースでは、IP 誘導ブロードキャストはデフォルトでディセーブルになっています。ネットワークで IP 誘導ブロードキャストをサポートする必要がある場合は、次の作業のいずれかを行います。

IP マルチキャスト

IP マルチキャスト アドレスは、ローカル ネットワーク上のホストの任意のサブセットに到達するために使用されます。IP ブロードキャスト アドレスでは、処理が必要な情報が含まれているかどうかを確認するためにホストがそれぞれ各パケット内のデータを受信して処理しなければならないため、問題が生じます。IP マルチキャスト アドレスでは、送信されてきたパケットを処理する前に認識するようにホストを設定した既知の IP アドレスを使用することで、この問題を解決します。ホストが IP マルチキャスト パケットを受信すると、ホストはこの IP マルチキャスト アドレスを、認識するように設定されたマルチキャスト アドレスのリストと比較します。IP マルチキャスト アドレスを認識しないように設定されている場合、ホストはパケットを無視します（パケットを処理してパケット内のデータを分析することはしません）。ホストはパケットを無視できるため、（パケットが処理対象の IP ブロードキャストであるかどうかについて時間をかけて確認する場合と比較して）時間やリソースを節約できます。

表 1 に、マルチキャスト アドレスに予約されている IP アドレスの範囲を示します。

表 1　　IIP マルチキャスト アドレス範囲

クラス	範囲
D	224.0.0.0 ～ 239.255.255.255/32（255.255.255.255）

今日使用されている大部分の TCP/IP ルーティング プロトコルは、IP マルチキャスト アドレスを使用して、同じローカル ネットワーク上で同じルーティング プロトコルを実行しているホストにルーティング更新およびその他の情報を送信します。インターネット上の多くのアプリケーション（オーディオ/ビデオ ストリーミングなど）は、IP マルチキャスト アドレスを使用します。現在割り当てられている IP マルチキャスト アドレスのリストについては、次の URL に掲載されている「*Internet Multicast Addresses*」を参照してください。http://www.iana.org/assignments/multicast-addresses。

IP マルチキャスト サポートのネットワーク デバイスを設定する方法の詳細については、次のマニュアルを参照してください。

- 『*Cisco IOS IP Multicast Configuration Guide*』
- 『*Cisco IOS IP Multicast Command Reference*』

初期の IP 実装

初期の IP 実装では、現在のブロードキャスト アドレス標準である 255.255.255.255 は使用されていないことがありました。ブロードキャスト アドレスを指すオール 1 のアドレスではなく、古い標準であるすべてゼロ（000.000.000.000）のアドレスを呼び出していました。このような実装の多くは、すべてが 1 のブロードキャスト アドレスを認識しないため、ブロードキャストに正しく応答できません。他の転送ではすべて 1 のブロードキャスト（デフォルト）が使用されましたが、重大なネットワーク過負荷（「*ブロードキャスト ストーム*」といいます）が生じました。このような問題が生じる実装として、バージョン 4.3 よりも前の Berkeley Standard Distribution（BSD）UNIX バージョンをベースとしたシステムがあります。

DHCP

DHCP では、クライアント（DHCP サーバからの情報を要求するホスト）がブロードキャスト パケットを送信し、DHCP サーバを検出して設定情報を求めることが必要です。DHCP サーバが、DHCP ブロードキャストを送信するクライアントと同じネットワーク セグメント上にない場合は、DHCP 要求を適切なネットワークに転送するようにルータを設定する必要があります。

DHCP の詳細については、次の URL に掲載されている RFC 2131「*Dynamic Host Configuration Protocol*」（http://www.ietf.org/rfc/rfc2131.txt）を参照してください。

UDP ブロードキャスト パケットの転送

UDP ブロードキャスト パケットは、複数のホストに同時に同じデータを送信する必要のある、DHCP などの TCP/IP プロトコルやアプリケーションによって使用されます。ルータはデフォルトでブロードキャスト パケットを転送しないため、UDP ブロードキャスト トラフィックが発生するネットワークではルータの設定をカスタマイズする必要があります。UDP ブロードキャスト パケットを転送するための 1 つのオプションとして、UDP 転送機能を使用する方法があります。UDP 転送は、UDP パケットのブロードキャスト IP アドレスをユニキャスト（特定のホスト）IP アドレスまたは誘導 IP ブロードキャストに書き換えます。アドレスが書き換えられた後、UDP パケットはパス内のすべてのルータによって宛先ネットワークに転送されます。この場合、他のルータに設定変更が要求されることはありません。

DHCP 要求などの UDP ブロードキャスト パケットを、同じターゲット ネットワークのホスト（1 つまたは複数）に転送することができます。UDP ブロードキャスト パケットを転送すると、宛先 IP アドレスは、設定したアドレスに一致するように書き換えられます。たとえば、**ip helper-address 172.16.10.2** コマンドを実行すると、IP 宛先アドレスが 255.255.255.255 から 172.16.10.2 に書き換えられます。

UDP ブロードキャスト パケットを特定のホストに転送できるようにするには、**ip helper-address** *address* コマンドを設定するときに特定のホストの IP アドレスをヘルパー アドレスとして使用します。ある範囲のホストに転送する UDP ブロードキャスト パケットでロード シェアリングと冗長性を可能にするには、**ip helper-address** *address* コマンドを設定するときに IP 誘導ブロードキャスト アドレスをヘルパー アドレスとして使用します。

UDP ブロードキャスト パケットのフラッディング

UDP ブロードキャスト パケットを確実にホストに到達させるための別のオプションとして、レイヤ 2 ブリッジング Spanning Tree Protocol（STP; スパニング ツリー プロトコル）によって作成された転送データベースを使用して、ネットワーク全体で制御されたやり方で IP ブロードキャストをフラッディングさせる方法があります。この機能をイネーブルにすると、フラッディング ループも回避されます。この機能をサポートするため、ルータ上の Cisco IOS ソフトウェアで透過的なブリッジングをサポートする必要があります。透過的なブリッジングは、フラッディングに関与する各インターフェイスに設定することが必要です。ブリッジングが設定されていないインターフェイスでは、ブロードキャストを受信できる状態が続きます。ただし、このインターフェイスが受信したブロードキャストを転送することはなく、別のインターフェイスで受信されたブロードキャストを、このインターフェイスを使用してルータが送信することもありません。

IP ヘルパー アドレス メカニズムを使用して単一のネットワーク アドレスに転送されたパケットは、フラッディングすることがあります。各ネットワーク セグメントには、パケットの 1 つのコピーだけが送信されます。

フラッディングを考慮して、パケットは次の基準を満たす必要があります（これらの同じ条件を使用して、IP ヘルパー アドレスを使用したパケット転送を考慮します）。

- パケットは MAC レベルのブロードキャスト（FFFF.FFFF.FFFF）であることが必要です。
- パケットは IP レベルのブロードキャスト（255.255.255.255）であることが必要です。
- パケットは、Trivial File Transfer Protocol（TFTP; 簡易ファイル転送プロトコル）、DNS、Time、NetBIOS、ND、または BOOTP パケットであることが必要です。または、UDP プロトコルが **ip forward-protocol udp** グローバル コンフィギュレーション コマンドで指定される必要があります。
- パケットの Time-to-Live（TTL; 存続可能時間）値は 2 以上でなければなりません。

