ファーストホップ冗長プロトコルコンフィギュレーションガイド

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

【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。

目 次

第 1 章

最初にお読みください。

Cisco IOS XE 16 に関する重要な情報

現行の Cisco IOS XE リリース 3.7.0E（Catalyst スイッチ用）および Cisco IOS XE リリース 3.17S（アクセスおよびエッジルーティング用）の 2 つのリリースは、1 つのバージョンの統合されたリリース（Cisco IOS XE 16）へと発展しています。これにより、スイッチングおよびルーティング ポートフォリオの幅広い範囲のアクセスおよびエッジ製品に 1 つのリリースで対応できます。

（注） 技術設定ガイドの機能情報の表には、機能が導入された時期が示されています。その他のプラットフォームでその機能がサポートされた時期については示されていない場合があります。特定の機能がご使用のプラットフォームでサポートされているかどうかを特定するには、製品のランディング ページに示されている技術設定ガイドを参照してください。技術設定ガイドが製品のランディング ページに表示されている場合は、その機能がプラットフォームでサポートされていることを示します。

第 2 章

『Configuring GLBP』

ゲートウェイ ロード バランシング プロトコル（GLBP）は、ホットスタンバイ ルータ プロトコル（HSRP）や仮想ルータ冗長プロトコル（VRRP）のように、機能を停止したデバイスや回路からデータ トラフィックを保護します。このとき、冗長化されたデバイス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。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

GLBP の制限事項

拡張オブジェクト トラッキング（EOT）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、デバイスが物理インターフェイス上の複数のMACアドレスをサポートできることを確認してください。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 に関する情報

GLBP の概要

GLBP は、IEEE 802.3 LAN 上でデフォルト ゲートウェイを 1 つだけ指定して設定された IP ホストの自動デバイス バックアップを行います。LAN 上の複数のファーストホップ デバイスを連結し、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 デバイスを提供します。LAN 上にあるその他のデバイスは、冗長化された GLBP デバイスとして動作できます。このデバイスは、既存のフォワーディング デバイス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 および VRRP は、仮想 IP アドレスを指定して設定された仮想デバイス グループに、複数のデバイスを参加させます。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 デバイスとして、1 つのメンバが選択されます。グループ内の他のデバイスは、アクティブ デバイスで障害が発生するまでは冗長デバイスです。これらのスタンバイ デバイスには、プロトコルによって使用されていない未使用帯域幅があります。同じデバイスセットに対して複数の仮想デバイス グループを設定できますが、ホストは異なるデフォルト ゲートウェイに対して設定する必要があります。その結果、管理上の負担が大きくなります。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、複数のデバイス（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デバイス間に分散されるため、単一のデバイスだけが処理して残りのデバイスがアイドルのままになるようなことはありません。各ホストは、同じ仮想IPアドレスで設定され、仮想デバイス グループ内のすべてのデバイス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、UDP ポート 3222（送信元と宛先）に送信されます。

GLBP パケット タイプ

GLBP は実行に 3 つの異なるパケット タイプを使用します。そのパケット タイプは、Hello、要求、および応答です。Hello パケットはプロトコル情報をアドバタイズするために使用されます。

Hello パケットはマルチキャストで、仮想ゲートウェイまたはバーチャル フォワーダが Speak、Standby、Active のいずれかの状態のときに送信されます。要求パケットと応答パケットは、仮想 MACアドレスの割り当てに使用されます。これらはどちらもアクティブ仮想ゲートウェイ（AVG）間のユニキャスト メッセージです。

GLBP アクティブ仮想ゲートウェイ

GLBP グループのメンバは、1 つのゲートウェイをそのグループのアクティブ仮想ゲートウェイ（AVG）として選択します。他のグループ メンバは、AVG が使用できなくなった場合のバックアップとなります。AVG は GLBP グループの各メンバに仮想 MAC アドレスを割り当てます。各ゲートウェイは、AVG によって割り当てられている仮想 MAC アドレスに送信されたパケットを転送する役割を引き継ぎます。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 アドレスのアドレス解決プロトコル（ARP）要求への応答も行います。ロードシェアリングは、AVG が異なる仮想 MAC で ARP 要求に応答することによって行われます。

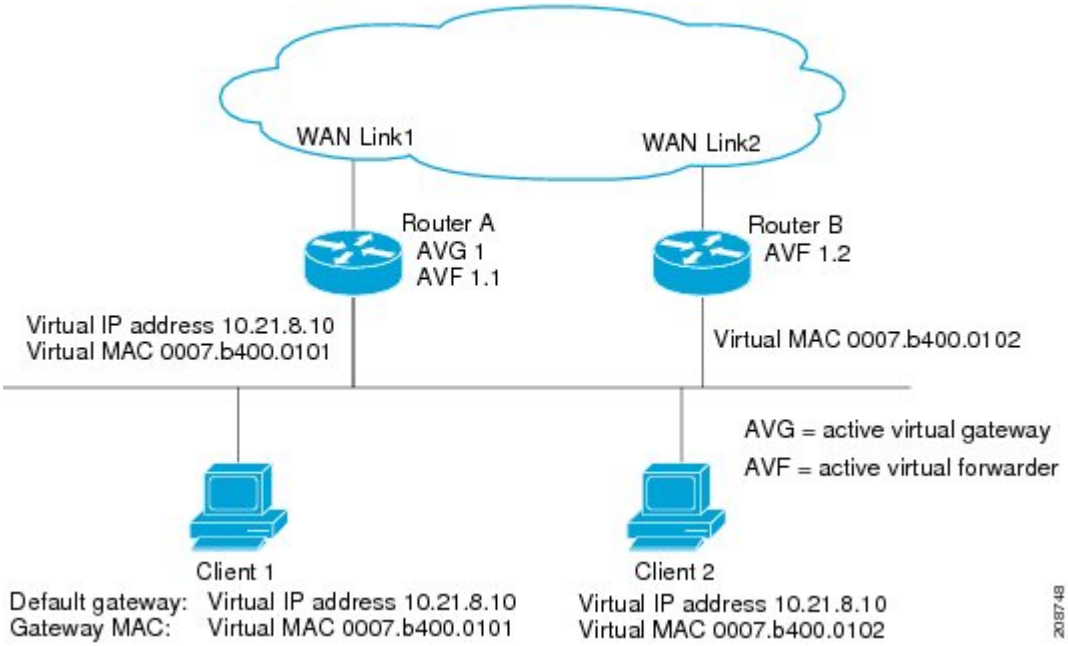
Cisco IOS Release 15.0(1)M1 および 12.4(24)T2 よりも前のリリースでは、**noglbpload-balancing** コマンドが設定されている場合は、必ず、AVG がその AVF の MAC アドレスで ARP 要求に応答します。

Cisco IOS Release 15.0(1)M1 および 12.4(24)T2 以降のリリースでは、**noglbpload-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、先頭のバーチャル フォワーダ（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。

下の図では、ルータ A（またはデバイス 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（またはデバイス B）は同じ GLBP グループのメンバであり、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、ルータ B がルータ A とトラフィック負荷を分担するため、ゲートウェイ MAC アドレス 0007.b400.0102 が与えられます。

図 *1*：*GLBP* トポロジ



ルータ A が使用できなくなった場合でも、クライアント 1 は WAN にアクセスできます。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引き継ぎ、ルータ B 自身の仮想 MAC アドレスに送信されたパケットに応答するからです。ルータ B は、GLBP グループ全体の AVG の役割も引き継ぎます。GLBP グループ内のデバイスで障害が発生しても、GLBP メンバの通信は継続されます。

GLBP 仮想 MAC アドレスの割り当て

GLBP 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。AVG は、仮想 MAC アドレスをグループの各メンバに割り当てます。他のグループ メンバは、hello メッセージを通じて AVG を検出したあとで仮想 MAC アドレスを要求します。ゲートウェイには、シーケンスにおける次の MAC アドレスが割り当てられます。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性

GLBP では、HSRP と同じ方法で仮想ゲートウェイの冗長性が実現されます。1 つのゲートウェイが AVG として選択され、もう 1 つ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ッスン状態になります。

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。その後、リッスン状態のゲートウェイから新しいスタンバイ仮想ゲートウェイが選択されます。

GLBP 仮想フォワーダの冗長性

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 で障害が発生すると、リッスン状態のセカンダリ仮想フォワーダの 1 つが仮想 MAC アドレスの役割を引き継ぎます。

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でもあります。GLBP は、ゲートウェイがアクティブ仮想フォワーダ状態に変わるとすぐに始動する 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。GLBP は hello メッセージを使用してタイマーの現在の状態を通信します。

リダイレクト時間は、AVG がホストを古い仮想フォワーダ MAC アドレスにリダイレクトし続ける時間です。リダイレクト時間が経過すると、仮想フォワーダが、古い仮想フォワーダ MAC アドレスに送信されたパケットを転送し続けても、AVG は、ARP 応答で古い仮想フォワーダ MAC アドレスの使用を停止します。

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。期限切れになった仮想フォワーダ番号は、AVG による再割り当てが可能になります。

GLBP ゲートウェイのプライオリティ

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 デバイス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、および現在の AVG で障害が発生した場合に AVG になる順番も決まります。各バックアップ仮想ゲートウェイのプライオリティには、**glbppriority** コマンドを使用して 1 ～ 255 の値を設定できます。

「GLBP トポロジ」の図では、LAN トポロジ内の AVG であるルータ A（またはデバイス A）で障害が発生すると、選択プロセスが実行され、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、ルータ B（またはデバイス B）がグループ内の唯一の他のメンバであるため、ルータ B（またはデバイス B）が自動的に新しい AVG になります。同じ GLBP グループ内にプライオリティの高い別のデバイスが存在していた場合は、そのプライオリティの高いデバイスが選択されます。両方のデバイス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方式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、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にかかわらず、現在の AVG で障害が発生した場合だけです。**glbppreempt** コマンドを使用すると、GLBP 仮想ゲートウェイのプリエンプティブ方式をイネーブルにすることができます。プリエンプションを使用すると、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に、そのバックアップ仮想ゲートウェイを AVG にすることができます。

GLBP ゲートウェイの重み付けとトラッキング

GLBP では、重み付けによって GLBP グループ内の各デバイスの転送容量を決定します。GLBP グループ内のデバイスに割り当てられた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、転送する場合はパケットを転送する LAN 内のホストの比率を決定できます。しきい値は、GLBP の重み付けが一定の値を下回ったときに転送を無効化し、別のしきい値を上回ったときには自動的に転送を再度有効化にするように設定できます。

GLBP グループの重み付けは、デバイス内のインターフェイス状態のトラッキングによって自動的に調整できます。追跡対象のインターフェイスがダウンした場合、GLBP グループの重み付けは指定された値だけ小さくなります。GLBP の重み付けの減少値は、追跡対象のインターフェイスごとに変えることができます。

デフォルトでは、GLBP 仮想フォワーダのプリエンプティブ方式はイネーブルになっており、遅延は 30 秒です。現在の AVF の重み付けが下限しきい値を下回り、その状態で 30 秒経過すると、バックアップ仮想フォワーダが AVF になります。**noglbpforwarderpreempt** コマンドを使用して GLBP 転送のプリエンプティブ方式を無効化するか、**glbpforwarderpreemptdelayminimum** コマンドを使用して遅延を変更することができます。

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 認証を使用すると、別のプレーンテキスト認証方式よりもセキュリティを強化でき、スプーフィング ソフトウェアから保護できます。

MD5 認証では、各 GLBP グループ メンバが秘密キーを使用して、発信パケットに含まれるキー付き 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、着信パケット内のハッシュが生成されたハッシュに一致しない場合、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で直接指定するか、またはキー チェーンを使用して間接的に指定できます。キー ストリングは、100 文字の長さを超えることはできません。

デバイスは、GLBP グループに対する認証設定と異なる設定を持つデバイスからの着信 GLBP パケットを無視します。GLBP には、次の 3 つの認証方式があります。

- 認証なし
- プレーン テキスト認証

- MD5 認証

GLBP パケットは、次のいずれかの場合に拒否されます。

- 認証方式がデバイスと着信パケットの間で異なっている。
- MD5 ダイジェストがデバイスと着信パケットで異なる。
- テキスト認証文字列がデバイスと着信パケットで異なる。

ISSU-GLBP

GLBP はインサービス ソフトウェア アップグレード（ISSU）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ルート プロセッサ（RP）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 Release 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、『*Cisco IOS High Availability Configuration Guide*』の「*Cisco IOS In Service Software Upgrade Process*」を参照してください。

7600 シリーズ デバイスでの ISSU の詳細については、『*ISSU and eFSU on Cisco 7600 Series Routers*』を参照してください。

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、デバイスがセカンダリ ルータ プロセッサ（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。

SSO を認識せずに RP が冗長化されたデバイスに 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、デバイスの GLBP グループ メンバとしてのアクティビティは破棄され、デバイス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 内で引き続きデバイス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 **noglbpsso** コマンドを使用します。

詳細については、『*Cisco IOS High Availability Configuration Guide*』の「*Stateful Swithover*」のマニュアル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デバイスで共有するように GLBP を設定できるため、利用可能なデバイス間でより公平にトラフィックの負荷を共有できます。

複数の仮想デバイス

GLBP では、デバイスの各物理インターフェイス上に最大 1024 台の仮想デバイス（GLBP グループ）とグループごとに最大 4 つの仮想フォワーダがサポートされます。

プリエンプション

GLBP の冗長性スキームにより、使用可能になっているプライオリティの高いバックアップ仮想ゲートウェイをアクティブ仮想ゲートウェイ（AVG）にすることができます。フォワーダ プリエンプションも同じように機能しますが、フォワーダ プリエンプションはプライオリティの代わりに重み付けを使用し、デフォルトでイネーブルになっている点が異なります。

認証

GLBP は、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の業界標準のメッセージ ダイジェスト 5（MD5）アルゴリズムをサポートしています。GLBP グループ内のデバイスの認証文字列が他のデバイスとは異なる場合、そのデバイスは他のグループ メンバによって無視されます。GLBP グループ メンバ間で簡単なテキスト パスワード認証方式を使用して、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、設定と動作を確認するには、次の作業を実行します。GLBP は、簡単に設定できる設計になっています。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。その他のすべての必須パラメータは学習できます。

はじめる前に

インターフェイスで VLAN が使用されている場合、GLBP グループ番号は VLAN ごとに異なる値にする必要があります。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **interface***typenumber*
4. **ipaddress***ip-addressmask* [**secondary**]
5. **glbp***group***ip** [*ip-address* [**secondary**]]
6. **exit**
7. **showglbp** [*interface-typeinterface-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	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# 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***typenumber* 例：	インターフェイスの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	**ipaddress***ip-addressmask* [**secondary**] 例： `Device(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。

	コマンドまたはアクション	目的
ステップ 5	**glbp***group***ip** [*ip-address* [**secondary**]] 例： `Device(config-if)# glbp 10 ip 10.21.8.10`	インターフェイス上で GLBP を設定し、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 アドレスの指定後は、**secondary** キーワードを指定して **glbp***group***ip** コマンドを再び使用し、このグループでサポートする他の IP アドレスを指定できます。
ステップ 6	**exit** 例： `Device(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、デバイスをグローバル コンフィギュレーション モードに戻します。
ステップ 7	**showglbp** [*interface-typeinterface-number*] [*group*] [*state*] [**brief**] 例： `Device(config)# show glbp 10`	（任意）デバイス上の 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 行表示されます。