フラッディングされた UDP パケットを特定のホストに送信するには、インターフェイス コンフィギュレーション モードで **ip broadcast-address** コマンドを使用して、フラッディングされた UDP パケットのレイヤ 3 IP ブロードキャスト アドレスを変更できます。フラッディングされた UDP パケットのアドレスは、任意の IP アドレスに設定できます。フラッディングされた UDP パケットの送信元アドレスは変更されません。フラッディングされた UDP パケットの TTL 値は減じられます。

インターフェイス上でデータグラムを送信することが決定されると（宛先 IP アドレスが変わることがあります）、データグラムは通常の IP 出力 ルーチンに渡されるため、アクセス リストに制約されます（出力インターフェイスに指定されている場合）。

実際のブリッジングを必要としない場合は、ブリッジされたすべてのタイプのパケットを拒否する type-code ブリッジング フィルタを設定できます。アクセス リストを使用してブリッジされたトラフィックをフィルタリングする方法の詳細については、『*Cisco IOS Bridging and IBM Networking Configuration Guide*』の「Configuring Transparent Bridging」を参照してください。スパニング ツリー データベースを使用して、IP 転送コードを使ってフラッディングを行うことができます。

IP ブロードキャストのフラッディングの高速化

スパニング ツリー アルゴリズムを使用して UDP データグラムのフラッディングを高速化できます。グローバル コンフィギュレーション モードで **ip forward-protocol spanning-tree** コマンドとともに使用すると、この機能はスパニング ツリー ベースの UDP フラッディングのパフォーマンスを 4 ～ 5 倍に高めます。「*ターボ フラッディング*」と呼ばれるこの機能は、Advanced Research Projects Agency（ARPA）でカプセル化されたイーサネット インターフェイス、FDDI、および High-Level Data-Links Control（HDLC; 高レベル データ リンク制御）でカプセル化されたシリアル インターフェイス上でサポートされます。ただし、トークン リング インターフェイスではサポートされません。トークン リング インターフェイスおよび HDLC 以外のシリアル インターフェイスが UDP フラッディングに使用されているブリッジ グループの一部を構成していないときは、ターボ フラッディングは通常どおりに動作します。

デフォルト UDP ポート番号

ヘルパー アドレスが指定され、UDP 転送が有効になっている場合は、次のポート番号宛てのブロードキャスト パケットがデフォルトで転送されます。

- Trivial File Transfer Protocol（TFTP; 簡易ファイル転送プロトコル）（ポート 69）
- Domain Naming System（DNS; ドメイン ネーム システム）（ポート 53）
- タイム サービス（ポート 37）
- NetBIOS ネーム サーバ（ポート 137）
- NetBIOS データグラム サーバ（ポート 138）
- Boot Protocol（BOOTP; ブート プロトコル）クライアントおよびサーバ パケット（ポート 67 および 68）
- TACACS サービス（ポート 49）
- IEN-116 ネーム サービス（ポート 42）

UDP ブロードキャスト パケット フラッディング

IP ブロードキャストは、ブリッジング Spanning Tree Protocol（STP; スパニング ツリー プロトコル）で作成されたデータベースを使用した制御されたやり方で、ネットワーク全体でフラッディングさせることができます。この機能をイネーブルにすると、ループも回避されます。この機能をサポートするために、ルーティング ソフトウェアにトランスペアレント ブリッジングを組み込み、フラッディングに参加するインターフェイスごとにブリッジングを設定する必要があります。ブリッジングが設定されていないインターフェイスでは、ブロードキャストを受信できる状態が続きます。ただし、このインターフェイスが受信したブロードキャストを転送することはなく、別のインターフェイスで受信されたブロードキャストを、このインターフェイスを使用してルータが送信することもありません。

- IP ヘルパー アドレス メカニズムを使用して単一のネットワーク アドレスに転送されたパケットは、フラッディングすることがあります。各ネットワーク セグメントには、パケットの 1 つのコピーだけが送信されます。

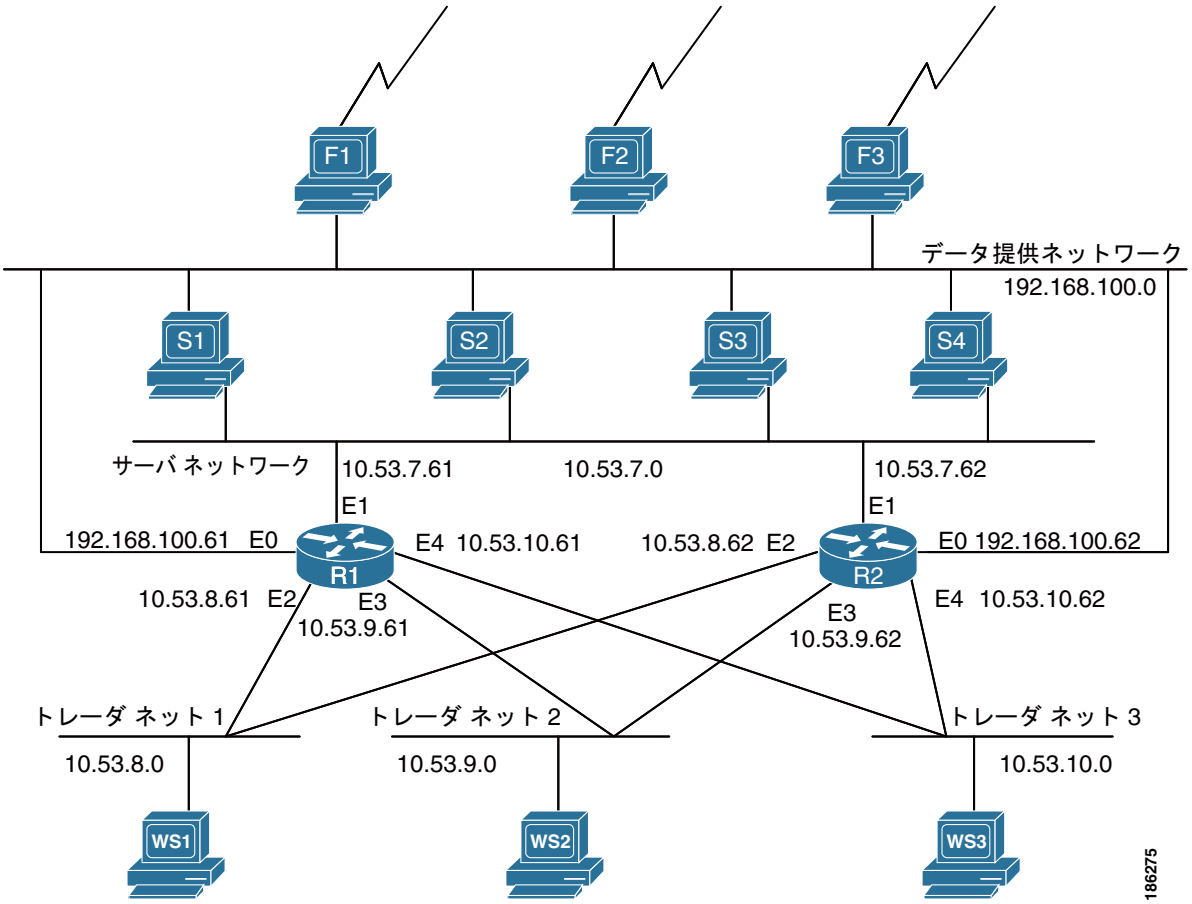
デフォルト IP ブロードキャスト アドレス

Cisco IOS ソフトウェアは、LAN と WAN の両方での IP ブロードキャスト送信をサポートします。IP ブロードキャスト アドレスを指定するには、いくつかの方法があります。現在、最も一般的な方法であり、デフォルトでもある方法は、すべてが 1 で構成されたアドレス（255.255.255.255）ですが、ソフトウェアは、任意の形式の IP ブロードキャスト アドレス（すべてが 0（0.0.0.0）など）や 172.16.255.255 などの誘導ブロードキャストを生成するように設定することができます。Cisco IOS ソフトウェアはほとんどの IP ブロードキャスト アドレスを受信して処理できます。

UDP ブロードキャスト パケット ケース スタディ

このケース スタディは、金融会社の立会場アプリケーションを事例に挙げたものです。図 2 に示すワークステーション（WS1、WS2、おおび WS3）は、データ提供ネットワークから財務データを受信します。財務データは UDP ブロードキャストを使用して送信されます。

図 1　UDP ブロードキャスト転送が必要なトポロジ



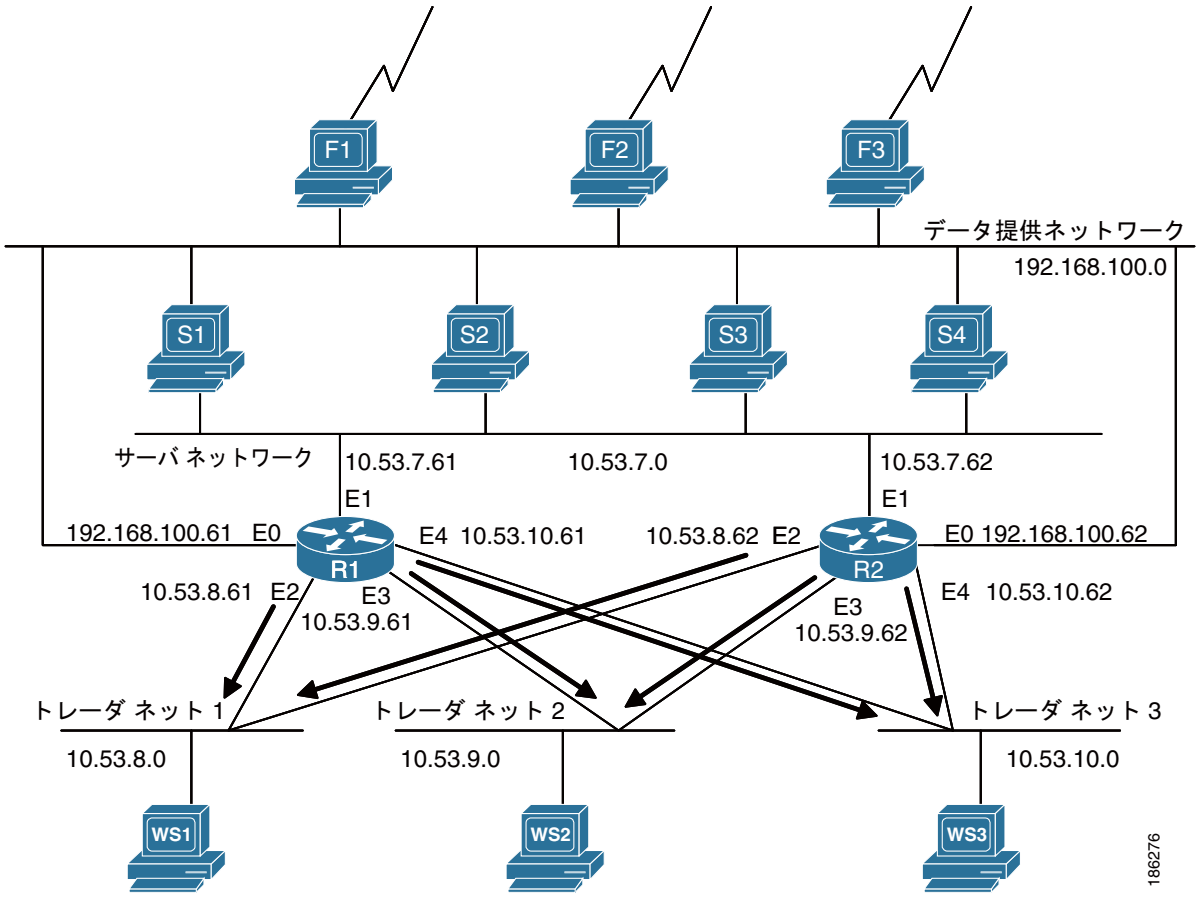
次に、このアプリケーションで可能性のある解決策を説明します。

- 「UDP ブロードキャスト パケット転送」（P.9）
- 「UDP ブロードキャスト パケット フラッディング」（P.11）

UDP ブロードキャスト パケット転送

最初のオプションとして、ヘルパー アドレスを使用した UDP ブロードキャスト パケットがあります。ヘルパー アドレッシングを設定するには、転送されるべき UDP ブロードキャストを受信するルータごとに、各インターフェイスで **ip helper-address** コマンドを指定する必要があります。図 1 のルータ 1 とルータ 2 では、サーバ ネットワークからトレーダ ネットワークにデータを移動するように、IP ヘルパー アドレスを設定できます。ただし、IP ヘルパー アドレッシングは、このタイプのトポロジに最適な解決策であるとはいえません。なぜなら、各ルータが他のルータから不要なブロードキャストを受信するためです（図 2）。

図 2　ルータからトレーダ ネットワークへの UDP パケットのフロー（IP ヘルパー アドレッシングを採用したルータからトレーダ ネットワークへの IP ヘルパー アドレッシング パケットを使用）



この場合、ルータ 1 はルータ 2 によって送信された各ブロードキャストをセグメントごとに 1 回、計 3 回受信します。ルータ 2 はルータ 1 によって送信された各ブロードキャストをセグメントごとに 1 回、計 3 回受信します。ブロードキャストを受信するごとに、ルータはそれを分析し、ブロードキャストを転送する必要があるかどうか判断しなければなりません。ネットワークに追加されるセグメントが多くなるにつれて、ルータは（分析して破棄する）不要なトラフィックで過負荷になります。

このタイプのトポロジで IP ヘルパー アドレッシングを使用すれば、UDP ブロードキャストの転送に複数のルータを設定することはできなくなります（受信するアプリケーションが重複するブロードキャストを処理できる場合を除きます）。これは、トレーダ ネットワークに重複するパケットが到達するためです。これにより設計上の冗長化を制限できますが、実装によってはこの制限は望ましくないことがあります。

このタイプのトポロジで UDP ブロードキャストを双方向に送信するには、UDP ブロードキャストを受信する各ルータ インターフェイスに別の **ip helper-address** コマンドを適用する必要があります。ネットワークに追加されるセグメントやデバイスが多くなるにつれて、ブロードキャストを到達させるために必要となる ip helper-address コマンドの数が多くなり、これらのルータの管理は時間の経過とともに複雑化します。

（注）　このトポロジの双方向トラフィックは、ルータのパフォーマンスに著しい影響を及ぼします。

IP ヘルパー アドレッシングは非冗長であるブロードキャスト ループを制御するためのメカニズムを必要としない非並列トポロジに適していますが、これらの欠点を考慮すると、IP ヘルパー アドレッシングはこのトポロジでは適切に機能しません。パフォーマンスを向上させるため、ネットワーク設計者は次の 4 つの案を考えました。