例

次に、デバイス上の GLBP グループ 10 のステータスに関する出力例を示します。

```
Device# show glbp 10

GigabitEthernet0/0/0 - 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 600 sec, forwarder time-out 7200 sec
  Authentication text "stringabc"
  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 動作のカスタマイズは任意です。GLBP グループをイネーブルにすると、そのグループはすぐに動作します。GLBP グループをイネーブルにしてから GLBP をカスタマイズすると、機能のカスタマイズを完了する前にデバイスがグループの制御を引き継ぎ、AVG になる可能性があります。したがって、GLBP をカスタマイズする場合は、GLBP をイネーブルにする前に行うことを推奨します。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **interface***typenumber*
4. **ipaddress***ip-addressmask* [**secondary**]
5. **glbp***group***timers** [**msec**] *hellotime* [**msec**] *holdtime*
6. **glbp***group***timersredirect***redirecttimeout*
7. **glbp***group***load-balancing** [**host-dependent** | **round-robin** | **weighted**]
8. **glbp***group***priority***level*
9. **glbp***group***preempt** [**delayminimum***seconds*]
10. **glbp***group***client-cachemaximum***number* [**timeout***minutes*]
11. **glbp***group***name***redundancy-name*
12. **exit**
13. **noglbpsso**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# 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***typenumber* 例： `Device(config)# interface fastethernet 0/0`	インターフェイスの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	**ipaddress***ip-addressmask* [**secondary**] 例： `Device(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： `Device(config-if)# glbp 10 timers 5 18`	GLBP グループ内の AVG によって連続的に送信される hello パケットの間隔を設定します。 • *holdtime* 引数には、hello パケット内の仮想ゲートウェイと仮想フォワーダの情報が無効と見なされるまでの時間を秒数で指定します。 • オプションの **msec** キーワードは、そのあとに続く引数がデフォルトの秒単位ではなくミリ秒単位であることを指定します。
ステップ 6	**glbp***group***timersredirect***redirecttimeout* 例： `Device(config-if)# glbp 10 timers redirect 1800 28800`	AVG がクライアントを AVF にリダイレクトし続ける時間を設定します。デフォルトは 600 秒（10 分）です。 • *timeout* 引数には、セカンダリ仮想フォワーダが無効になるまでの時間を秒数で指定します。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ず、デバイスに障害が発生すると、新しいホストがバックアップへリダイレクトされずに、障害が発生したデバイスに引き続き割り当てられます。
ステップ 7	**glbp***group***load-balancing** [**host-dependent** | **round-robin** | **weighted**] 例： `Device(config-if)# glbp 10 load-balancing host-dependent`	GLBP AVG で使用するロードバランシングの方式を指定します。

	コマンドまたはアクション	目的
ステップ 8	**glbp***group***priority***level* 例： `Device(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** [**delayminimum***seconds*] 例： `Device(config-if)# glbp 10 preempt delay minimum 60`	デバイスのプライオリティが現在の AVG よりも高い場合に、GLBP グループの AVG として処理を引き継ぐようにルータを設定します。 • 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。 • AVG の交替が行われるまでの最小遅延インターバルを秒数で指定するには、オプションの **delay** キーワードおよび **minimum** キーワードおよび *seconds* 引数を指定します。
ステップ 10	**glbp***group***client-cachemaximum***number* [**timeout***minutes*] 例： `Device(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 ネットワークには、予測されるエンド ホストの Address Resolution Protocol（ARP）キャッシュの最大タイムアウト値よりも若干長いGLBPクライアントキャッシュの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： `Device(config-if)# glbp 10 name abc123`	GLBP グループに名前を割り当てることによって、IP 冗長性をイネーブルにします。 • 冗長クライアントと GLBP グループを接続できるように、GLBP 冗長クライアントに同じ GLBP グループ名を設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 12	**exit** 例： `Device(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、デバイスをグローバル コンフィギュレーション モードに戻します。
ステップ 13	**noglbpsso** 例： `Device(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. イネーブル化
2. **configureterminal**
3. **interface***typenumber*
4. **ipaddress***ip-addressmask* [**secondary**]
5. **glbp***group-number***authenticationmd5key-string** [**0** | **7**] *key*
6. **glbp***group-number***ip** [*ip-address* [**secondary**]]
7. 通信する各デバイスに対してステップ 1 ～ 6 を繰り返します。
8. **end**
9. **showglbp**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# 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***typenumber* 例： `Device(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	**ipaddress***ip-addressmask* [**secondary**] 例： `Device(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***authenticationmd5key-string** [**0** | **7**] *key* 例： `Device(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 文字の長さを超えることはできません。 • *key* 引数にはプレフィッ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、キーは暗号化されます。**servicepassword-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場合、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： `Device(config-if)# glbp 1 ip 10.0.0.10`	インターフェイス上でGLBPを設定し、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	通信する各デバイスに対してステップ 1 ～ 6 を繰り返します。	—
ステップ 8	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 9	**showglbp** 例： `Device# show glbp`	（任意）GLBP の情報を表示します。 • このコマンドを使用して、設定を確認します。設定されている場合はキーストリングと認証タイプが表示されます。

キー チェーンを使用した GLBP MD5 認証の設定

キー チェーンを使用した GLBP MD5 認証を設定するには、次の作業を実行します。キー チェーンを使用すると、キー チェーン設定に従って異なる時点で異なるキー ストリングを使用できます。GLBP は、適切なキー チェーンを照会して、指定されたキー チェーンの現在アクティブなキーとキー ID を取得します。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **keychain***name-of-chain*
4. **key***key-id*
5. **key-string***string*
6. **exit**
7. **exit**
8. **interface***typenumber*
9. **ipaddress***ip-addressmask* [**secondary**]
10. **glbp***group-number***authenticationmd5key-chain***name-of-chain*
11. **glbp***group-number***ip** [*ip-address* [**secondary**]]
12. 通信する各デバイスに対してステップ 1 ～ 10 を繰り返します。
13. **end**
14. **showglbp**
15. **showkeychain**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# 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	**keychain***name-of-chain* 例： `Device(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、キー チェーン キー 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	**key***key-id* 例： `Device(config-keychain)# key 100`	キー チェーンの認証キーを識別します。 • *key-id* 引数の値には数値を指定する必要があります。
ステップ 5	**key-string***string* 例： `Device(config-keychain-key)# key-string abc123`	キーの認証文字列を指定し、キー チェーン キー コンフィギュレーション モードを開始します。 • *string* 引数の値は、1 ～ 80 文字の大文字または小文字の英数字を指定できます。最初の文字には数字を使用できません。
ステップ 6	**exit** 例： `Device(config-keychain-key)# exit`	キー チェーン キー 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： `Device(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***typenumber* 例： `Device(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	**ipaddress***ip-addressmask* [**secondary**] 例： `Device(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。

	コマンドまたはアクション	目的
ステップ 10	**glbp***group-number***authenticationmd5key-chain***name-of-chain* 例： `Device(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 で指定した名前に一致する必要があります。
ステップ 11	**glbp***group-number***ip** [*ip-address* [**secondary**]] 例： `Device(config-if)# glbp 1 ip 10.21.0.12`	インターフェイス上で GLBP を設定し、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	通信する各デバイスに対してステップ 1 ～ 10 を繰り返します。	—
ステップ 13	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 14	**showglbp** 例： `Device# show glbp`	（任意）GLBP の情報を表示します。 • このコマンドを使用して、設定を確認します。設定されている場合はキーチェーンと認証タイプが表示されます。
ステップ 15	**showkeychain** 例： `Device# 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

テキスト認証は最小限のセキュリティを提供します。セキュリティが必須の場合は、MD5 認証を使用してください。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **interface***typenumber*
4. **ipaddress***ip-addressmask* [**secondary**]
5. **glbp***group-number***authenticationtext***string*
6. **glbp***group-number***ip** [*ip-address* [**secondary**]]
7. 通信する各デバイスに対してステップ 1 ～ 6 を繰り返します。
8. **end**
9. **showglbp**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# 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***typenumber* 例： `Device(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	**ipaddress***ip-addressmask* [**secondary**] 例： `Device(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***authenticationtext***string* 例： `Device(config-if)# glbp 10 authentication text stringxyz`	グループ内の他のデバイスから受信したGLBPパケットを認証します。 • 認証を設定する場合は、GLBP グループ内のすべてのデバイスで同じ認証文字列を使用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 6	**glbp***group-number***ip** [*ip-address* [**secondary**]] 例： `Device(config-if)# glbp 1 ip 10.0.0.10`	インターフェイス上で GLBP を設定し、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	通信する各デバイスに対してステップ 1 ～ 6 を繰り返します。	—
ステップ 8	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 9	**showglbp** 例： `Device# show glbp`	（任意）GLBP の情報を表示します。 • このコマンドを使用して、設定を確認します。

GLBP の重み付けの値とオブジェクト トラッキング

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。重み付けの初期値を設定したり、オプションのしきい値を指定したりできます。インターフェイスの状態を追跡し、インターフェイスがダウンした場合に重み付けの値を減らすための減少値を設定できます。GLBP グループの重み付けが指定の値を下回ると、グループはアクティブ仮想フォワーダでなくなります。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. イネーブル化
2. **configureterminal**
3. **track***object-number***interface***typenumber* {**line-protocol** | **iprouting**}
4. **exit**
5. **interface***typenumber*
6. **glbp***group***weighting***maximum* [**lower***lower*] [**upper***upper*]
7. **glbp***group***weightingtrack***object-number* [**decrement***value*]
8. **glbp***group***forwarderpreempt** [**delayminimum***seconds*]
9. **exit**
10. **showtrack** [*object-number* | **brief**] [**interface** [**brief**] | **iproute** [**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	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# 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***typenumber* {**line-protocol** | **iprouting**} 例： `Device(config)# track 2 interface POS 6/0/0 ip routing`	GLBP ゲートウェイの重み付けに影響する状態変化を追跡するインターフェイスを設定し、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。 • このコマンドは、**glbpweightingtrack** コマンドで使用されるインターフェイスと対応するオブジェクトの数を設定します。 • **line-protocol** キーワードを指定すると、インターフェイスがアップ状態かどうかが追跡されます。**iprouting** 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であり、IP アドレスが設定されているかどうかもチェックされます。
ステップ 4	**exit** 例： `Device(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	**interface***typenumber* 例： `Device(config)# interface GigabitEthernet 0/0/0`	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： `Device(config-if)# glbp 10 weighting 110 lower 95 upper 105`	GLBP ゲートウェイの重み付けの初期値、上限しきい値、および下限しきい値を指定します。

	コマンドまたはアクション	目的
ステップ 7	**glbp***group***weightingtrack***object-number* [**decrement***value*] 例： `Device(config-if)# glbp 10 weighting track 2 decrement 5`	GLBP ゲートウェイの重み付けに影響する、追跡対象のオブジェクトを指定します。 • *value* 引数には、追跡対象のオブジェクトで障害が発生した場合に GLBP ゲートウェイの重み付けを減らす量を指定します。
ステップ 8	**glbp***group***forwarderpreempt** [**delayminimum***seconds*] 例： `Device(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デバイスを設定します。 • このコマンドは、デフォルトでイネーブルになっており、遅延は 30 秒です。 • AVF の交替が行われるまでの最小遅延インターバルを秒数で指定するには、オプションの **delay** キーワードおよび **minimum** キーワードおよび *seconds* 引数を指定します。
ステップ 9	**exit** 例： `Device(config-if)# exit`	特権 EXEC モードに戻ります。
ステップ 10	**showtrack** [*object-number* | **brief**] [**interface** [**brief**] | **iproute** [**brief**] | **resolution** | **timers**] 例： `Device# 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 動作に関する各種イベントに関連する診断出力を可視化する 5 つの特権 EXEC モード コマンドが導入されています。**debugconditionglbp**、**debugglbperrors**、**debugglbpevents**、**debugglbppackets**、**debugglbpterse** の各コマンドは、トラブルシューティング専用です。これはソフトウェアによって生成される出力のボリュームが、デバイスの深刻なパフォーマンスの低下を引き起こす可能性があるためです。**debugglbp** コマンドを使用した場合の影響を最小限に抑えるには、次の作業を実行します。

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、**debugconditionglbp** コマンドまたは **debugglbp** コマンドを使用することでデバイスにかかる負荷が最小限に抑えられます。直接コンソールに接続できない場合は、ターミナル サーバを介して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デバイス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。

はじめる前に

この作業では、コンソールに直接接続された GLBP を実行しているデバイスが必要です。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **nologgingconsole**
4. Telnet を使用してデバイス ポートにアクセスし、ステップ 1 と 2 を繰り返します。
5. **end**
6. **terminalmonitor**
7. **debugconditionglbp***interface-typeinterface-numbergroup* [*forwarder*]
8. **terminalnomonitor**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# 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	**nologgingconsole** 例： `Device(config)# no logging console`	コンソール端末へのすべてのロギングをディセーブルにします。 • コンソールへのロギングを再度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 **loggingconsole** 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 を使用してデバイス ポートにアクセスし、ステップ 1 と 2 を繰り返します。	再帰 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ます。
ステップ 5	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**terminalmonitor** 例： `Device# 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	**debugconditionglbp***interface-typeinterface-numbergroup* [*forwarder*] 例： `Device# debug condition glbp GigabitEthernet0/0/0 1`	GLBP 状態に関するデバッグ メッセージを表示します。 • 特定の **debugconditionglbp** または **debugglbp** コマンドだけを入力して、出力を特定のサブコンポーネントに分離し、プロセッサの負荷を最小限に抑えます。適切な引数とキーワードを使用して、指定したサブコンポーネント上に詳細なデバッグ情報を生成します。 • 終了したら、特定の **nodebugconditionglbp** または **nodebugglbp** コマンドを入力します。
ステップ 8	**terminalnomonitor** 例： `Device# terminal no monitor`	仮想端末でのロギング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

```
Device(config)# interface fastethernet 0/0
Device(config-if)# ip address 10.21.8.32 255.255.255.0
```

```
Device(config-if)# glbp 10 timers 5 18
Device(config-if)# glbp 10 timers redirect 1800 28800
Device(config-if)# glbp 10 load-balancing host-dependent
Device(config-if)# glbp 10 priority 254
Device(config-if)# glbp 10 preempt delay minimum 60

Device(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。

```
Device(config)# interface Ethernet 0/1
Device(config-if)# ip address 10.0.0.1 255.255.255.0
Device(config-if)# glbp 2 authentication md5 key-string ThisStringIsTheSecretKey
Device(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

次に、GLBP がキー チェーン「AuthenticateGLBP」を照会して、指定されたキー チェーンの現在アクティブなキーとキー ID を取得する例を示します。

```
Device(config)# key chain AuthenticateGLBP
Device(config-keychain)# key 1
Device(config-keychain-key)# key-string ThisIsASecretKey
Device(config-keychain-key)# exit
Device(config-keychain)# exit
Device(config)# interface Ethernet 0/1
Device(config-if)# ip address 10.0.0.1 255.255.255.0
Device(config-if)# glbp 2 authentication md5 key-chain AuthenticateGLBP
Device(config-if)# glbp 2 ip 10.0.0.10
```

例：GLBP テキスト認証の設定