- サーバのブロードキャスト アドレスをオール 1（255.255.255.255）に設定する：データ提供ネットワークにサーバ ブロードキャストを送り返すことからサーバには複数のインターフェイスが設定されるため、この案は却下されました。また、一部のワークステーション実装では、複数のインターフェイスが存在する場合にブロードキャストを 1 つに集約することは不可能です。
- サーバのブロードキャスト アドレスを主要なネットワーク ブロードキャスト IP アドレスに設定する：ネットワークがサブネット化されている場合はサーバの TCP/IP 実装で主要なネットワーク IP ブロードキャスト アドレスを使用することができないため、この案は却下されました。
- サブネットをなくし、ワークステーションが Address Resolution Protocol（ARP; アドレス解決プロトコル）を使用してアドレスを学習できるようにする：プライマリ ルータが機能を停止した場合、サーバが代替ルートを迅速に学習できないため、この案は却下されました。
- UDP ブロードキャスト パケット フラッディング：この案では、透過的なブリッジングを使用して作成されるスパニング ツリー トポロジを採用し、冗長トポロジでの UDP ブロードキャスト パケットの転送を行います。この際、ループおよび重複したブロードキャスト トラフィックは回避されます。

ネットワーク設計者は、UDP 転送を使用した最初の 3 つの案を除外し、4 番目のオプションである UDP ブロードキャスト パケット フラッディング（「UDP フラッディング」と呼ばれることもあります）を採用しました。UDP フラッディングは、重複したパケットはない状態で冗長性をサポートします。また、ルータが機能を停止した際の高速コンバージェンスおよびデータ損失の最小化を確保します。

UDP ブロードキャスト パケット フラッディング

UDP フラッディングはスパニング ツリー アルゴリズムを使用して制御されたやり方でパケットを転送します。スパニング ツリーを構築することを目的に、各ルータ インターフェイス上でブリッジングをイネーブルにします。スパニング ツリーは、ブロードキャストを受信したインターフェイスからのブロードキャストの転送を停止することで、ループを回避します。また、スパニング ツリーは、特定のインターフェイスをブロック ステート（パケットは転送されません）にし、他のインターフェイスをフォワーディング ステート（転送が必要なパケットは転送されます）にすることで、パケットの複製も防ぎます。

UDP フラッディングをイネーブルにするには、ルータで透過的なブリッジングをサポートするソフトウェアを実行し、フラッディングに関与するインターフェイスごとにブリッジングを設定する必要があります。ブリッジングが設定されていないインターフェイスではブロードキャストを受信しますが、ルータはこれらのブロードキャストを転送せず、別のインターフェイスで受信したブロードキャストの送信先としてこのインターフェイスを使用することもありません。

（注） Cisco IOS ソフトウェア リリース 10.2 よりも前のリリースでは、フラッディング サブネット ブロードキャストはサポートされません。

UDP フラッディングが設定されているルータは、出力インターフェイスで **ip broadcast-address** コマンドによって指定された宛先アドレスを使用して、宛先アドレスを フラッディングされた UDP データグラムに割り当てます。このため、データグラムがネットワーク内を伝播するにつれて宛先アドレスが変わることがあります。ただし、送信元アドレスは変わりません。

UDP フラッディングにより、図 3 に示すルータはスパニング ツリーを使用してネットワーク トポロジを制御し、ブロードキャストの転送を行います。**bridge protocol** コマンドには、**dec** キーワード（DEC スパニング ツリー プロトコルの場合）または **ieee** キーワード（IEEE イーサネット プロトコル

の場合）を指定できます。ネットワーク上のすべてのルータでは、同じスパニング ツリー プロトコルを有効にする必要があります。**ip forward-protocol spanning-tree** コマンドは、**bridge protocol** コマンドで作成されたデータベースを使用します。各セグメントにはブロードキャスト パケットが 1 つだけ到着し、UDP ブロードキャストはネットワークを双方向に通過できます。

スパニング ツリー データベースを構築することを目的にブリッジングをイネーブルにしているため、アクセス リストを使用して、スパニング ツリーで非 UDP トラフィックが転送されないようにします。この章では、ブリッジされたすべてのパケットをブロックするアクセス リストを設定する例について、後述します。

パケットを転送またはブロックするインターフェイスを決定するため、ルータ設定で各インターフェイスのパス コストを指定します。イーサネットのデフォルトのパス コストは 100 です。ルータ 2 の各インターフェイスのパス コストを 50 に設定すると、スパニング ツリー アルゴリズムにより、ルータ 2 のインターフェイスがフォワーディング ステートに設定されます。この場合、ルータ 1 のインターフェイスにはより高いパス コスト（100）が設定されていると、ルータ 1 のインターフェイスはブロック ステートになり、ブロードキャストを転送しません。これらのインターフェイス ステートに基づいて、ブロードキャスト トラフィックはルータ 2 を経由します。ルータ 2 の機能が停止すると、スパニング ツリー アルゴリズムによりルータ 1 のインターフェイスがフォワーディング ステートに設定され、ルータ 1 によりブロードキャスト トラフィックの転送が行われます。

サーバ ネットワークからトレーダ ネットワークへのブロードキャスト トラフィックの転送を行うルータを 1 台にして、もう 1 つ別のユニキャスト トラフィック転送を設定できれば理想的です。このため、各ルータで ICMP Router Discovery Protocol（IRDP）をイネーブルにし、トレーダ ネットワーク上の各ワークステーションで IRDP デーモンを実行します。ルータ 1 で **preference** キーワードを使用することで、ルータ 2 よりも高い IRDP プリファレンスが設定されます。これにより、各 IRDP デーモンは、ユニキャスト トラフィック転送の優先するデフォルト ゲートウェイとしてルータ 1 を使用するようになります。これらのワークステーションのユーザは、**netstat -rn** を使って、ルータがどのように使用されているかを参照できます。