```
Device(config)# interface GigabitEthernet 0/0/0
Device(config-if)# ip address 10.21.8.32 255.255.255.0
Device(config-if)# glbp 10 authentication text stringxyz
Device(config-if)# glbp 10 ip 10.21.8.10
```

例：GLBP 重み付けの設定

次に、デバイスを POS インターフェイス 5/0/0 と 6/0/0 の IP ルーティング状態を追跡するように設定し、GLBP の重み付けの初期値、上限しきい値、下限しきい値、および重み付けの減少値 10 を設定する例を示します。POS インターフェイス 5/0/0 と 6/0/0 がダウンすると、デバイスの重み付けの値が小さくなります。

```
Device(config)# track 1 interface POS 5/0/0 ip routing
Device(config)# track 2 interface POS 6/0/0 ip routing
Device(config)# interface fastethernet 0/0/0
Device(config-if)# glbp 10 weighting 110 lower 95 upper 105
Device(config-if)# glbp 10 weighting track 1 decrement 10
```

```
Device(config-if)# glbp 10 weighting track 2 decrement 10
Device(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、デバイスは 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。

```
Device(config)# interface GigabitEthernet 0/0/0
Device(config-if)# ip address 10.21.8.32 255.255.255.0
Device(config-if)# glbp 10 ip 10.21.8.10
```

GLBP に関する追加情報

関連資料

関連項目	マニュアル タイトル
GLBP 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、使用上のガイドライン、および例	『Cisco IOS IP Application Services Command Reference』
インサービス ソフトウェア アップグレード（ISSU）の設定	『*Cisco IOS High Availability Configuration Guide*』の「In Service Software Upgrade Process」のモジュール
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 Protocol-Independent Command Reference*』
オブジェクト トラッキング	「Configuring Enhanced Object Tracking」のモジュール
『Stateful Switchover』	『*Cisco IOS High Availability Configuration Guide*』の「Stateful Switchover」のモジュール
VRRP	「Configuring VRRP」のモジュール
HSRP	「Configuring HSRP」のモジュール
GLBP の IPv6 サポート	「FHRP - GLBP Support for IPv6」のモジュール

シスコのテクニカル サポート

説明	Link
★枠で囲まれた Technical Assistance の場合★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。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。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

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *1*：*GLBP* の機能情報

機能名	リリース	機能の設定情報
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。 次のコマンドは、この機能によって導入または修正されました。**glbpforwarderpreempt**、**glbpip**、**glbpload-balancing**、**glbpname**、**glbppreempt**、**glbppriority**、**glbpsso**、**glbptimers**、**glbptimersredirect**、**glbpweighting**、**glbpweightingtrack**、**showglbp**
GLBP MD5 認証		MD5 認証を使用すると、別のプレーン テキスト認証方式よりもセキュリティを強化できます。MD5 認証では、各 GLBP グループ メンバが秘密キーを使用して、発信パケットに含まれるキー付き 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、着信パケット内のハッシュが生成されたハッシュに一致しない場合、そのパケットは無視されます。 **glbpauthentication** および **showglbp** の各コマンドがこの機能により変更されました。

機能名	リリース	機能の設定情報
ISSU と GLBP		GLBP はインサービス ソフトウェア アップグレード（ISSU）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ルートプロセッサ（RP）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。 この機能により、新規追加または変更されたコマンドはありません。

機能名	リリース	機能の設定情報
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。 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。 **debugglbpevents**、**glbpsso**、**showglbp** 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

アクティブ RP：ルート プロセッサ（RP）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。

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）。アクティブ バーチャル ゲートウェイとして選択され、プロトコルの動作を担当する、GLBP グループ内の 1 つのバーチャル 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。

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。

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 XE 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、計画的なソフトウェア 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、パケット転送中にソフトウェアを変更できるため、ネットワークのアベイラビリティが向上し、計画的なソフトウェア 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：ルート プロセッサ。シャーシに搭載される、集中化されたコントロール ユニットの総称です。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。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。

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。

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。

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。

第 3 章

HSRP for IPv6。

IPv6 ルーティング プロトコルは、デバイス間の復元力とフェールオーバーを提供します。ただし、ホストとファーストホップデバイス間のパスで障害が発生した場合、またはファーストホップ デバイスで障害が発生した場合は、First Hop Redundancy Protocol（FHRP）によってホストとデバイス間の復元力とフェールオーバーが確保されます。

ホットスタンバイルータプロトコル（HSRP）は、ゲートウェイで障害が発生した場合にデータトラフィックを保護します。

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。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

HSRP for IPv6 の前提条件

HSRP for IPv6 を設定する前に、インターフェイスに対して HSRP バージョン 2 をイネーブルにする必要があります。

HSRP for IPv6 について

HSRP for IPv6 の概要

HSRP は、ファーストホップ IP デバイスの透過的なフェールオーバーを可能にする FHRP です。デフォルト ゲートウェイの IP アドレスが設定されたイーサネット上の IP ホストにファーストホップのルーティング冗長性を確保することによって、高いネットワーク アベイラビリティを提供します。HSRP は、アクティブ デバイスおよびスタンバイ デバイスを選択するためデバイス グループで使用されます。デバイスインターフェイスのグループでは、アクティブデバイスは、パケットをルーティングするために選択されるデバイスです。スタンバイデバイスはアクティブデバイスで障害が生じるか、事前設定された条件が満たされた場合にそのロールを引き継ぐデバイスです。

IPv6 ホストは、IPv6 ネイバー探索の RA メッセージを通じて使用可能な IPv6 デバイスを学習します。これらのメッセージは定期的にマルチキャストされるか、またはホストによって請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 ホップだけを提供するように設計されています。

HSRP IPv6 グループには、HSRP グループ番号に基づく仮想 MAC アドレスと、デフォルトでは HSRP 仮想 MAC アドレスに基づく仮想 IPv6 リンクローカル アドレスが割り当てられます。HSRP グループがアクティブな場合、定期的な RA が HSRP 仮想 IPv6 リンクローカル アドレス宛てに送信されます。これらの RA は、グループがアクティブ状態ではなくなるときに最後の RA が送信されると停止します。

インターフェイスのリンクローカル アドレスに対する定期的な RA は、少なくとも 1 つの仮想 IPv6 リンクローカル アドレスがインターフェイスに設定されているときに最後の RA が送信されると停止します。インターフェイスの IPv6 リンクローカル アドレスには、RA について説明したこと以外に制約事項はありません。他のプロトコルは、このアドレスへのパケットを送受信し続けます。

HSRP では、プライオリティ メカニズムを使用して、デフォルトのアクティブ デバイスにする HSRP 設定済みデバイスを決定します。デバイスをアクティブ デバイスとして設定するには、他のすべての HSRP 設定済みデバイスのプライオリティよりも高いプライオリティをそのデバイスに割り当てます。デフォルトのプライオリティは 100 です。したがって、100 よりも高いプライオリティを持つデバイスを 1 つだけ設定した場合、そのデバイスがデフォルトのアクティブ デバイスになります。

HSRP IPv6 仮想 MAC アドレスの範囲

HSRP IPv6 では、次に示すように、HSRP for IP とは異なる仮想 MAC アドレス ブロックを使用します。

0005.73A0.0000 through 0005.73A0.0FFF（4096 のアドレス）

HSRP IPv6 UDP ポート番号

HSRP IPv6 には、ポート番号 2029 が割り当てられています。

HSRP for IPv6 をイネーブルにする方法

IPv6 用 HSRP グループの動作のイネーブル化

HSRP IPv6 を設定する前に、インターフェイスに対して HSRP バージョン 2 をイネーブルにする必要があります。

HSRP バージョン 2 のイネーブル化

手順の概要

1. イネーブル化
2. **configureterminal**
3. **interface***typenumber*
4. **standbyversion** {**1** | **2**}

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# 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***typenumber* 例： `Device(config)# interface GigabitEthernet 0/0/0`	インターフェイスのタイプと番号を指定し、デバイスをインターフェイス コンフィギュレーション モードにします。
ステップ 4	**standbyversion** {**1** | **2**} 例： `Device(config-if)# standby version 2`	HSRP のバージョンを変更します。 • デフォルトはバージョン 1 です。

IPv6 用 HSRP グループの動作のイネーブル化と確認

この作業では、**standbyipv6** コマンドを入力すると、リンクローカル プレフィクスからリンクローカル アドレスが生成され、変更後の EUI-64 形式のインターフェイス識別子が生成されます。EUI-64 インターフェイス識別子は、関連する HSRP 仮想 MAC アドレスからこの形式で作成されます。

リンクローカル アドレスは、リンクローカル プレフィックス FE80::/10（1111 1110 10）と変更された EUI-64 形式のインターフェイス識別子を使用するすべてのインターフェイスを自動的に設定できる IPv6 ユニキャスト アドレスです。リンクローカル アドレスは、ステートレス自動設定プロセスで使用されます。ローカルリンク上のノードは、リンクローカルアドレスを使用して通信できます。ノードの通信にサイトローカル アドレスまたはグローバルに一意のアドレスは不要です。

IPv6 では、リンク上のデバイスが RA メッセージでサイトローカル プレフィックスやグローバル プレフィックス、およびリンクのデフォルト デバイスとして動作することをアドバタイズします。RA メッセージは、定期的に送信される場合と、システム始動時にホストから送信されるルータ送信要求メッセージに対する応答として送信される場合があります。

リンク上のノードは、RA メッセージに含まれるプレフィックス（64 ビット）にそのインターフェイス ID（64 ビット）を付加して、自動的にサイトローカル アドレスとグローバル IPv6 アドレスを設定できます。ノードによって設定された 128 ビットの IPv6 アドレスは、重複アドレス検出の対象となり、リンク上での一意性が確保されます。RA メッセージでアドバタイズされたプレフィックスがグローバルに一意である場合、ノードによって設定された IPv6 アドレスもグローバルに一意になります。ICMP パケット ヘッダーのタイプ フィールドの値が 133 であるルータ送信要求メッセージは、システム始動時にホストによって送信されるため、ホストは次のスケジュールされた RA メッセージを待機することなくすぐに自動設定できます。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **ipv6unicast-routing**
4. **interface***typenumber*
5. **standby** [*group-number*] **ipv6** {*link-local-address* | **autoconfig**}
6. **standby** [*group-number*] **preempt** [**delayminimum***seconds* | **reload***seconds* | **sync***seconds*]
7. **standby** [*group-number*] **priority***priority*
8. **exit**
9. **showstandby** [*typenumber* [*group*]] [**all** | **brief**]
10. **showipv6interface** [**brief**] [*interface-typeinterface-number*] [**prefix**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# 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	**ipv6unicast-routing** 例： `Device(config)# ipv6 unicast-routing`	IPv6ユニキャストデータグラムの転送をイネーブルにします。 • HSRP for IPv6 を機能させるには、**ipv6unicast-routing** コマンドをイネーブルにする必要があります。
ステップ 4	**interface***typenumber* 例： `Device(config)# interface GigabitEthernet 0/0/0`	インターフェイスのタイプと番号を指定し、デバイスをインターフェイス コンフィギュレーション モードにします。
ステップ 5	**standby** [*group-number*] **ipv6** {*link-local-address* | **autoconfig**}	IPv6 の HSRP をアクティブにします。

	コマンドまたはアクション	目的
	例： `Device(config-if)# standby 1 ipv6 autoconfig`	
ステップ 6	**standby** [*group-number*] **preempt** [**delayminimum***seconds* | **reload***seconds* | **sync***seconds*] 例： `Device(config-if)# standby 1 preempt`	HSRP 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。
ステップ 7	**standby** [*group-number*] **priority***priority* 例： `Device(config-if)# standby 1 priority 110`	HSRP プライオリティを設定します。
ステップ 8	**exit** 例： `Device(config-if)# exit`	デバイスを特権 EXEC モードに戻します。
ステップ 9	**showstandby** [*typenumber* [*group*]] [**all** | **brief**] 例： `Device# show standby`	HSRP 情報を表示します。
ステップ 10	**showipv6interface** [**brief**] [*interface-typeinterface-number*] [**prefix**] 例： `Device# show ipv6 interface GigabitEthernet 0/0/0`	IPv6 向けに設定されたインターフェイスの使用状況を表示します。

HSRP for IPv6 の設定例

例：HSRP グループの設定と確認

次に、デバイス 1 とデバイス 2 で構成される IPv6 用 HSRP グループの設定および確認の例を示します。デバイスの設定を確認するために、各デバイスに対して **show standby** コマンドが発行されています。

デバイス 1 の設定

```
interface FastEthernet0/0.100
description DATA VLAN for PCs
encapsulation dot1Q 100
ipv6 address 2001:DB8:CAFE:2100::BAD1:1010/64
standby version 2
standby 101 priority 120
standby 101 preempt delay minimum 30
standby 101 authentication ese
standby 101 track Serial0/1/0.17 90
standby 201 ipv6 autoconfig
standby 201 priority 120
standby 201 preempt delay minimum 30
standby 201 authentication ese
standby 201 track Serial0/1/0.17 90
Device1# show standby
FastEthernet0/0.100 - Group 101 (version 2)
State is Active
2 state changes, last state change 5w5d
Active virtual MAC address is 0000.0c9f.f065
Local virtual MAC address is 0000.0c9f.f065 (v2 default)
Hello time 3 sec, hold time 10 sec
Next hello sent in 2.296 secs
Authentication text "ese"
Preemption enabled, delay min 30 secs
Active router is local
Priority 120 (configured 120)
Track interface Serial0/1/0.17 state Up decrement 90
IP redundancy name is "hsrp-Fa0/0.100-101" (default)
FastEthernet0/0.100 - Group 201 (version 2)
State is Active
2 state changes, last state change 5w5d
Virtual IP address is FE80::5:73FF:FEA0:C9
Active virtual MAC address is 0005.73a0.00c9
Local virtual MAC address is 0005.73a0.00c9 (v2 IPv6 default)
Hello time 3 sec, hold time 10 sec
Next hello sent in 2.428 secs
Authentication text "ese"
Preemption enabled, delay min 30 secs
Active router is local
Standby router is FE80::20F:8FFF:FE37:3B70, priority 100 (expires in 7.856 sec)
Priority 120 (configured 120)
Track interface Serial0/1/0.17 state Up decrement 90
IP redundancy name is "hsrp-Fa0/0.100-201" (default)
```

デバイス 2 の設定

```
interface FastEthernet0/0.100
description DATA VLAN for Computers
encapsulation dot1Q 100
ipv6 address 2001:DB8:CAFE:2100::BAD1:1020/64
standby version 2
standby 101 preempt
standby 101 authentication ese
standby 201 ipv6 autoconfig
standby 201 preempt
```

```
standby 201 authentication ese
Device2# show standby
FastEthernet0/0.100 - Group 101 (version 2)
State is Standby
7 state changes, last state change 5w5d
Active virtual MAC address is 0000.0c9f.f065
Local virtual MAC address is 0000.0c9f.f065 (v2 default)
Hello time 3 sec, hold time 10 sec
Next hello sent in 0.936 secs
Authentication text "ese"
Preemption enabled
MAC address is 0012.7fc6.8f0c
Standby router is local
Priority 100 (default 100)
IP redundancy name is "hsrp-Fa0/0.100-101" (default)
FastEthernet0/0.100 - Group 201 (version 2)
State is Standby
7 state changes, last state change 5w5d
Virtual IP address is FE80::5:73FF:FEA0:C9
Active virtual MAC address is 0005.73a0.00c9
Local virtual MAC address is 0005.73a0.00c9 (v2 IPv6 default)
Hello time 3 sec, hold time 10 sec
Next hello sent in 0.936 secs
Authentication text "ese"
Preemption enabled
Active router is FE80::212:7FFF:FEC6:8F0C, priority 120 (expires in 7.548 sec)
MAC address is 0012.7fc6.8f0c
Standby router is local
Priority 100 (default 100)
IP redundancy name is "hsrp-Fa0/0.100-201" (default)
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
VRRP コマンド	『*Cisco IOS IP Application Services Command Reference*』
オブジェクト トラッキング	拡張オブジェクト トラッキングの設定
ホット スタンバイ ルーティング プロトコル（HSRP）	『Configuring HSRP』
In Service Software Upgrade（ISSU）	『*High Availability Configuration Guide*』の「In Service Software Upgrade Process」
ゲートウェイ ロード バランシング プロトコル（GLBP）	『Configuring GLBP』
『Stateful Switchover』	『*High Availability Configuration Guide*』の「Stateful Switchover」のセクション

標準

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

MIB

MIB	MIB のリンク
VRRP MIB	選択したプラットフォーム、Cisco 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場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	Title
RFC 2338	『Virtual Router Redundancy Protocol』
RFC 2787	Virtual Router Redundancy Protocol の管理対象オブジェクトの定義
RFC 3768	仮想ルータ冗長プロトコル（VRRP）

シスコのテクニカル サポート

説明	Link
★枠で囲まれた Technical Assistance の場合★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。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。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 for IPv6 の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *2*：***HSRP for IPv6*** の機能情報

機能名	リリース	機能情報
HSRP for IPv6。	Cisco IOS XE Release 3.1S Cisco IOS XE Release 3.9S	HSRP は、ファーストホップ IPv6 ルータの透過的なフェールオーバーを可能にする FHRP です。 **show standby**、**standby ipv6**、**standby preempt**、**standby priority** の各コマンドが導入または修正されました。
VRF インターフェイスでの ISSU - HSRPv6	Cisco IOS XE Release 3.1S	この機能は、Cisco IOS XE Release 3.1S でサポートされます。
VRF インターフェイスでの NSF/SSO - HSRPv6	Cisco IOS XE Release 3.1S	この機能は、Cisco IOS XE Release 3.1S でサポートされます。

用語集

- **CPE**：Customer Premises Equipment（加入者宅内機器）
- **FHRP**：First Hop Redundancy Protocol（FHRP）
- **GLBP**：ゲートウェイ ロード バランシング プロトコル（GLBP）
- **HSRP**：Hot Standby Routing Protocol（HSRP）
- **NA**：ネイバー アドバタイズメント（NA）
- **ND**：ネイバー探索（ND）

- **NS**：ネイバー請求（NS）
- **PE**：Provider Equipment（PE）
- **RA**--ルータ アドバタイズメント
- **RS**--ルータ請求（RS）

第 4 章

『Configuring HSRP』

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 デバイス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ファーストホップ冗長プロトコル（FHRP）です。デフォルト ゲートウェイの IP アドレスが設定されたネットワーク上の IP ホストにファーストホップのルーティング冗長性を確保することによって、高いネットワーク アベイラビリティを提供します。HSRP は、アクティブ デバイスおよびスタンバイ デバイスを選択するためルータ グループで使用されます。デバイスインターフェイスのグループでは、アクティブデバイスは、パケットをルーティングするために選択されるデバイスです。スタンバイ デバイスはアクティブ デバイスで障害が生じるか、事前設定された条件が満たされた場合にそのロールを引き継ぐデバイスです。

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。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

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 ブロードキャスト対応イーサネット LAN で使用するために設計されています。HSRP 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。

HSRP について

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ている単一のデバイスの IP アドレスがあります。HSRP を使用すると、デバイスの 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、ディスカバリ プロトコル（ICMP Router Discovery Protocol [IRDP] など）をサポートしないホスト、および選択したデバイスがリロードしたときやデバイスの電源が失われたときに新しいデバイスに切り替えることができないホストに便利です。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 をネットワーク セグメントに設定すると、HSRP が動作するデバイスのグループ間で仮想 MAC アドレスと IP アドレスを共有できるようになります。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。このようなデバイスの 1 つが、アクティブ デバイスとしてプロトコルによって選択されます。アクティブ デバイスは、グループの MAC アドレス宛のパケットを受信してルーティングします。*n* 台のデバイスで HSRP が稼動している場合、*n*+ 1 個の IP アドレスおよび MAC アドレスが割り当てられます。

指定されたアクティブ デバイスの障害を HSRP が検出すると、選択されているスタンバイ デバイスがホット 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。この時点で新しいスタンバイ デバイスも選択されます。

HSRP では、プライオリティ メカニズムを使用して、デフォルトのアクティブ デバイスにする HSRP 設定済みデバイスを決定します。デバイスをアクティブ デバイスとして設定するには、他のすべての HSRP 設定済みデバイスのプライオリティよりも高いプライオリティをそのデバイスに割り当てます。デフォルトのプライオリティは 100 です。したがって、100 よりも高いプライオリティを持つデバイスを 1 つだけ設定した場合、そのデバイスがデフォルトのアクティブ デバイスになります。

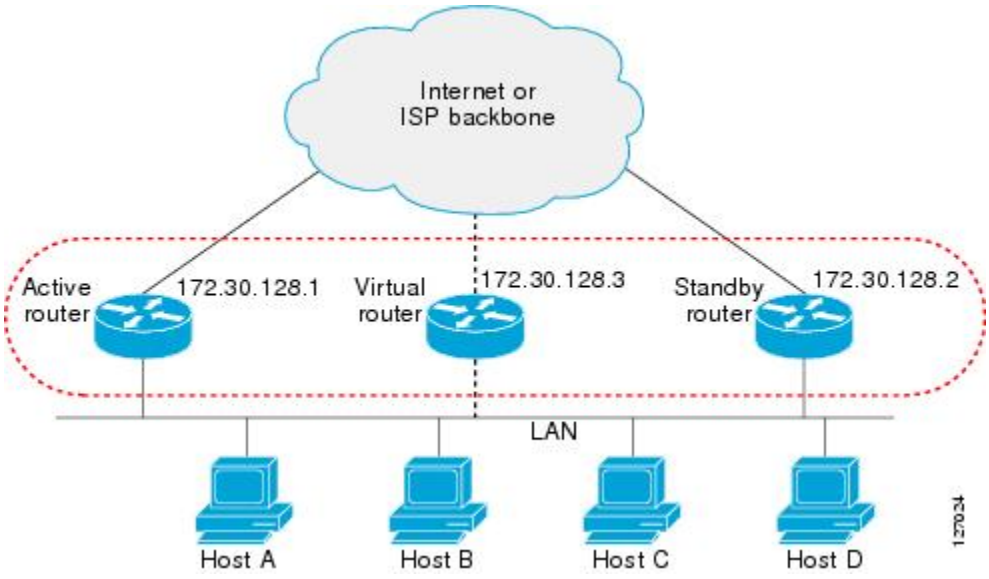
HSRP を実行しているデバイスは、UDP ベースのマルチキャスト hello メッセージを送信および受信して、デバイスの障害を検出したり、アクティブデバイスとスタンバイデバイスを割り当てた

りします。アクティブ デバイスが設定された時間内に hello メッセージを送信できなかった場合は、最高のプライオリティのスタンバイデバイスがアクティブデバイスになります。このようにパケット転送機能が別のデバイスに移行しても、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、冗長デバイスおよびロード 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。

次の図は、HSRP 用に設定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、複数台のデバイスが 1 台の仮想ルータとして機能します。仮想デバイス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デバイスの共有のデフォルト ゲートウェイになります。アクティブ デバイスの IP アドレスを使用して、LAN 上でホストを設定する必要はありません。その代わりに、仮想デバイスの 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 デバイスが hello メッセージを送信できない場合、スタンバイ デバイス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デバイスになり、アクティブデバイスの役割を引き受けます。

図 *2*：*HSRP* のトポロジ



HSRP バージョン 2 の設計

HSRP バージョン 2 は、バージョン 1 の次の制限に対応するために設計されています。

- HSRP バージョン 1 では、ミリ秒のタイマー値はアドバタイズまたは学習されませんでした。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。
- HSRP バージョン 1 では、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、アクティブな HSRP hello メッセージを使用してメッセージを送信した物理デバイスを特定できませんでした。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。
- マルチキャスト アドレス 224.0.0.2 が HSRP hello メッセージを送信するために使用されます。このアドレスは、シスコ グループ管理プロトコル（CGMP）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 では、HSRP バージョン 1 で使用されていたマルチキャスト アドレス 224.0.0.2 の代わりに、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。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広がっても、インターフェイスが多くの HSRP グループをサポートするわけではありません。グループ番号範囲が拡大することにより、グループ番号がサブインターフェイスの VLAN 番号に一致するようになりました。

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 では HSRP バージョン 1 とは異なるパケット フォーマットを使用します。パケット フォーマットは Type-Length-Value（TLV）です。HSRP バージョン 1 のデバイスが受信した 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、ゲートウェイ ロード バランシング プロトコル（GLBP）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 の同じ制限が解消されます。GLBP の詳細については、『*Configuring GLBP*』を参照してください。

ジッター タイマー

ジッター タイマーは、HSRP で使用されます。これらはリアルタイムで機能し拡張するサービスで動作するタイマーに推奨されます。ジッター タイマーは、HSRP グループ操作のバンチングの可能性を減らすことによって HSRP とその他の FHRP プロトコルの信頼性を大幅に改善し、CPU とネットワーク トラフィックのスパイクを削減することを意図しています。HSRP の場合、特定のデバイスで最大 4,000 の運用グループを構成することができます。デバイスやネットワークへの負荷を分散するために、HSRP タイマーはジッターを使用します。特定のタイマー インスタンスでは、設定した値よりも最大 20% 多くかかる場合があります。たとえば、15 秒に設定されているホールド時間の場合、実際のホールド時間は 18 秒かかることがあります。

HSRP では、Hello タイマー（Hello パケットを送信する）は負のジッターを持ち、ホールドダウン タイマー（ピア障害をチェックする）は正のジッターを持ちます。

HSRP の設定の変更

CSCsv12265 を使用すると、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 アドレスを使って HSRP グループを設定できます。

HSRP グループの仮想 IP アドレスをセカンダリ インターフェイス IP アドレスと同じネットワーク ID で設定すると、HSRP メッセージの送信元アドレスが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。この設定変更により、次の設定が可能になります。