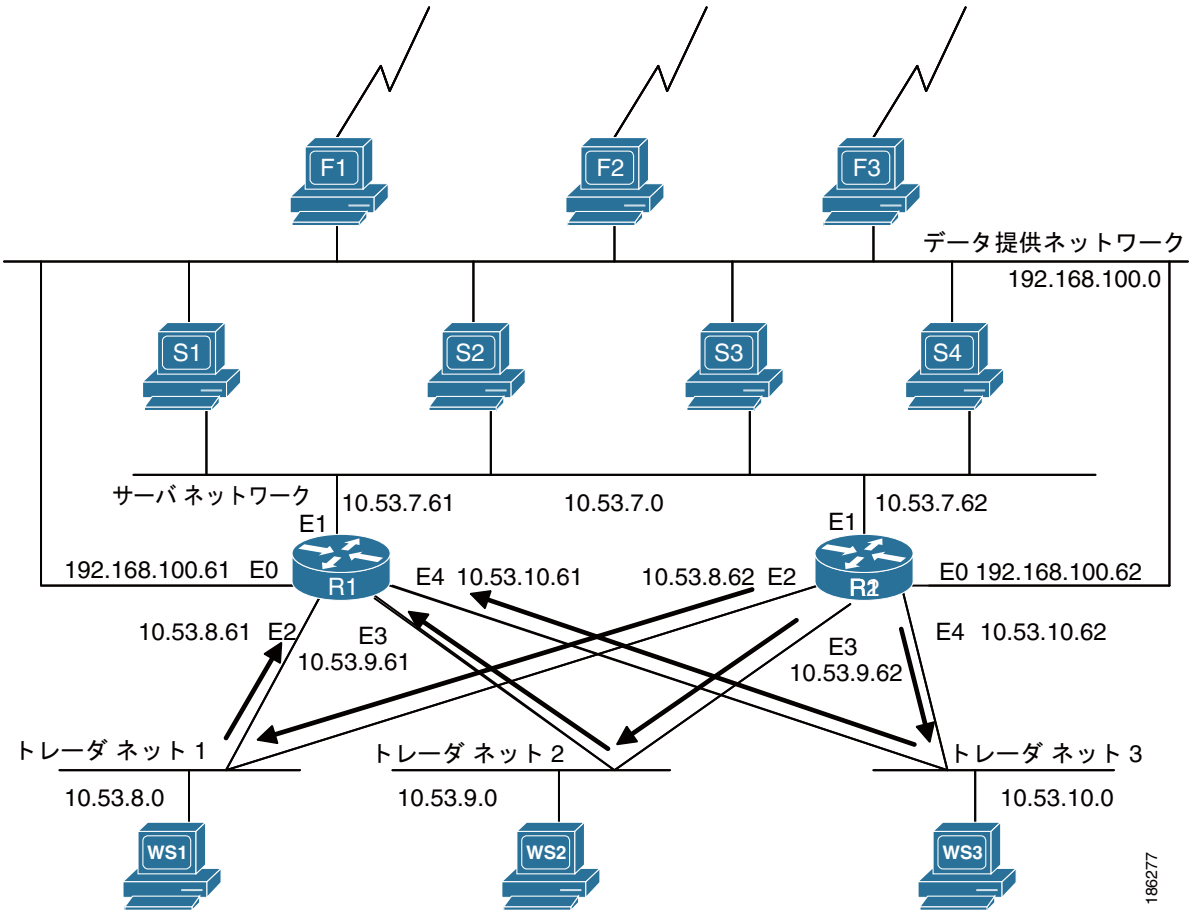
ルータ で **holdtime**、**maxadvertinterval**、および **minadvertinterval** キーワードを使用するとアドバタイズ インターバルがデフォルトよりも短くなり、ホストで実行している IRDP デーモンのアドバタイズメントを参照する頻度が高くなります。アドバタイズ インターバルの値を減少させると、ルータ 1 が使用できなくなった場合にワークステーションはより迅速にルータ 2 を使用できるようになります。この設定では、ルータが使用できなくなった場合に IRDP が提供するコンバージェンス時間は 1 分未満になります。

次の理由により、IRDP が Routing Information Protocol（RIP）やデフォルト ゲートウェイよりも優先されます。

- コンバージにかかる時間は RIP の方が長く、通常は 1 ～ 2 分を要します。
- トレーダ ネットワーク上にある各 Sun ワークステーションでルータ 1 をデフォルト ゲートウェイとして設定すると、これらの Sun ワークステーションからルータ 1 にユニキャスト トラフィックを送信できるようになりますが、ルータ 1 が使用できなくなった場合に代替ルートは提供されません。

図 3 に、ネットワークが UDP フラッディング用に設定されている場合のデータ フローを示します。

図 3　UDP フラッディングおよび IRDP を使用したデータ フロー



（注） このトポロジは、ブロードキャスト集約型です。ブロードキャストが イーサネット帯域幅（10MB）の 20% を消費することがあります。ただし、IP ヘルパー アドレッシングを設定した場合と比較して好ましい数値です。同じネットワークに IP ヘルパー アドレッシングを設定すると、ブロードキャストがイーサネット帯域幅（10MB）の最大 50% を消費することがあります。

トレーダ ネットワークのホストは、ユニキャスト トラフィックを処理するルータの選択に使用される IRDP、Hot Standby Routing Protocol（HSRP; ホット スタンバイ ルーティング プロトコル）、Virtual Router Redundancy Protocol（VRRP; 仮想ルータ冗長プロトコル）、または Gateway Load Balancing Protocol（GLBP; ゲートウェイ ロード バランシング プロトコル）をサポートしません。これらのプロトコルにより、プライマリ ルータが使用できなくなったときにスタンバイ ルータが迅速に引き継ぐことができます。First Hop Redundancy Protocol の詳細については、『*Cisco IOS IP Application Services Configuration Guide*』の「FHRP Features Roadmap」を参照してください。

ルータのターボ フラッディングをイネーブルにして、UDP フラッディングのパフォーマンスを向上させます。

（注） ターボ フラッディングは割り込みレベルで実行する処理量を増加させ、これにより、ルータの CPU 負荷が高くなります。ターボ フラッディングは、すでに CPU 負荷の高いルータや他の CPU 集約型アクティビティを実行する必要のあるルータでの使用は適切でないことがあります。

IP ブロードキャスト パケット処理の設定方法

IP 誘導ブロードキャストのイネーブル化（アクセス リストなし）

任意の送信元から IP 誘導ブロードキャストを転送できるようにするには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip address** *address mask*
5. **ip directed-broadcast**
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* **例：** `Router(config)# interface fastethernet 0/1`	インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	**ip address** *address mask* 例： `Router(config-if)# ip address 172.16.10.1 255.255.255.0`	インターフェイスに IP アドレスを割り当てます。
ステップ 5	**ip directed-broadcast** 例： `Router(config-if)# ip directed-broadcast`	インターフェイスの IP 誘導ブロードキャストをイネーブルにします。誘導ブロードキャスト パケットの IP ネットワーク アドレスに接続されているインターフェイスでこのコマンドを設定します。 この例では、誘導ブロードキャスト パケットは 172.16.10.255 宛てに送信されます。
ステップ 6	**end** 例： `Router(config-if)# end`	現在のコンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

IP 誘導ブロードキャストのイネーブル化（アクセス リスト使用）

ip directed-broadcast コマンドにアクセス リストを適用して IP 誘導ブロードキャストの転送を制限するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **access-list list 100-199 permit ip** *source-address mask destination-address mask*
4. **interface** *type number*
5. **ip address** *address mask*
6. **ip directed-broadcast** *access-list*
7. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**access-list list 100-199 permit ip** *source-address mask destination-address mask* **例：** `Router(config)# access-list 100 permit ip 10.4.9.167 0.0.0.0 172.16.10.0 0.0.0.255`	転送する IP 誘導ブロードキャストを制限するアクセス リストを作成します。 この例では、IP 誘導ブロードキャストは、IP アドレスが 10.4.9.167 のホストによって IP 誘導ブロードキャスト アドレス 172.16.10.255 に送信されます。
ステップ 4	**interface** *type number* **例：** `Router(config)# interface fastethernet 0/0`	インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 5	**ip address** *address mask* **例：** `Router(config-if)# ip address 172.16.10.1 255.255.255.0`	インターフェイスに IP アドレスを割り当てます。
ステップ 6	**ip directed-broadcast** *access-list* **例：** `Router(config-if)# ip directed-broadcast 100`	割り当てたアクセス リストによって許可されたブロードキャスト パケットのインターフェイスで、IP 誘導ブロードキャストをイネーブルにします。誘導ブロードキャスト パケットの IP ネットワーク アドレスに接続されているインターフェイスでこのコマンドを設定します。 この例では、誘導ブロードキャスト パケットは 172.16.10.255 宛てに送信されます。
ステップ 7	**end** **例：** `Router(config-if)# end`	現在のコンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

UDP ブロードキャスト パケットの特定ホストへの転送のイネーブル化

UDP ブロードキャスト パケットのシングル ホストへの転送をイネーブルにするには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip forward-protocol udp**
4. **interface** *type number*
5. **ip address** *address mask*
6. **ip helper-address** *address*
7. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip forward-protocol udp** 例： `Router(config)# ip forward-protocol udp`	UDP ブロードキャストへの転送を有効にします。
ステップ 4	**interface** *type number* 例： `Router(config)# interface fastethernet 0/1`	インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 5	**ip address** *address mask* 例： `Router(config-if)# ip address 172.16.10.1 255.255.255.0`	インターフェイスに IP アドレスを割り当てます。
ステップ 6	**ip helper-address** *address* 例： `Router(config-if)# ip helper-address 172.16.10.2`	UDP ブロードキャスト パケットを受信しているインターフェイスの IP ヘルパー アドレスを有効にします。 この例では、IP UDP ブロードキャスト パケットの IP 宛先アドレスが 172.16.10.2 に書き換えられます。
ステップ 7	**end** 例： `Router(config-if)# end`	現在のコンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

UDP ブロードキャスト パケットのアドレス範囲内ホストへの転送のイネーブル化

宛先ホスト間のロード シェアリングを可能にし、1 つまたは複数の宛先ホストが機能停止した場合に冗長化を提供するように、ホストのアドレス範囲を指定して UDP ブロードキャスト パケットを転送できるようにするには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip forward-protocol udp**
4. **interface** *type number*
5. **ip address** *address mask*
6. **ip helper-address** *address*
7. **interface** *type number*
8. **ip address** *address mask*
9. **ip directed-broadcast**
10. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip forward-protocol udp** 例： `Router(config)# ip forward-protocol udp`	UDP ブロードキャストへの転送を有効にします。
ステップ 4	**interface** *type number* 例： `Router(config)# interface fastethernet 0/0`	インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 5	**ip address** *address mask* 例： `Router(config-if)# ip address 192.168.10.1 255.255.255.0`	インターフェイスに IP アドレスを割り当てます。

	コマンドまたはアクション	目的
ステップ 6	**ip helper-address** *address* 例： `Router(config-if)# ip helper-address 172.16.10.255`	UDP ブロードキャスト パケットを受信しているインターフェイスの IP ヘルパー アドレスを有効にします。 この例では、1 つの IP 誘導ブロードキャスト アドレスを使用しています。IP UDP ブロードキャスト パケットの IP 宛先アドレスが 172.16.10.255 に書き換えられます。 UDP ブロードキャスト パケットが対象とするアプリケーションまたはサービスをサポートする 172.16.10.0/24 ネットワーク上のすべてのホストが、UDP ブロードキャスト パケットに応答します。 **（注）** この場合、UDP ブロードキャスト パケットの送信元が複数のホストから応答を受信することがよくあります。ほとんどの場合、UDP ブロードキャスト パケットの送信元は最初の応答を受け入れ、それ以降の応答は無視します。UDP ブロードキャスト パケットの送信元が重複した応答を処理できず、クラッシュしたり予期できない動作を行ったりすることがあります。
ステップ 7	**interface** *type number* 例： `Router(config)# interface fastethernet 0/1`	インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 8	**ip address** *address mask* 例： `Router(config-if)# ip address 172.16.10.1 255.255.255.0`	インターフェイスに IP アドレスを割り当てます。
ステップ 9	**ip directed-broadcast** 例： `Router(config-if)# ip directed-broadcast`	UDP ブロードキャストを送信しているインターフェイスの IP 誘導ブロードキャストを有効にします。
ステップ 10	**end** 例： `Router(config-if)# end`	現在のコンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

ルータの全インターフェイスのデフォルト IP ブロードキャスト アドレスを 0.0.0.0 に変更（不揮発性メモリなし）

ルータが不揮発性メモリ（NVRAM）を装備していない場合に IP ブロードキャスト アドレスを 0.0.0.0 に変更する必要があるときは、プロセッサ コンフィギュレーション レジスタのジャンパを設定し、IP ブロードキャスト アドレスを手動で変更します。ビット 10 を設定すると、デバイスはすべてゼロ（0）を使用するようになります。ビット 10 は、ブロードキャスト アドレスのネットワーク部とサブネット部を制御するビット 14 と相互に作用します。ビット 14 を設定すると、デバイスに、ブロードキャスト アドレスのアドレスのネットワーク部とサブネット部が含まれるようになります。表 2 に、ビット 10 とビット 14 の設定の組み合わせの効果を示します。

表 2　ブロードキャスト アドレス宛先のコンフィギュレーション レジスタ設定

ビット 14	ビット 10	アドレス（<ネット><ホスト>）
Out	Out	<オール 1><オール 1>
Out	In	<ゼロ><ゼロ>
In	In	<ネット><ゼロ>
In	Out	<ネット><オール 1>

ルータでのハードウェア ジャンパ設定の詳細については、ルータに付属のハードウェア マニュアルを参照してください。

ルータの全インターフェイスのデフォルト IP ブロードキャスト アドレスを 0.0.0.0 に変更（不揮発性メモリ使用）

NVRAM を装備した Cisco IOS ベースのルータにはソフトウェア コンフィギュレーション レジスタがあり、これを使用してルータの一部の動作を変更できます。たとえば、ロードするイメージの検索場所、使用する IP ブロードキャスト アドレス、およびコンソールの回線速度を変更できます。コンフィギュレーション レジスタの出荷時デフォルト値は 0x2102 です。ここで、*0X* はこの数値が 16 進数であることを示します。ソフトウェア コンフィギュレーション レジスタの設定を変更するには、**config-register** コマンドを使用します。

config-register コマンドを使用してソフトウェア コンフィギュレーション レジスタの動作を設定する方法の詳細については、次のマニュアルを参照してください。

- 『*Cisco IOS Configuration Fundamentals Configuration Guide*』の「Loading and Managing System Images」
- 『*Cisco IOS Configuration Fundamentals Command Reference*』

注意　ルータのソフトウェア コンフィギュレーション レジスタの変更は慎重に行ってください。コンソール ポートに設定する速度を把握していてターミナル アプリケーションの回線速度の変更方法を知っている場合を除き、コンソール ポートの回線速度を不注意に変更するとコンソール ポートのターミナル サーバを使用するようにルータを設定できなくなります。Telnet や Web ブラウザなどの代替方法を使用して CLI にアクセスするようにルータを設定している場合は、この方法を使用してルータにログインし、ソフトウェア コンフィギュレーション レジスタを 0x2102 に戻します。

各インターフェイスの IP ブロードキャスト アドレスを 0.0.0.0 に設定するには、次の手順を実行します（その他はソフトウェア コンフィギュレーション レジスタ設定のデフォルト値をそのまま使用します）。

手順の概要

1. **enable**
2. **configure terminal**
3. **config-register** *value*
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**config-register** *value* 例： `Router(config)# config-register 0x2502`	各インターフェイスの IP ブロードキャスト アドレスを 0.0.0.0 に設定します。その他はソフトウェア コンフィギュレーション レジスタ設定のデフォルト値をそのまま使用します。
ステップ 4	**end** 例： `Router(config-if)# end`	現在のコンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

IP ブロードキャスト アドレスをルータの 1 つ以上のインターフェイスにある任意の IP アドレスに変更

ネットワークで 255.255.255.255 または 0.0.0.0 以外の IP ブロードキャスト アドレスが必要な場合や、ルータのすべてのインターフェイスではなくインターフェイスのサブセットの IP ブロードキャスト アドレスを 0.0.0.0 に変更したい場合は、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip address** *address mask*
5. **ip broadcast-address** *address*
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* **例：** `Router(config)# interface fastethernet 0/1`	インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ip address** *address mask* **例：** `Router(config-if)# ip address 172.16.10.1 255.255.255.0`	インターフェイスに IP アドレスを割り当てます。
ステップ 5	**ip broadcast-address** *address* **例：** `Router(config-if)# ip broadcast-address 172.16.10.255`	IP ブロードキャスト アドレスを指定します。 この例では、IP ブロードキャストは 172.16.10.255 に送信されます。
ステップ 6	**end** **例：** `Router(config-if)# end`	現在のコンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