```
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
```

CSCsv12265 以前は、HSRP 仮想 IP アドレスにプライマリ インターフェイス アドレスと同じネットワーク ID がない限り、HSRP グループは INIT ステートのままでした。

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 はファースト ホップ デバイスの透過的なフェールオーバーを提供します。

プリエンプション

プリエンプションにより、スタンバイ デバイス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 のメッセージ ダイジェスト 5（MD5）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属性

CLI を使用して、次のものにグループ属性を適用できます。

- 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デバイスが HSRP アクティブ デバイスになったとき、HSRP アクティブ デバイスがすで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。HSRP のプリエンプションが正しく機能していないように見える原因は、新しい HSRP アクティブ デバイスが現在の HSRP アクティブ デバイスから 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デバイスの決定で考慮されないためです。

HSRP は、パケットを受信するインターフェイスで遅延が発生する可能性がある一部の大規模なハードウェア プラットフォームで機能していないように見える場合があります。

通常は、すべての HSRP デバイスを次のように設定することを推奨します。

standbydelayminimum30reload60

インターフェイス コンフィギュレーション コマンド **standbydelayminimumreload** 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 プリエンプション遅延を有効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 **standbypreemptdelay** とは異なるコマンドです。

HSRP のプライオリティとプリエンプション

プリエンプションは、最もプライオリティが高い HSRP ルータをすぐにアクティブ ルータにすることができます。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。プライオリティが等しい場合、プライマリ IPアドレスが比較され、大きいIPアドレスが優先されます。どちらの場合も、値の大きい方がプライオリティが高くなります。ルータの設定で **standby preempt** インターフェイス コンフィギュレーション コマンドを使用しない場合、そのルータのプライオリティが他のルータよりも高い場合でもそのルータはアクティブ ルータになりません。

プライオリティが等しくて IP アドレスが大きいスタンバイ ルータは、アクティブ ルータをプリエンプション処理しません。

ルータが最初に起動したとき、ルータのルーティング テーブルは完全ではありません。プリエンプションを設定可能な期間遅延させることができるプリエンプション遅延を設定できます。この遅延期間により、ルータがアクティブルータになる前にルーティングテーブルを実装できるようになります。

プリエンプションが有効になっていない場合は、ルータはアクティブ ルータからのhelloメッセージを受信しないアクティブ ルータをプリエンプション処理するように見えます。

オブジェクト トラッキングが HSRP デバイスのプライオリティに及ぼす影響

デバイスがオブジェクト トラッキング対応として設定されていて、なおかつトラッキング対象のオブジェクトがダウンした場合、デバイスのプライオリティはダイナミックに変更されます。トラッキング プロセスは定期的に、トラッキング対象オブジェクトをポーリングし、値の変更を確認します。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。よりプライオリティの高いHSRPデバイスは、**standbypreempt** コマンドが設定されている場合にはアクティブなデバイスになることができます。

HSRP のアドレス指定

HSRPデバイスが互いに通信するときは、HSRPhelloパケットをやり取りします。これらのパケットは、UDP ポート 1985 上の宛先 IP マルチキャスト アドレス 224.0.0.2（すべてのデバイスと通信するための予約済みマルチキャストアドレス）に送信されます。アクティブデバイスは、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 デバイスは、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.AC*xy* 形式の仮想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 LAN セグメント上のホストは、標準のアドレス解決プロトコル（ARP）プロセスを使用して、関連付けられた MAC アドレスを解決します。

HSRP バージョン 2 では新しい 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 では、このマルチキャスト アドレスが 224.0.0.2 です。この新しいマルチキャスト アドレスにより、シスコ グループ管理プロトコル（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。

HSRP 仮想 MAC アドレスと BIA MAC アドレス

各 HSRP デバイスの仮想 MAC アドレスはデバイスで自動的に生成されます。ただし、拡張分散ネットワーク機能（APPN）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、グループの **standbymac-address** コマンドを使用して、仮想 MAC アドレスを指定します。仮想 IP アドレスは、これらのプロトコルには重要ではありません。

standbyuse-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バーンドイン 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デバイスが存在する場合に、**standbyuse-bia** コマンドを設定すると、ルーティング情報フィールド（RFI）に関する混乱を防ぐことができます。

standbyuse-bia コマンドはインターフェイス用に使用され、**standbymac-address** コマンドは、HSRP グループに使用されます。

HSRP タイマー

HSRP バージョン 1 では、非アクティブ デバイスは、ミリ秒のタイマー値が使用されていない場合、アクティブ デバイスのタイマー値を学習します。ミリ秒のタイマー値が使用されている場合は、すべてのデバイス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 パケットが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 では、タイマー値をミリ秒単位でアドバタイズするため、この制限はありません。

ジッター タイマー

ジッター タイマーは、HSRP で使用されます。これらはリアルタイムで機能し拡張するサービスで動作するタイマーに推奨されます。ジッター タイマーは、HSRP グループ操作のバンチングの可能性を減らすことによって HSRP とその他の FHRP プロトコルの信頼性を大幅に改善し、CPU とネットワーク トラフィックのスパイクを削減することを意図しています。HSRP の場合、特定のデバイスで最大 4,000 の運用グループを構成することができます。デバイスやネットワークへの負荷を分散するために、HSRP タイマーはジッターを使用します。特定のタイマー インスタンスでは、設定した値よりも最大20%多くかかる場合があります。たとえば、15秒に設定されているホールド時間の場合、実際のホールド時間は 18 秒かかることがあります。

HSRP では、Hello タイマー（Hello パケットを送信する）は負のジッターを持ち、ホールドダウンタイマー（ピア障害をチェックする）は正のジッターを持ちます。

HSRP MAC の更新間隔

HSRP が FDDI で実行されている場合、ラーニング ブリッジおよびスイッチで MAC キャッシュを更新するためにパケットが送信される間隔を変更できます。HSRP の hello パケットは、FDDI インターフェイスでは MAC 仮想アドレスではなく、バーンドイン アドレス（BIA）を使用します。更新パケットは、スイッチおよびラーニング ブリッジ上の MAC キャッシュを最新に保ちます。更新パケットは定期的な hello メッセージを送信しないため、マルチグループのスレーブとして設定された HSRP グループにも使用できます。

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 更新パケットが必要ない場合（FDDI はあるがラーニング ブリッジやスイッチがない場合）は、送信されないようにできます。

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、デバイス A のプライオリティが 120 で、これがアクティブ デバイスであるとします。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、デバイス A はアクティブ デバイスとしての動作を停止します。デバイス 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、デバイス A はアクティブ デバイスのままです。

HSRP パケットが拒否されるのは、次のいずれかの場合です。

- 認証方式がデバイスと着信パケットの間で異なっている。
- テキスト認証文字列がデバイスと着信パケットで異なる。

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 認証を使用すると、別のプレーン テキスト認証方式よりもセキュリティを強化できます。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で直接指定するか、またはキー チェーンを使用して間接的に指定できます。

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、デバイス A のプライオリティが 120 で、これがアクティブ デバイスであるとします。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、デバイス A はアクティブ デバイスとしての動作を停止します。デバイス 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、デバイス A はアクティブ デバイスのままです。

HSRP パケットが拒否されるのは、次のいずれかの場合です。

- 認証方式がデバイスと着信パケットの間で異なっている。
- MD5 ダイジェストがデバイスと着信パケットで異なる。
- テキスト認証文字列がデバイスと着信パケットで異なる。

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 ネイバー探索のルータ アドバタイズメント（RA）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。これらのメッセージは定期的にマルチキャストされるか、またはホストによって請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 ホップだけを提供するように設計されています。

HSRP IPv6 グループには、HSRP グループ番号に基づく仮想 MAC アドレスと、デフォルトでは HSRP 仮想 MAC アドレスに基づく仮想 IPv6 リンクローカル アドレスが割り当てられます。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な場合、定期的な RA が HSRP 仮想 IPv6 リンクローカル アドレス宛てに送信されます。これらの RA は、グループがアクティブ状態ではなくなるときに最後の RA が送信されると停止します。

インターフェイスのリンクローカル アドレスに対する定期的な RA は、少なくとも 1 つの仮想 IPv6 リンクローカル アドレスがインターフェイスに設定されているときに最後の RA が送信されると停止します。インターフェイスの IPv6 リンクローカル アドレスには、RA について説明したこと以外に制約事項はありません。他のプロトコルは、このアドレスへのパケットを送受信し続けます。

HSRP では、プライオリティ メカニズムを使用して、デフォルトのアクティブ ルータにする HSRP 設定済みルータを決定します。ルータをアクティブ ルータとして設定するには、他のすべての HSRP 設定済みルータのプライオリティよりも高いプライオリティをそのルータに割り当てます。デフォルトのプライオリティは 100 です。したがって、100 よりも高いプライオリティを持つルータを 1 つだけ設定した場合、そのルータ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デバイスは、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。

- Coup：スタンバイ デバイスがアクティブ デバイスの機能を引き受けるときに、coup メッセージを送信します。
- hello：hello メッセージは、デバイスの HSRP プライオリティとステートに関する情報を他の HSRP デバイスに伝達します。
- Resign：このメッセージは、アクティブ デバイスであるデバイスがシャットダウン直前、またはプライオリティの高いデバイスから hello または coup メッセージが送信されたときに、デバイスから送信されます。

常に、HSRP を使用して設定されているデバイスは次のいずれかのステートになっています。

- Active：デバイスはパケット転送機能を実行しています。
- Init または Disabled：デバイスは 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。スヌーピングにより学習されたネットワーク上の他のデバイスで設定された HSRP グループは、Init ステートとして表示されます。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。
- Learn：デバイスは、仮想 IP アドレスを特定しておらず、アクティブ デバイスからの認証済みの 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、デバイスはアクティブ デバイスからのメッセージを引き続き待機します。
- Listen：デバイスは hello メッセージの受信中です。
- Speak：デバイスは hello メッセージの送受信中です。
- Standby：デバイスはアクティブ デバイス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。

HSRP は、HSRP ステートの変更に関連する syslog メッセージのロギング レベル 5 を使用して、デバイスの syslog バッファを最もプライオリティが低いレベル 6 のメッセージングで満たすことなく、イベントのロギングを可能にします。

IP 冗長性クライアントへの HSRP グループのリンク

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。

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。デバイスがオブジェクト トラッキング対応として設定されていて、なおかつトラッキング対象のオブジェクトがダウンした場合、デバイスのプライオリティはダイナミックに変更されます。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。

HSRP、仮想ルータ冗長プロトコル（VRRP）、Gateway Load Balancing Protocol（GLBP）などのクライアントプロセスで、トラッキング オブジェクトに対する興味を登録し、追跡対象オブジェクトの状態が変化したときに通知を受け取るようにすることができます。

オブジェクト トラッキングの詳細については、『Configuring Enhanced Object Tracking』を参照してください。

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 **standbytrack** 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、**nostandbytrack** 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 **standbytrack** 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。

ICMP リダイレクト メッセージの HSRP サポート

デフォルトでは、Internet Control Message Protocol（ICMP）リダイレクト メッセージの HSRP フィルタリングは、HSRP が実行されているデバイスでイネーブルになっています。

ICMP は、エラーをレポートするためのメッセージ パケットや IP 処理に関連する他の情報を提供する、ネットワーク層インターネット プロトコルです。ICMP は、ホストにエラー パケットとリダイレクト パケットを送信できます。

HSRP を実行しているときは、HSRP グループに属するデバイス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 によってホストがデバイスの実際の IP アドレスにリダイレクトされた場合、そのデバイス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。

HSRP が設定されたインターフェイスでは、ICMP リダイレクト メッセージが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 デバイスへの ICMP リダイレクト

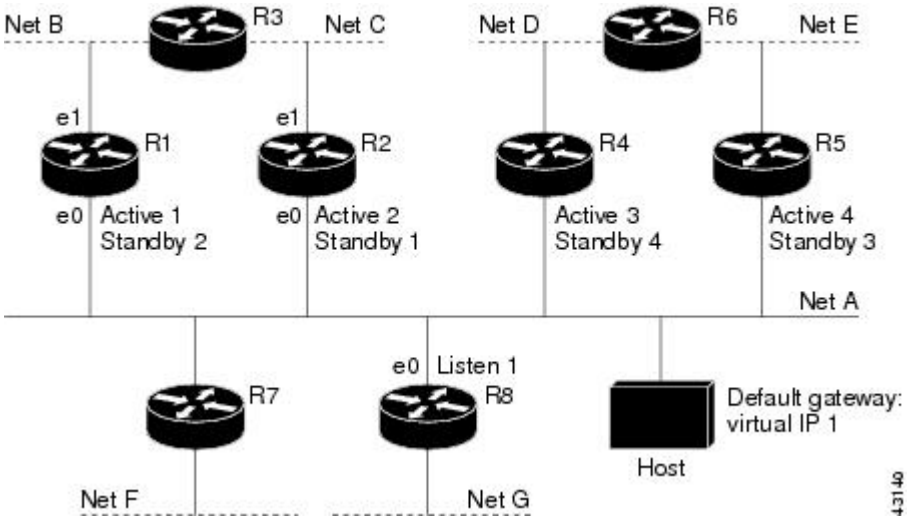
ネクストホップ IP アドレスは、そのネットワーク上のアクティブな HSRP デバイスのリストと比較され、一致が見つかると、実際のネクストホップ IP アドレスが対応する仮想 IP アドレスに置き換えられ、リダイレクト メッセージの続行が許可されます。

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デバイスが HSRP を実行していない場合だけです。パッシブ HSRP デバイスへのリダイレクトは許可されません（パッシブ HSRP デバイスとは、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デバイスです）。

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デバイスには、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 デバイス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 デバイスはネットワークの HSRP パケットをすべてスヌーピングして、アクティブ デバイスのリスト（仮想 IP アドレスと実際の IP アドレス）を管理します。

下の図に示されている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 3 : *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
```

デバイス R1 は、このパケットを受信し、デバイス 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、デバイス 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）。

デバイス 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、デバイス R1 の HSRP プロセスでデバイス R4 がグループ 3 のアクティブ HSRP デバイス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 ホップがデバイス 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。

2 つの変更されたフィールド（*）を示す変更された ICMP リダイレクト メッセージは次のようになります。

```
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 デバイスへの ICMP リダイレクト

パッシブ HSRP デバイスへの ICMP リダイレクトは許可されません。ホストが HSRP デバイスの実際の IP アドレスが検出されると、冗長性が失われる可能性があります。

「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」の図では、デバイス R8 へのリダイレクションは、R8 がパッシブ デバイスのため、許可されます。この場合、ホストからネット D へのパケットは、まずデバイス R1 に到着した後、デバイス 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 デバイス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 リダイレクションが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上のすべてのデバイスに、少なくとも 1 つのアクティブな HSRP グループが含まれている必要があります。

非 HSRP デバイスへの ICMP リダイレクト

ローカル インターフェイスで HSRP を実行していないデバイスへの ICMP リダイレクトは許可されます。非 HSRP デバイスの実際の 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。

「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」の図では、デバイス R7 へのリダイレクションは、R7 が HSRP を実行していないため、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、**nostandbyredirectunknown** コマンドを使用します。

パッシブ HSRP アドバタイズメント メッセージ

パッシブ HSRP デバイスは、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 デバイスが、ネットワークにある任意の HSRP デバイスの 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 デバイスに伝えます。

- アクティブ：インターフェイスには少なくとも 1 つのアクティブなグループがあります。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。
- 休止：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。
- パッシブ：インターフェイスには少なくとも 1 つの非アクティブなグループがあり、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。

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、**standbyredirecttimers** 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 デバイスが、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 デバイス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 **standbyuse-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 デバイス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。

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 デバイスは送信先 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。HSRP デバイスが複数の IP アドレスに同じ 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 アドレスを一意に判別することができなくなるので、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 **debugstandbyeventsicmp** 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 10.0.0.4 for dest 10.0.1.2
10:43:08: HSRP: could not uniquely determine IP address for mac 00d0.bbd3.bc22
```

HSRP の MPLS VPN サポート

HSRP のマルチプロトコル ラベル スイッチング（MPLS）VPN 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 つのプロバイダー エッジ（PE）デバイス間でイーサネット LAN が接続されている場合です。

- カスタマー エッジ（CE）デバイスに 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 つ以上の VPN ルーティングおよび転送（VRF）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 テーブル
- Cisco Express Forwarding 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 テーブルおよび CEF テーブルに格納されます。各 VRF カスタマーに対して、別個の一連のルーティング テーブルおよび Cisco Express Forwarding テーブルが維持されます。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 内のデバイス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上で、数百ものサブインターフェイスがそれぞれ独自の HSRP グループを持つ構成は、複数の HSRP グループのネゴシエーションとメンテナンスのプロセスが発生して、ネットワーク トラフィックと CPU 使用率に悪影響を与える可能性があります。

アクティブ デバイスとスタンバイ デバイス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デバイス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

インサービス ソフトウェア アップグレード（ISSU）プロセスにより、パケット 転送を続行しながら、Cisco 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、計画的なソフトウェア 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、パケット転送中に Cisco ソフトウェアを変更できるため、ネットワークのアベイラビリティが向上し、計画的なソフトウェア アップグレードによるダウンタイムを短縮できます。

ISSU の詳細については、『*Cisco IOS In Service Software Upgrade Process*』の「*High Availability Configuration Guide*」を参照してください。

SSO HSRP

SSO HSRP は、冗長なルート プロセッサ（RP）を装備したデバイスがステートフル スイッチオーバー（SSO）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 デバイスの両方の RP に障害が発生しても、スタンバイ状態の HSRP デバイスが HSRP アクティブ デバイス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 Cisco 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 ノンストップ フォワーディング（NSF）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 機能により、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 デバイスを通じて引き続き転送されます。

SSO HSRP 機能が登場する前は、アクティブ デバイスのプライマリ 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 スイッチとして処理を引き継ぐ、グループの別のスイッチ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 デバイスで 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 デバイスにスイッチ 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、**nostandbysso** 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 ピアリング機能は、ホット スタンバイ ルータ プロトコル（HSRP）グループのメンバのヘルス モニタリング システムに双方向フォワーディング検出（BFD）を導入します。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、hello タイマーやホールドタイマー（ミリ秒単位）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 台のデバイス間の 1 つの BFD セッションだけです。

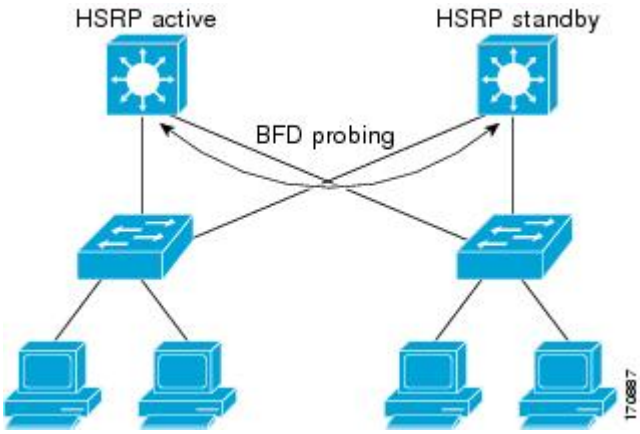
この機能は、デフォルトでイネーブルにされています。HSRP スタンバイ デバイスは、HSRP アクティブ デバイスの実際の IP アドレスを HSRP hello メッセージから検出します。また、BFD クライアントとして登録し、アクティブ デバイスが使用不能になった場合に通知するように要求します。BFD はスタンバイ デバイスとアクティブ デバイス間の接続が失敗したことを確認すると、アクティブ デバイスとしてすぐに引き継ぐスタンバイ デバイス上の HSRP に通知します。

BFD は、インターフェイス、データ リンク、および転送プレーンを含む、2 つの隣接デバイス間の転送パスで、オーバーヘッドの少ない短期間の障害検出方法を提供します。BFD はインターフェイス レベルおよびルーティング 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。シスコでは BFD 非同期モードをサポートしています。これは、デバイス間の BFD ネイバーセッションをアクティブにして維持するための、2 台のシステム間の BFD 制御パケットの送信に依存します。したがって、BFD セッションを作成するには、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 用にデバイス 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 は、あらゆるメディア タイプ、カプセル化、トポロジ、および Border Gateway Protocol（BGP）、Enhanced Interior Gateway Routing Protocol（EIGRP）、Hot Standby Router Protocol（HSRP）、Intermediate System to Intermediate System（IS-IS）、Open Shortest Path First（OSPF）などのルーティングプロトコルとは関係なく、BFD ピアの障害検出時間を短縮します。ローカルデバイスのルーティングプロトコルに高速障害検出通知を送信して、ルーティングテーブル再計算プロセスを開始すると、BFD はネットワーク コンバージェンス時間全体を大幅に短縮できます。下の図は、HSRP と BFD を実行する 2 台のデバイスがある単純なネットワークを示しています。

図 *4*：*HSRP* の *BFD* ピアリング



BFD の詳細については、『*IP Routing: BFD Configuration Guide*』を参照してください。

HSRP MIB トラップ

HSRP MIB は、簡易ネットワーク管理プロトコル（SNMP）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、デバイスがアクティブ 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 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

- CISCO-HSRP-EXT-MIB.my で定義されている cHsrpExtSecAddrEntry
- CISCO-HSRP-EXT-MIB.my で定義されている cHsrpExtIfEntry

cHsrpGrpEntry テーブルは、RFC 2281 の「*Cisco Hot Standby Router Protocol*」で定義されているすべてのグループ情報で構成されています。他のテーブルは、CISCO-HSRP-EXT-MIB.my で定義されている、RFC 2281 へのシスコの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 **standbyip** 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。指定したデバイスが 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 台のデバイスに仮想 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デバイスによって検出されます。

はじめる前に

認証、タイマー、プライオリティ、プリエンプションなど、HSRP で多くの属性を設定できます。HSRP グループをイネーブルにする前に、属性を設定する必要があります。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、他の設定を行う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. イネーブル化
2. **configureterminal**
3. **interface***typenumber*
4. **ipaddress***ip-addressmask*
5. **standby** [*group-number*] **ip** [*ip-address* [**secondary**]]
6. **end**
7. **showstandby** [**all**] [**brief**]
8. **showstandby***typenumber* [*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	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# 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***typenumber* 例： `Device(config)# interface GigabitEthernet 0/0/0`	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	**ipaddress***ip-addressmask* 例： `Device(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： `Device(config-if)# standby 1 ip 172.16.6.100`	HSRP をアクティブにします。 • グループ番号を設定しない場合、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。 • value for the *ip-address* 引数は仮想デバイスの仮想 IP アドレスです。指定したデバイスが 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 台のデバイスに仮想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デバイスによって検出されます。
ステップ 6	**end** 例： `Device(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	**showstandby** [**all**] [**brief**] 例： `Device# show standby`	（任意）HSRP 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 **standbyip** 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	**showstandby***typenumber* [*group-number* | **all**] [**brief**] 例： `Device# show standby GigabitEthernet 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

standbydelay 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デバイス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。

standbytimers コマンドがミリ秒単位で設定されている場合、または VLAN インターフェイスに HSRP が設定されている場合は、**standbyminimumreload** コマンドを使用することを推奨します。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **interface***typenumber*
4. **ipaddress***ip-addressmask*
5. **standbydelayminimum***min-seconds***reload***reload-seconds*
6. **standby** [*group-number*] **ip** [*ip-address* [**secondary**]]
7. **end**
8. **showstandbydelay** [*typenumber*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化	特権 EXEC モードをイネーブルにします。

	コマンドまたはアクション	目的
	例： `Device> enable`	• パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# 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***typenumber* 例： `Device(config)# interface GigabitEthernet 1/0/0`	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	**ipaddress***ip-addressmask* 例： `Device(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	**standbydelayminimum***min-seconds***reload***reload-seconds* 例： `Device(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、デバイスのリロード後に遅延する時間です。この遅延時間は、デバイス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： `Device(config-if)# standby 1 ip 10.0.0.3 255.255.255.0`	HSRP をアクティブにします。

	コマンドまたはアクション	目的
ステップ 7	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 8	**showstandbydelay** [*typenumber*] 例： `Device# show standby delay`	（任意）HSRP の遅延時間に関する情報を表示します。

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. イネーブル化
2. **configureterminal**
3. **interface***typenumber*
4. **ipaddress***ip-addressmask*
5. **standby** [*group-number*] **priority***priority*
6. **standby** [*group-number*] **preempt** [**delay** {**minimum** | **reload** | **sync**} *seconds*]
7. **standby** [*group-number*] **ip***ip-address* [**secondary**]]
8. **end**
9. **showstandby** [**all**] [**brief**]
10. **showstandby***typenumber* [*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	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： `Device# 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***typenumber* 例： `Device(config)# interface GigabitEthernet0/0/0`	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	**ipaddress***ip-addressmask* 例： `Device(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： `Device(config-if)# standby 1 priority 110`	HSRP 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。
ステップ 6	**standby** [*group-number*] **preempt** [**delay** {**minimum** | **reload** | **sync**} *seconds*] 例： `Device(config-if)# standby 1 preempt delay minimum 380`	HSRP 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、デバイス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、後で起動したデバイスはスタンバイ デバイスになります。
ステップ 7	**standby** [*group-number*] **ip***ip-address* [**secondary**]] 例： `Device(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： `Device(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 9	**showstandby** [**all**] [**brief**] 例： `Device# show standby`	（任意）HSRP 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 **standbyip** 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	**showstandby***typenumber* [*group-number* | **all**] [**brief**] 例： `Device# show standby GigabitEthernet 0/0/0`	（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。

HSRP 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。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **track***object-number***interface***typenumber* {**line-protocol** | **iprouting**}
4. **exit**
5. **interface***typenumber*
6. **standby** [*group-number*] **track***object-number* [**decrement***priority-decrement*] [**shutdown**]
7. **standby** [*group-number*] **ip** [*ip-address* [**secondary**]]
8. **end**
9. **showtrack** [*object-number* | **brief**] [**interface** [**brief**] | **iproute** [**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	イネーブル化	特権 EXEC モードをイネーブルにします。

	コマンドまたはアクション	目的
	例： `Device> enable`	• パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# 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***typenumber* {**line-protocol** | **iprouting**} 例： `Device(config)# track 100 interface GigabitEthernet 0/0/0 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： `Device(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	**interface***typenumber* 例： `Device(config)# interface GigabitEthernet 0/0/0`	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 6	**standby** [*group-number*] **track***object-number* [**decrement***priority-decrement*] [**shutdown**] 例： `Device(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、デバイス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。

	コマンドまたはアクション	目的
		• トラッキング対象のオブジェクトがダウンしたときにデバイスの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。 （注） 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、**nostandbytrack** 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 **standbytrack** 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。
ステップ 7	**standby** [*group-number*] **ip** [*ip-address* [**secondary**]] 例： `Device(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 8	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 9	**showtrack** [*object-number* | **brief**] [**interface** [**brief**] | **iproute** [**brief**] | **resolution** | **timers**] 例： `Device# 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

（注） 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、受信側のデバイスの 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。

（注） あるグループのデバイスのキー ストリングを変更する場合、アクティブ デバイスを最後に変更して、HSRP ステートが変化しないようにします。アクティブ デバイスのキー ストリングの変更は、アクティブでないデバイスの後、インターフェイス コンフィギュレーション コマンド **standytimers** 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、アクティブでないデバイスでアクティブ デバイスのタイムアウトが発生することがなくなります。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **terminalinterface***typenumber*
4. **ipaddress***ip-addressmask* [**secondary**]
5. **standby** [*group-number*] **priority***priority*
6. **standby** [*group-number*] **preempt** [**delay** {**minimum** | **reload** | **sync**} *seconds*]
7. **standby** [*group-number*] **authenticationmd5key-string** [**0** | **7**] *key* [**timeout***seconds*]
8. **standby** [*group-number*] **ip** [*ip-address*] [**secondary**]]
9. 通信する各デバイスに対してステップ 1 ～ 8 を繰り返します。
10. **end**
11. **showstandby**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# 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	**terminalinterface***typenumber* 例： `Device(config)# interface GigabitEthernet 0/0/0`	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。

	コマンドまたはアクション	目的
ステップ 4	**ipaddress***ip-addressmask* [**secondary**] 例： `Device(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： `Device(config-if)# standby 1 priority 110`	HSRP プライオリティを設定します。
ステップ 6	**standby** [*group-number*] **preempt** [**delay** {**minimum** | **reload** | **sync**} *seconds*] 例： `Device(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*] **authenticationmd5key-string** [**0** | **7**] *key* [**timeout***seconds*] 例： `Device(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* 引数の長さは、最大 64 文字です。16 文字以上を使用することをお勧めします。 • *key* 引数にはプレフィッ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。**servicepassword-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場合、key-string 認証キーは自動的に暗号化されます。 • **timeout** 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： `Device(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	通信する各デバイスに対してステップ 1 ～ 8 を繰り返します。	—

	コマンドまたはアクション	目的
ステップ 10	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 11	**showstandby** 例： `Device# show standby`	（任意）HSRP 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）。

キー チェーンを使用した HSRP MD5 認証の設定

キー チェーンを使用して HSRP 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 チェーン設定に従って異なる時点で異なるキー 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. イネーブル化
2. **configureterminal**
3. **keychain***name-of-chain*
4. **key***key-id*
5. **key-string***string*
6. **exit**
7. **exit**
8. **interface***typenumber*
9. **ipaddress***ip-addressmask* [**secondary**]
10. **standby** [*group-number*] **priority***priority*
11. **standby** [*group-number*] **preempt** [**delay** {**minimum** | **reload** | **sync**} *seconds*]
12. **standby** [*group-number*] **authenticationmd5key-chain***key-chain-name*
13. **standby** [*group-number*] **ip** [*ip-address* [*secondary*]]
14. 通信する各デバイスに対してステップ 1 ～ 12 を繰り返します。
15. **end**
16. **showstandby**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# 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	**keychain***name-of-chain* 例： `Device(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、キー チェーン キー 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	**key***key-id* 例： `Device(config-keychain)# key 100`	キーチェーンの認証キーを識別し、キーチェーンキーコンフィギュレーション モードを開始します。 • *key-id* 引数の値には数値を指定する必要があります。
ステップ 5	**key-string***string* 例： `Device(config-keychain-key)# key-string mno172`	キーの認証文字列を指定します。 • *string* 引数の値は、1 ～ 80 文字の大文字または小文字の英数字を指定できます。最初の文字には数字を使用できません。
ステップ 6	**exit** 例： `Device(config-keychain-key)# exit`	キー チェーン キー 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： `Device(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***typenumber* 例： `Device(config)# interface GigabitEthernet 0/0/0`	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。

	コマンドまたはアクション	目的
ステップ 9	**ipaddress***ip-addressmask* [**secondary**] 例： `Device(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 10	**standby** [*group-number*] **priority***priority* 例： `Device(config-if)# standby 1 priority 110`	HSRP プライオリティを設定します。
ステップ 11	**standby** [*group-number*] **preempt** [**delay** {**minimum** | **reload** | **sync**} *seconds*] 例： `Device(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 12	**standby** [*group-number*] **authenticationmd5key-chain***key-chain-name* 例： `Device(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 で指定した名前に一致する必要があります。
ステップ 13	**standby** [*group-number*] **ip** [*ip-address* [*secondary*]] 例： `Device(config-if)# standby 1 ip 10.21.8.12`	HSRP をアクティブにします。
ステップ 14	通信する各デバイスに対してステップ 1 ～ 12 を繰り返します。	—
ステップ 15	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 16	**showstandby** 例： `Device# show standby`	（任意）HSRP 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）。

	コマンドまたはアクション	目的

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. イネーブル化
2. **debugstandbyerrors**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**debugstandbyerrors** 例： `Device# 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。

例

次の例では、デバイス A には MD5 テキスト文字列認証が設定されていますが、デバイス B にはデフォルトのテキスト認証が設定されています。

```
Device# 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、デバイス A とデバイス B の両方に別々の MD5 認証文字列が設定されています。

```
Device# 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. イネーブル化
2. **configureterminal**
3. **interface***typenumber*
4. **ipaddress***ip-addressmask* [**secondary**]
5. **standby** [*group-number*] **priority***priority*
6. **standby** [*group-number*] **preempt** [**delay** {**minimum** | **reload** | **sync**} *seconds*]
7. **standby** [*group-number*] **authenticationtext***string*
8. **standby** [*group-number*] **ip** [*ip-address* [**secondary**]]
9. 通信する各デバイスに対してステップ 1 ～ 8 を繰り返します。
10. **end**
11. **showstandby**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# 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***typenumber* 例： `Device(config)# interface GigabitEthernet 0/0/0`	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	**ipaddress***ip-addressmask* [**secondary**] 例： `Device(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。

	コマンドまたはアクション	目的
ステップ 5	**standby** [*group-number*] **priority***priority* 例： `Device(config-if)# standby 1 priority 110`	HSRP プライオリティを設定します。
ステップ 6	**standby** [*group-number*] **preempt** [**delay** {**minimum** | **reload** | **sync**} *seconds*] 例： `Device(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*] **authenticationtext***string* 例： `Device(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： `Device(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	通信する各デバイスに対してステップ 1 ～ 8 を繰り返します。	--
ステップ 10	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 11	**showstandby** 例： `Device# show standby`	（任意）HSRP 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

（注） hello-time と hold-time 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。

standbydelay 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。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **interface***typenumber*
4. **ipaddress***ip-addressmask* [**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	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# 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***typenumber* 例： `Device(config)# interface Gigabit Ethernet 0/0/1`	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	**ipaddress***ip-addressmask* [**secondary**]] 例： `Device(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。

	コマンドまたはアクション	目的
ステップ 5	**standby** [*group-number*] **timers** [**msec**] *hellotime* [**msec**] *holdtime* 例： `Device(config-if)# standby 1 timers 5 15`	hello パケットの間隔と、他のデバイスがアクティブホットスタンバイまたはスタンバイデバイスの終了を宣言するまでの時間を設定します。
ステップ 6	**standby** [*group-number*] **ip** [*ip-address* [**secondary**]] 例： `Device(config-if)# standby 1 ip 10.0.0.3`	HSRP をアクティブにします。

HSRP MAC リフレッシュ インターバルの設定

手順の概要

1. イネーブル化
2. **configureterminal**
3. **interface***typenumber*
4. **ipaddress***ip-addressmask* [**secondary**]
5. **standbymac-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	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# 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***typenumber* 例： `Device(config)# interface GigabitEthernet 0/0/1`	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	**ipaddress***ip-addressmask* [**secondary**] 例： `Device(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	**standbymac-refresh***seconds* 例： `Device(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 で動作する HSRP のみに適用されます。
ステップ 6	**standby** [*group-number*] **ip** [*ip-address* [**secondary**]] 例： `Device(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、冗長デバイスを余すところなく活用できるようになります。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デバイスは、別のグループに対してスタンバイ ステートやリッスン ステートになることができます。