UDP ブロードキャスト パケット フラッディングの設定

前提条件

ルータに搭載されている Cisco IOS ソフトウェアには、透過的なブリッジングをサポートするバージョンを使用する必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **bridge** *number* **protocol ieee**
4. **ip forward-protocol spanning-tree**
5. **ip forward-protocol turbo-flood**
6. **ip forward-protocol udp**
7. **interface** *type number*
8. **ip address** *address mask*
9. **bridge-group** *number*
10. **interface** *type number*
11. **ip address** *address mask*
12. **bridge-group** *number*
13. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**bridge** *number* **protocol ieee** 例： `Router(config)# bridge 1 protocol ieee`	スパニング ツリー ブリッジングをイネーブルにし、ブリッジング プロトコルを指定します。
ステップ 4	**ip forward-protocol spanning-tree** 例： `Router(config)# ip forward-protocol spanning-tree`	スパニング ツリー転送テーブルを使用してブロードキャスト パケットをフラッディングできるようにします。

	コマンドまたはアクション	目的
ステップ 5	**ip forward-protocol turbo-flood** **例：** `Router(config)# ip forward-protocol turbo-flood`	（任意）スパニング ツリー転送テーブルを使用したブロードキャスト パケットの高速転送を行うことができるようにします。
ステップ 6	**ip forward-protocol udp** **例：** `Router(config)# ip forward-protocol udp`	UDP ブロードキャストへの転送を有効にします。
ステップ 7	**interface** *type number* **例：** `Router(config)# interface fastethernet 0/0`	インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 8	**ip address** *address mask* **例：** `Router(config-if)# ip address 192.168.10.1 255.255.255.0`	インターフェイスに IP アドレスを割り当てます。
ステップ 9	**bridge-group** *number* **例：** `Router(config-if)# bridge-group 1`	指定のスパニング ツリー ブリッジ グループにインターフェイスを設定します。
ステップ 10	**interface** *type number* **例：** `Router(config-if)# interface fastethernet 0/1`	インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 11	**ip address** *address mask* **例：** `Router(config-if)# ip address 172.16.10.1 255.255.255.0`	インターフェイスに IP アドレスを割り当てます。
ステップ 12	**bridge-group** *number* **例：** `Router(config-if)# bridge-group 1`	指定のスパニング ツリー ブリッジ グループにインターフェイスを設定します。
ステップ 13	**end** **例：** `Router(config-if)# end`	現在のコンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

IP ブロードキャスト パケット処理の設定例

ここでは、次の設定例について説明します。

例：アクセス リストを使用した IP 誘導ブロードキャストのイネーブル化

次に、アクセス リストを使用して IP 誘導ブロードキャストを設定し、転送される誘導ブロードキャストを制御する方法の例を示します。

```
Router(config)# access-list 100 permit ip 10.4.9.167 0.0.0.0 172.16.10.0 0.0.0.255
Router(config)# interface fastethernet 0/0
Router(config-if)# ip address 172.16.10.1 255.255.255.0
Router(config-if)# ip directed-broadcast 100
```

例：UDP ブロードキャスト パケット フラッディングの設定

次に、UDP ブロードキャスト パケット フラッディングを設定する方法の例を示します。

```
Router(config)# bridge 1 protocol ieee
Router(config)# ip forward-protocol spanning-tree
Router(config)# ip forward-protocol turbo-flood
Router(config)# ip forward-protocol udp
Router(config)# interface fastethernet 0/0
Router(config-if)# ip address 192.168.10.1 255.255.255.0
Router(config-if)# bridge-group 1
Router(config)# interface fastethernet 0/1
Router(config-if)# ip address 172.16.10.1 255.255.255.0
Router(config-if)# bridge-group 1
```

その他の参考資料

関連資料

内容	参照先
Cisco IOS コマンド	『*Cisco IOS Master Commands List, All Releases*』
現在割り当てられている IP マルチキャスト アドレス	『*Internet Multicast Addresses*』 http://www.iana.org/assignments/multicast-addresses
基礎的な設定作業	『*Cisco IOS Configuration Fundamentals Configuration Guide*』
基礎的な設定作業	『*Cisco IOS Configuration Fundamentals Command Reference*』
Cisco IOS ブリッジングおよび IBM ネットワーキングの設定作業	『*Cisco IOS Bridging and IBM Networking Configuration Guide*』
Cisco IOS ブリッジングおよび IBM ネットワーキングの設定作業	『*Cisco IOS Bridging and IBM Networking Command Reference*』

規格

規格	タイトル
IEEE spanning-tree Bridging	『802.1D MAC Bridges』 http://www.ieee802.org/1/pages/802.1D-2003.html

MIB

MIB	MIB リンク
—	新しい MIB または変更された MIB はサポートされていません。また、既存の MIB に対するサポートに変更はありません。

RFC

RFC	タイトル
RFC 1812	「*Requirements for IP Version 4 Routers*」 http://www.ietf.org/rfc/rfc1812.txt
RFC 2131	「*Dynamic Host Configuration Protocol*」 http://www.ietf.org/rfc/rfc2131.txt

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 ・テクニカル サポートを受ける ・ソフトウェアをダウンロードする ・セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける ・ツールおよびリソースへアクセスする - Product Alert の受信登録 - Field Notice の受信登録 - Bug Toolkit を使用した既知の問題の検索 ・Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する ・トレーニング リソースへアクセスする ・TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

IP ブロードキャスト パケット処理の機能情報

表 3 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。

プラットフォーム サポートとソフトウェア イメージ サポートに関する情報を入手するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator を使用すると、特定のソフトウェア リリース、フィーチャ セット、またはプラットフォームをサポートするソフトウェア イメージを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 表 3 に、特定のソフトウェア リリース トレイン内の機能に対するサポートが導入されたソフトウェア リリースだけを示します。特に断りのないかぎり、そのソフトウェア リリース トレイン以降のリリースでもその機能がサポートされます。

表 3　IP ブロードキャスト パケット処理の機能情報

機能名	リリース	機能情報
IP 誘導ブロードキャスト	10.0	誘導ブロードキャストの物理ブロードキャストへの変換をイネーブルにします。 この機能については、次の項に説明があります。 • 「IP 誘導ブロードキャスト」（P.4） • 「IP 誘導ブロードキャストのイネーブル化（アクセス リストなし）」（P.14） • 「IP 誘導ブロードキャストのイネーブル化（アクセス リスト使用）」（P.15） • 「例：アクセス リストを使用した IP 誘導ブロードキャストのイネーブル化」（P.25） コマンド **ip directed-broadcast** がこの機能により導入または変更されました。
UDP ブロードキャスト パケット転送	10.0	UDP ブロードキャスト パケットの転送をイネーブルにします。 この機能については、次の項に説明があります。 • 「UDP ブロードキャスト パケットの転送」（P.6） • 「UDP ブロードキャスト パケットのフラッディング」（P.6） • 「IP ブロードキャストのフラッディングの高速化」（P.7） **ip forward-protocol** および **ip helper-address** の各コマンドがこの機能により導入または変更されました。