2 台のデバイスを使用している場合、デバイス 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、デバイス 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。図と設定例については、「例：ロード バランシング用の複数の HSRP グループの設定」を参照してください。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **interface***typenumber*
4. **ipaddress***ip-addressmask* [**secondary**]
5. **standby** [*group-number*] **priority***priority*
6. **standby** [*group-number*] **preempt** [**delay** {**minimum** | **reload** | **sync**} *delay*]
7. **standby** [*group-number*] **ip** [*ip-address*] **secondary**]
8. 同じデバイスでステップ 5 ～ 7 を繰り返して、別のスタンバイ グループのデバイス属性を設定します。
9. **exit**
10. もう 1 つのデバイスでステップ 3 ～ 9 を繰り返します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# 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***typenumber* 例： `Device(config)# interface GigabitEthernet 0/0/0`	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	**ipaddress***ip-addressmask* [**secondary**] 例： `Device(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： `Device(config-if)# standby 1 priority 110`	HSRP プライオリティを設定します。

	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** | **reload** | **sync**} *delay*] 例： `Device(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： `Device(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	同じデバイスでステップ 5 ～ 7 を繰り返して、別のスタンバイ グループのデバイス属性を設定します。	たとえば、デバイス A をグループ 1 のアクティブ デバイス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 デバイスまたはスタンバイ デバイスとして設定することができます。
ステップ 9	**exit** 例： `Device(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 つのデバイスでステップ 3 ～ 9 を繰り返します。	もう 1 つのデバイスで複数の 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

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。

standbyfollow 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。

standbymac-refresh*seconds* コマンドを使用して、HSRP クライアント グループの更新間隔を直接変更します。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。

（注）

- 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。

```
Device(config-if)# standby 1 priority 110
%Warning: This setting has no effect while following another group.
Device(config-if)# standby 1 timers 5 15
    % Warning: This setting has no effect while following another group.
Device(config-if)# standby 1 preempt delay minimum 300
    % Warning: This setting has no effect while following another group.
```

はじめる前に

「ロード バランシング用の複数の HSRP グループの設定」セクションのステップを使用して、HSRP グループのマスター グループを設定します。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **interface***typenumber*
4. **ipaddress***ip-addressmask* [**secondary**]
5. **standbymac-refresh***seconds*
6. **standby***group-number***follow***group-name*
7. **exit**
8. 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	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# 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***typenumber* 例： `Device(config)# interface GigabitEthernet 0/0/0`	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	**ipaddress***ip-addressmask* [**secondary**] 例： `Device(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	**standbymac-refresh***seconds* 例： `Device(config-if)# standby mac-refresh 30`	HSRP クライアント グループの更新間隔を設定します。
ステップ 6	**standby***group-number***follow***group-name* 例： `Device(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 7	**exit** 例： `Device(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 8	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。

ICMP リダイレクト メッセージの HSRP 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 が実行されているデバイス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、デバイス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. イネーブル化
2. **configureterminal**
3. **interface***typenumber*
4. **standbyredirect** [**timers***advertisementholddown*] [**unknown**]
5. **end**
6. **showstandbyredirect** [*ip-address*] [*interface-typeinterface-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	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# 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***typenumber* 例： `Device(config)# interface GigabitEthernet 0/0/0`	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	**standbyredirect** [**timers***advertisementholddown*] [**unknown**] 例： `Device(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： `Device(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 6	**showstandbyredirect** [*ip-address*] [*interface-typeinterface-number*] [**active**] [**passive**] [**timers**] 例： `Device# 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

（注） **standbyuse-bia** コマンドと **standbymac-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。

standbyuse-bia コマンドには次の欠点があります。

- あるデバイス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 デバイスは、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。
- プロキシ ARP は、**standbyuse-bia** コマンドを設定すると機能しません。デバイス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 デバイスはそれに対応できなくなります。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **interface***typenumber*
4. **ipaddress***ip-addressmask* [**secondary**]
5. 次のいずれかのコマンドを入力します。
   - **standby** [*group-number*] **mac-address***mac-address*
   - または
   - **standbyuse-bia** [**scopeinterface**]
   - または
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	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# 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***typenumber* 例： `Device(config)# interface GigabitEthernet 0/0/0`	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	**ipaddress***ip-addressmask* [**secondary**] 例： `Device(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	次のいずれかのコマンドを入力します。
	• **standby** [*group-number*] **mac-address***mac-address*
	• または
	• **standbyuse-bia** [**scopeinterface**]
	• または
	
	例：
	`Device(config-if)# standby 1 mac-address 5000.1000.1060`
	
	例：
	`Device(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。
		• **scopeinterface** 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**]]	HSRP をアクティブにします。

	コマンドまたはアクション	目的
	例： `Device(config-if)# standby 1 ip 172.16.6.100`	

HSRP グループへの IP 冗長性クライアントのリンク

はじめる前に

クライアント アプリケーションでは、**standbyname** 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. イネーブル化
2. **configureterminal**
3. **interface***typenumber*
4. **ipaddress***ip-addressmask*
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	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# 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***typenumber* 例： `Device(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。

	コマンドまたはアクション	目的
ステップ 4	**ipaddress***ip-addressmask* 例： `Device(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： `Device(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： `Device(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 では HSRP バージョン 1 とは異なるパケット フォーマットを使用します。

（注）

- 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。どちらのバージョンも相互に排他的なので、インターフェイスはバージョン 1 およびバージョン 2 の両方を運用できません。しかし、同一デバイスの異なる物理インターフェイス上であれば、異なるバージョンを実行できます。バージョン 1 で認められるグループ番号範囲（0 ～ 255）を超えるグループを設定している場合は、バージョン 2 からバージョン 1 への変更はできません。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **interface***typenumber*
4. **ipaddress***ip-addressmask*
5. **standbyversion** {**1** | **2**}
6. **standby** [*group-number*] **ip** [*ip-address* [**secondary**]]
7. **end**
8. **showstandby**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# 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***typenumber* 例： `Device(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。
ステップ 4	**ipaddress***ip-addressmask* 例： `Device(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	**standbyversion** {**1** | **2**} 例： `Device(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**]]	HSRP をアクティブにします。

	コマンドまたはアクション	目的
	例： `Device(config-if)# standby 400 ip 10.10.28.5`	• HSRP バージョン 2 のグループ番号範囲は 0 ～ 4095 です。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： `Device(config-if)# end`	現在のコンフィギュレーションセッションを終了して、特権 EXEC モードに戻ります。
ステップ 8	**showstandby** 例： `Device# show standby`	（任意）HSRP 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

SSO 対応 HSRP 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、**nostandbysso** 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. イネーブル化
2. **configureterminal**
3. 冗長性
4. **modesso**
5. **exit**
6. **nostandbysso**
7. **standbysso**
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	**イネーブル化** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# 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	**冗長性** 例： `Device(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	**modesso** 例： `Device(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。 • 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： `Device(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。
ステップ 6	**nostandbysso** 例： `Device(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	**standbysso** 例： `Device(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： `Device(config)# end`	現在のコンフィギュレーションセッションを終了して、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. **showstandby**
2. **debugstandbyeventsha**

手順の詳細

ステップ 1 **showstandby**

showstandby 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。

例：

```
Device# show standby

GigabitEthernet0/0/0 - Group 1
 State is Active (standby RP)
 Virtual IP address is 10.1.0.7
 Active virtual MAC address is unknown
  Local virtual MAC address is 000a.f3fd.5001 (bia)
 Hello time 1 sec, hold time 3 sec
 Authentication text "authword"
 Preemption enabled
 Active router is unknown
 Standby router is unknown
 Priority 110 (configured 120)
  Track object 1 state Down decrement 10
 Group name is "name1" (cfgd)
```

ステップ 2 **debugstandbyeventsha**

debugstandbyeventsha 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。

例：

```
Device# debug standby events ha

!Active RP
*Apr 27 04:13:47.755: HSRP: Gi0/0/1 Grp 101 RF Encode state Listen into sync buffer
*Apr 27 04:13:47.855: HSRP: CF Sync send ok
*Apr 27 04:13:57.755: HSRP: Gi0/0/1 Grp 101 RF Encode state Speak into sync buffer
*Apr 27 04:13:57.855: HSRP: CF Sync send ok
*Apr 27 04:14:07.755: HSRP: Gi0/0/1 Grp 101 RF Encode state Standby into sync buffer
*Apr 27 04:14:07.755: HSRP: Gi0/0/1 Grp 101 RF Encode state Active into sync buffer
*Apr 27 04:14:07.863: HSRP: CF Sync send ok
*Apr 27 04:14:07.867: HSRP: CF Sync send ok
!Standby RP
*Apr 27 04:11:21.011: HSRP: RF CF client 32, entity 0 got msg len 24
```

```
*Apr 27 04:11:21.011: HSRP: Gi0/0/1 Grp 101 RF sync state Init -> Listen
*Apr 27 04:11:31.011: HSRP: RF CF client 32, entity 0 got msg len 24
*Apr 27 04:11:31.011: HSRP: Gi0/0/1 Grp 101 RF sync state Listen -> Speak
*Apr 27 04:11:41.071: HSRP: RF CF client 32, entity 0 got msg len 24
*Apr 27 04:11:41.071: HSRP: RF CF client 32, entity 0 got msg len 24
*Apr 27 04:11:41.071: HSRP: Gi0/0/1 Grp 101 RF sync state Speak -> Standby
*Apr 27 04:11:41.071: HSRP: Gi0/0/1 Grp 101 RF sync state Standby -> Active
```

HSRP MIB トラップのイネーブル化

手順の概要

1. イネーブル化
2. **configureterminal**
3. **snmp-serverenabletrapshsrp**
4. **snmp-serverhost***hostcommunity-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	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# 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-serverenabletrapshsrp** 例： `Device(config)# snmp-server enable traps hsrp`	SNMP トラップ、SNMP インフォーム、HSRP 通知をデバイスが送信できるようにします。
ステップ 4	**snmp-serverhost***hostcommunity-string***hsrp** 例： `Device(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、Bidirectional Forwarding Detection（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。BFDネイバーに対して BFD セッションを実行するインターフェイスごとに、この手順を繰り返します。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **interface***typenumber*
4. **bfdinterval***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	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# 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***typenumber* 例： `Device(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	**bfdinterval***milliseconds***min_rx***milliseconds***multiplier***interval-multiplier* 例： `Device(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。

	コマンドまたはアクション	目的
ステップ 5	**end** 例： `Device(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、Hot Standby Router Protocol（HSRP）Bidirectional Forwarding Detection（BFD）ピアリングをイネーブルにする作業を行います。この作業のステップは、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 ピアリングがディセーブルになっている場合、デバイス 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。

はじめる前に

この作業を進める前に

- HSRP は、参加しているすべてのデバイスで実行されている必要があります。
- シスコ エクスプレス フォワーディングをイネーブルにする必要があります。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **ipcef**[**distributed**]
4. **interface***typenumber*
5. **ipaddress***ip-addressmask*
6. **standby** [*group-number*] **ip** [*ip-address* [**secondary**]]
7. **standbybfd**
8. **exit**
9. **standbybfdall-interfaces**
10. **exit**
11. **showstandby**[**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	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# 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	**ipcef**[**distributed**] 例： `Device(config)# ip cef`	シスコ エクスプレス フォワーディングまたは分散型シスコ エクスプレス フォワーディングをイネーブルにします。
ステップ 4	**interface***typenumber* 例： `Device(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	**ipaddress***ip-addressmask* 例： `Device(config-if)# ip address 10.0.0.11 255.255.255.0`	インターフェイスに IP アドレスを設定します。
ステップ 6	**standby** [*group-number*] **ip** [*ip-address* [**secondary**]] 例： `Device(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	**standbybfd** 例： `Device(config-if)# standby bfd`	（任意）インターフェイスで BFD に対する HSRP 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 8	**exit** 例： `Device(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	**standbybfdall-interfaces** 例： `Device(config)# standby bfd all-interfaces`	（任意）すべてのインターフェイスで BFD に対する HSRP をイネーブルにします。
ステップ 10	**exit** 例： `Device(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	**showstandby**[**neighbors**] 例： `Device# show standby neighbors`	（任意）BFD に対する HSRP サポートについての情報を表示します。

HSRP BFD ピアリングの検証

Hot Standby Router Protocol（HSRP）Bidirectional Forwarding Detection（BFD）ピアリングを確認するには、次のオプション コマンドを使用します。

手順の概要

1. **showstandby**
2. **showstandby brief**
3. **showstandbyneighbors**[*typenumber*]
4. **showbfdneighbors**
5. **showbfdneighborsdetails**

手順の詳細

ステップ 1 **showstandby**

showstandby コマンドを実行すると、HSRP に関する情報が表示されます。

例：

```
Device# 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 **showstandby brief**

showstandby brief コマンドを実行すると、HSRP スタンバイ デバイス情報が簡潔に表示されます。

例：

```
Device# show standby brief

Interface   Grp  Pri P State   Active  Standby                     Virtual IP

Et0/0       4    120 P Active  local   172.24.1.2                  172.24.1.254
Et1/0       6    120 P Active  local   FE80::A8BB:CCFF:FE00:3401   FE80::5:73FF:FEA0:6
```

ステップ 3 **showstandbyneighbors**[*typenumber*]

showstandbyneighbors コマンドを実行すると、インターフェイスの HSRP ピア デバイスに関する情報が表示されます。

例：

```
Device1# show standby neighbors

HSRP neighbors on FastEthernet2/0
    10.1.0.22
    No active groups
    Standby groups: 1
    BFD enabled !