表 3　IP ブロードキャスト パケット処理の機能情報 （続き）

機能名	リリース	機能情報
スパニング ツリーを使用したパケットのフラッディング	10.0	スパニング ツリー転送テーブルを使用した UDP ブロードキャスト パケットの高速転送を行うことができるようにします。 この機能については、次の項に説明があります。 • 「UDP ブロードキャスト パケット フラッディングの設定」（P.23） **ip forward-protocol spanning-tree** および **ip forward-protocol turbo-flood** の各コマンドがこの機能により導入または変更されました。
IP ブロードキャスト アドレスの指定	10.0	インターフェイスの IP ブロードキャスト アドレスを指定します。 この機能については、次の項に説明があります。 • 「IP 誘導ブロードキャスト アドレス」（P.3） • 「IP 誘導ブロードキャスト」（P.4） • 「デフォルト IP ブロードキャスト アドレス」（P.8） • 「ルータの全インターフェイスのデフォルト IP ブロードキャスト アドレスを 0.0.0.0 に変更（不揮発性メモリなし）」（P.19） • 「ルータの全インターフェイスのデフォルト IP ブロードキャスト アドレスを 0.0.0.0 に変更（不揮発性メモリ使用）」（P.20） • 「IP ブロードキャスト アドレスをルータの 1 つ以上のインターフェイスにある任意の IP アドレスに変更」（P.21） コマンド **ip broadcast-address** がこの機能により導入または変更されました。

UDP Forwarding Support for IP Redundancy Virtual Router Groups 機能の設定

User Datagram Protocol（UDP; ユーザ データグラム プロトコル）転送は、特定の IP アドレスで受信したブロードキャスト パケットとマルチキャスト パケットを転送するために Cisco IOS ソフトウェアで使用する機能です。現在、Hot Standby Routing Protocol（HSRP; ホット スタンバイ ルーティング プロトコル）とともに Virtual Router Group（VRG; 仮想ルータ グループ）サポートが実装されているため、ルータのセットをグループ化して論理ルータとし、既知の IP アドレスに応答できます。UDP Forwarding Support for IP Redundancy Virtual Router Groups 機能を使用すると、UDP 転送で VRG を認識できるようになり、結果として VRG のアクティブ ルータのみを対象に転送できるようになります。

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、「UDP Forwarding Support for IP Redundancy Virtual Router Groups の機能情報」（P.6）を参照してください。

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

この章の構成

UDP Forwarding Support for IP Redundancy Virtual Router Groups 機能について

UDP Forwarding Support for Virtual Router Groups 機能の利点

転送先が、VRG 内のすべてのルータではなく、VRG 内のアクティブ ルータに限定されます。この機能が実装される前は、VRG をサポートしているのは HSRP だけでした。HSRP によって形成された VRG では、UDP ベースのブロードキャスト パケットおよびマルチキャスト パケットの転送は VRG 内のすべてのルータによって実行されます。このプロセスは、一部の DHCP サーバが正しく機能していない場合に発生します。転送先を VRG 内のアクティブ ルータに限定するには、UDP 転送コードで VRG を認識するようにします。

VRG の認識は、IP Redundancy Service（IRS; IP 冗長性サービス）を使用することで実現できます。IRS API により、特定の VRG のアップデートの通知、VRG の追加や削除、VRG の現在のステートの照会などを実行できます。ステート変化の通知は、VRG のステートの照会が必要になるたびにパフォーマンスに影響が及ぶことを避けるために行われます。UDP 転送コードは、定義されたヘルパー アドレスの VRG ステートをキャッシュします。UDP 転送コードの実行が必要になるたびに、ヘルパー アドレスに関連付けられた VRG の現在のステートをチェックし、アクティブな VRG に対してのみ転送を行います。

（注） UDP Forwarding Support for Virtual Router Groups 機能を使用できるのは、VRG をサポートするプラットフォームだけです。

UDP Forwarding Support for IP Redundancy Virtual Router Groups 機能の設定方法

UDP Forwarding Support for IP Redundancy Virtual Router Groups 機能の設定

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip helper-address** *address* **redundancy** *vrg-name*
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* 例： `Router(config)# interface fastethernet 0/0`	インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ip helper-address** *address* **redundancy** *vrg-name* 例： `Router(config-if)# ip helper-address 10.1.1.1 redundancy shop`	VRG の UDP 転送サポートを有効にします。
ステップ 5	**end** 例： `Router(config-if)# end`	現在のコンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

UDP Forwarding Support for IP Redundancy Virtual Router Groups 機能の設定例

• 「UDP Forwarding Support for IP Redundancy Virtual Router Groups の設定」（P.3）

UDP Forwarding Support for IP Redundancy Virtual Router Groups の設定

次に、UDP Forwarding Support for IP Redundancy Virtual Router Groups 機能を設定する例を示します。

```
Router(config)# interface fastethernet 0/0
Router(config-if)# no shutdown
Router(config-if)# ip address 172.16.10.1 255.255.255.0
Router(config-if)# ip helper-address 10.1.1.1 redundancy shop
```

その他の参考資料

関連資料

内容	参照先
IP アプリケーション サービス コマンド：コマンド構文、コマンド モード、コマンド履歴、デフォルト設定、使用に関する注意事項、および例	『*Cisco IOS IP Application Services Command Reference*』

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
この機能がサポートする新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択されたプラットフォーム、シスコ ソフトウェア リリース、およびフィーチャ セットの MIB を検索してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
新しい RFC または変更された RFC はサポートされていません。また、既存の RFC に対するサポートに変更はありません。	—

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 ・テクニカル サポートを受ける ・ソフトウェアをダウンロードする ・セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける ・ツールおよびリソースへアクセスする - Product Alert の受信登録 - Field Notice の受信登録 - Bug Toolkit を使用した既知の問題の検索 ・Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する ・トレーニング リソースへアクセスする ・TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/techsupport

UDP Forwarding Support for IP Redundancy Virtual Router Groups の機能情報

表 1 に、この章に記載されている機能を示します。ここに記載のないテクノロジーの機能の詳細については、お使いの Cisco IOS リリースに該当する資料を参照してください。

プラットフォーム サポートとソフトウェア イメージ サポートに関する情報を入手するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator を使用すると、特定のソフトウェア リリース、フィーチャ セット、またはプラットフォームをサポートするソフトウェア イメージを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 表 1 に、特定のソフトウェア リリース トレイン内の機能に対するサポートが導入されたソフトウェア リリースだけを示します。特に断りのないかぎり、そのソフトウェア リリース トレイン以降のリリースでもその機能がサポートされます。

表 1　UDP Forwarding Support for IP Redundancy Virtual Router Groups の機能情報

機能名	リリース	機能情報
UDP Forwarding Support for IP Redundancy Virtual Router Group	Cisco IOS XE 3.1.0SG 12.2(15)T	User Datagram Protocol（UDP; ユーザ データグラム プロトコル）転送は、特定の IP アドレスで受信したブロードキャスト パケットとマルチキャスト パケットを転送するために Cisco IOS ソフトウェアで使用する機能です。現在、Hot Standby Routing Protocol（HSRP; ホット スタンバイ ルーティング プロトコル）とともに Virtual Router Group（VRG; 仮想ルータ グループ）サポートが実装されているため、ルータのセットをグループ化して論理ルータとし、既知の IP アドレスに応答できます。UDP Forwarding Support for IP Redundancy Virtual Router Groups 機能を使用すると、UDP 転送で VRG を認識できるようになり、結果として VRG のアクティブ ルータのみを対象に転送できるようになります。 コマンド **ip helper-address** が導入または変更されました。