Device2# show standby neighbors

HSRP neighbors on FastEthernet2/0
    10.0.0.2
    Active groups: 1
    No standby groups
    BFD enabled !
```

ステップ 4 **showbfdneighbors**

showbfdneighbors コマンドを実行すると、現在の双方向フォワーディング検出（BFD）の隣接関係が 1 行ずつ一覧表示されます。

例：

```
Device# show bfd neighbors

IPv6 Sessions

NeighAddr                              LD/RD         RH/RS     State     Int

FE80::A8BB:CCFF:FE00:3401               4/3          Up        Up        Et1/0
FE80::A8BB:CCFF:FE00:3401               4/3          Up        Up        Et1/0
```

ステップ 5 **showbfdneighborsdetails**

details キーワードを使用すると、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。

例：

```
Device# 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 の設定例

例：HSRP のプライオリティとプリエンプションの設定

次の例では、デバイス A は、デバイス 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 デバイスになっているほか、グループ 2 のスタンバイ デバイスになっています。デバイス B は、グループ 2 のアクティブ デバイスおよびグループ 1 のスタンバイ デバイスになるように設定されています。

デバイス A の設定

```
Device(config)# interface GigabitEthernet 0/0/0
Device(config-if)# ip address 10.1.0.21 255.255.0.0
Device(config-if)# standby 1 priority 110
Device(config-if)# standby 1 preempt
Device(config-if)# standby 1 ip 10.1.0.1
Device(config-if)# standby 2 priority 95
```

```
Device(config-if)# standby 2 preempt
Device(config-if)# standby 2 ip 10.1.0.2
```

デバイス B の設定

```
Device(config)# interface GigabitEthernet 0/0/0
Device(config-if)# ip address 10.1.0.22 255.255.0.0
Device(config-if)# standby 1 preempt
Device(config-if)# standby 1 priority 105
Device(config-if)# standby 1 ip 10.1.0.1
Device(config-if)# standby 2 priority 110
Device(config-if)# standby 2 preempt
Device(config-if)# standby 2 ip 10.1.0.2
```

例：HSRP オブジェクト トラッキングの設定

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。ギガビット イーサネット インターフェイス 0/0/0 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、デバイス A はデバイス B よりもプライオリティが高いので、デバイス A が HSRP アクティブ デバイスになります。ただし、デバイス 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デバイス B がアクティブ デバイス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。

デバイス A の設定

```
Device(config)# track 100 interface serial 1/0/0 ip routing
!
Device(config)# interface GigabitEthernet 0/0/0
Device(config-if)# ip address 10.1.0.21 255.255.0.0
Device(config-if)# standby 1 preempt
Device(config-if)# standby 1 priority 110
Device(config-if)# standby 1 track 100 decrement 10
Device(config-if)# standby 1 ip 10.1.0.1
```

デバイス B の設定

```
Device(config)# track 100 interface serial 1/0/0 ip routing
!
Device(config)# interface GigabitEthernet 0/0/0
Device(config-if)# ip address 10.1.0.22 255.255.0.0
Device(config-if)# standby 1 preempt
Device(config-if)# standby 1 priority 105
Device(config-if)# standby 1 track 100 decrement 10
Device(config-if)# standby 1 ip 10.1.0.1
```

例：HSRP グループ シャットダウンの設定

次の例では、トラッキング プロセスはギガビット イーサネット インターフェイス 0/0/0 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。ギガビット イーサネット インターフェイス 0/0/1 の HSRP は、ギガビット イーサネット インターフェイス 0/0/0 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。ギガビット イーサネット インターフェイス 0/0/0 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。

両方のギガビット イーサネット インターフェイスが動作している場合は、デバイス A はデバイス B よりもプライオリティが高いので、デバイス A が HSRP アクティブ デバイスになります。ただし、デバイス A のギガビット イーサネット インターフェイス 0/0/0 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デバイス B がアクティブ デバイス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。

デバイス A の設定

```
Device(config)# track 100 interface GigabitEthernet 0/0/0 ip routing
!
Device(config)# interface GigabitEthernet 0/0/1
Device(config-if)# ip address 10.1.0.21 255.255.0.0
Device(config-if)# standby 1 ip 10.1.0.1
Device(config-if)# standby 1 preempt
Device(config-if)# standby 1 priority 110
Device(config-if)# standby 1 track 100 shutdown
```

デバイス B の設定

```
Device(config)# track 100 interface GigabitEthernet 0/0/0 ip routing
!
Device(config)# interface GigabitEthernet 0/0/1
Device(config-if)# ip address 10.1.0.22 255.255.0.0
Device(config-if)# standby 1 ip 10.1.0.1
Device(config-if)# standby 1 preempt
Device(config-if)# standby 1 priority 105
Device(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、**nostandbytrack** 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 **standbytrack** 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。

```
Device(config)# no standby 1 track 100 decrement 10
Device(config)# standby 1 track 100 shutdown
```

例：キー ストリングを使用した HSRP MD5 認証の設定

```
Device(config)# interface GigabitEthernet 0/0/0
```

```
Device(config-if)# standby 1 priority 110
Device(config-if)# standby 1 preempt
Device(config-if)# standby 1 authentication md5 key-string 54321098452103ab timeout 30
Device(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、HSRP にはキー チェーン「hsrp1」が必要です。

```
Device(config)# key chain hsrp1
Device(config-keychain)# key 1
Device(config-keychain-key)# key-string 54321098452103ab
Device(config-keychain-key)# exit
Device(config)# interface GigabitEthernet 0/0/0
Device(config-if)# standby 1 priority 110
Device(config-if)# standby 1 preempt
Device(config-if)# standby 1 authentication md5 key-chain hsrp1
Device(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 認証の設定

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。

デバイス 1

```
Device(config)# key chain hsrp1
Device(config-keychain)# key 0
Device(config-keychain-key)# key-string 54321098452103ab
Device(config-keychain-key)# exit
Device(config)# interface GigabitEthernet 0/0/0
Device(config-if)# standby 1 authentication md5 key-chain hsrp1
Device(config-if)# standby 1 ip 10.21.0.10
```

デバイス 2

```
Device(config)# interface GigabitEthernet 0/0/0
Device(config-if)# standby 1 authentication md5 key-string 54321098452103ab
Device(config-if)# standby 1 ip 10.21.0.10
```

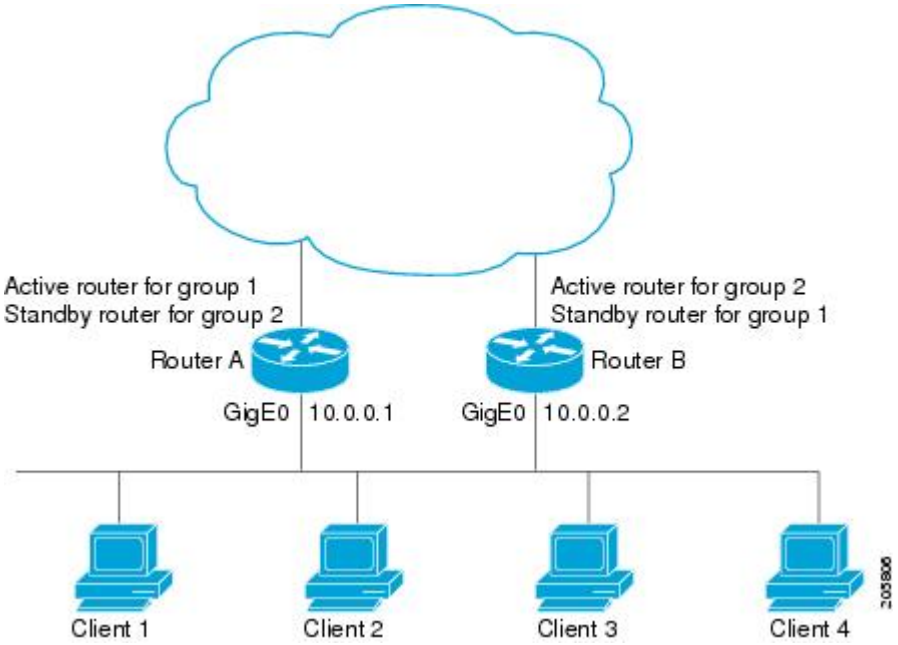
例：HSRP テキスト認証の設定

```
Device(config)# interface GigabitEthernet 0/0/0
Device(config-if)# standby 1 priority 110
Device(config-if)# standby 1 preempt
Device(config-if)# standby 1 authentication text company2
Device(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 グループの設定

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。下の図では、半分のクライアントがルータ A に設定されており、もう半分はルータ B に設定されています。ルータ A およびルータ B の設定により、合計 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 に最高のプライオリティが割り当てられているので、ルータ A がデフォルトのアクティブ ルータになり、ルータ B がスタンバイ ルータとなります。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。通常の運用では、2 つのルータが IP トラフィック負荷を分散します。いずれかのルータが使用できなくなると、もう一方のルータがアクティブになり、使用できない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 **standbypreempt** が必要です。

図 *5*：*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
!
Router(config)# interface GigabitEthernet 0/0/0
Router(config-if)# ip address 10.0.0.1 255.255.255.0
```

```
Router(config-if)# standby 1 priority 110
Router(config-if)# standby 1 preempt
Router(config-if)# standby 1 ip 10.0.0.3
Router(config-if)# standby 2 preempt
Router(config-if)# standby 2 ip 10.0.0.4
```

ルータ B の設定

```
Router(config)# hostname RouterB
!
Router(config)# interface GigabitEthernet 0/0/0
Router(config-if)# ip address 10.0.0.2 255.255.255.0
Router(config-if)# standby 1 preempt
Router(config-if)# standby 1 ip 10.0.0.3
Router(config-if)# standby 2 priority 110
Router(config-if)# standby 2 preempt
Router(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。

```
Device(config)# interface GigabitEthernet 0/0/0
Device(config-if)# no shutdown
Device(config-if)# standby mac-refresh 30
! Client Hello message interval
!
Device(config)# interface GigabitEthernet 0/0/1
Device(config-if)# no shutdown
Device(config-if)# ip vrf forwarding VRF2
Device(config-if)# ip address 10.0.0.100 255.255.0.0
Device(config-if)# standby 1 ip 10.0.0.254
Device(config-if)# standby 1 priority 110
Device(config-if)# standby 1 preempt
Device(config-if)# standby 1 name HSRP1
!Server group
!
Device(config)# interface GigabitEthernet 0/0/2
Device(config-if)# no shutdown
Device(config-if)# ip vrf forwarding VRF3
Device(config-if)# ip address 10.0.0.100 255.255.0.0
Device(config-if)# standby 2 ip 10.0.0.254
Device(config-if)# standby 2 follow HSRP1
! Client group
!
Device(config)# interface GigabitEthernet 0/0/3
Device(config-if)# no shutdown
Device(config-if)# ip vrf forwarding VRF4
Device(config-if)# ip address 10.0.0.100 255.255.0.0
Device(config-if)# standby 2 ip 10.0.0.254
Device(config-if)# standby 2 follow HSRP1
! Client group
```

例：ICMP リダイレクト メッセージの HSRP サポートの設定

デバイス 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

```
Device(config)# interface GigabitEthernet 0/0/0
Device(config-if)# ip address 10.0.0.10 255.0.0.0
Device(config-if)# standby redirect
Device(config-if)# standby 1 priority 120
Device(config-if)# standby 1 preempt delay minimum 20
Device(config-if)# standby 1 ip 10.0.0.1
Device(config-if)# standby 2 priority 105
Device(config-if)# standby 2 preempt delay minimum 20
Device(config-if)# standby 2 ip 10.0.0.2
```

デバイス 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

```
Device(config)# interface GigabitEthernet 0/0/0
Device(config-if)# ip address 10.0.0.11 255.0.0.0
Device(config-if)# standby redirect
Device(config-if)# standby 1 priority 105
Device(config-if)# standby 1 preempt delay minimum 20
Device(config-if)# standby 1 ip 10.0.0.1
Device(config-if)# standby 2 priority 120
Device(config-if)# standby 2 preempt delay minimum 20
Device(config-if)# standby 2 ip 10.0.0.2
```

例：HSRP 仮想 MAC アドレスと BIA MAC アドレスの設定

Advanced Peer-to-Peer Networking（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するのが通常です。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。

```
Device(config)# interface GigabitEthernet 0/0/0
Device(config-if)# ip address 10.0.0.1
Device(config-if)# standby 1 mac-address 4000.1000.1060
Device(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。

```
Device(config)# interface token 3/0
Device(config-if)# standby use-bia
```

（注） **standbyuse-bia** コマンドと **standbymac-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 Network Address Translation（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、**standbyname** 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 台のデバイスが HSRP アクティブ デバイスと HSRP スタンバイ デバイス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 デバイスの設定

```
Device(config)# interface BVI 10
Device(config-if)# ip address 192.168.5.54 255.255.255.255.0
Device(config-if)# no ip redirects
Device(config-if)# ip nat inside
Device(config-if)# standby 10 ip 192.168.5.30
Device(config-if)# standby 10 priority 110
Device(config-if)# standby 10 preempt
Device(config-if)# standby 10 name group1
Device(config-if)# standby 10 track Ethernet 2/1
!
!
Device(config)# ip default-gateway 10.0.18.126
Device(config)# ip nat inside source static 192.168.5.33 10.10.10.5 redundancy group1
Device(config)# ip classless
Device(config)# ip route 10.10.10.0 255.255.255.0 Ethernet 2/1
Device(config)# ip route 172.22.33.0 255.255.255.0 Ethernet 2/1
Device(config)# no ip http server
```

スタンバイ デバイスの設定

```
Device(config)# interface BVI 10
Device(config-if)# ip address 192.168.5.56 255.255.255.255.0
Device(config-if)# no ip redirects
Device(config-if)# ip nat inside
Device(config-if)# standby 10 priority 95
Device(config-if)# standby 10 preempt
Device(config-if)# standby 10 name group1
Device(config-if)# standby 10 ip 192.168.5.30
Device(config-if)# standby 10 track Ethernet 3/1
Device(config-if)# exit
Device(config)# ip default-gateway 10.0.18.126
Device(config)# ip nat inside source static 192.168.5.33 3.3.3.5 redundancy group1
Device(config)# ip classless
Device(config)# ip route 10.0.32.231 255.255.255 Ethernet 3/1
Device(config)# ip route 10.10.10.0 255.255.255.0 Ethernet 3/1
Device(config)# no ip http server
```

例：HSRP バージョン 2 の設定

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。

```
Device(config)# interface vlan 350
Device(config-if)# standby version 2
Device(config-if)# standby 350 priority 110
Device(config-if)# standby 350 preempt
```

```
Device(config-if)# standby 350 timers 5 15
Device(config-if)# standby 350 ip 172.20.100.10
```

例：SSO 対応 HSRP のイネーブル化

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。

```
Device(config)# redundancy
Device(config-red)# mode sso
```

nostandbysso コマンドを使用して SSO HSRP をディセーブルにすると、次の図に示すように、再度イネーブルにできます。

```
Device(config)# interface GigabitEthernet 1/0/0
Device(config-if)# ip address 10.1.1.1 255.255.0.0
Device(config-if)# standby priority 200
Device(config-if)# standby preempt
Device(config-if)# standby sso
```

例：HSRP MIB トラップのイネーブル化

次の例は、HSRP を 2 台のデバイスで設定し、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 台のデバイスがアクティブ デバイスとして優先されます。アクティブ デバイスとしてデバイスを設定するには、デバイスを高い優先順位に設定し、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 デバイスはプライマリ デバイスと呼ばれます。2 台目のデバイスはバックアップ デバイスと呼ばれます。

デバイス A

```
Device(config)# interface GigabitEthernet 0/0/0
Device(config-if)# ip address 10.1.1.1 255.255.0.0
Device(config-if)# standby priority 200
Device(config-if)# standby preempt
Device(config-if)# standby ip 10.1.1.3
Device(config-if)# exit
Device(config)# snmp-server enable traps hsrp
Device(config)# snmp-server host yourhost.cisco.com public hsrp
```

デバイス B

```
Device(config)#interface GigabitEthernet 1/0/0
Device(config-if)# ip address 10.1.1.2 255.255.0.0
Device(config-if)#  standby priority 101
Device(config-if)# standby ip 10.1.1.3
Device(config-if)# exit
Device(config)# snmp-server enable traps hsrp
Device(config)# snmp-server host myhost.cisco.com public hsrp
```

例：HSRP BFD ピアリング

Hot Standby Router Protocol（HSRP）は、HSRP グループ メンバのヘルス モニタリング システムの一部として Bidirectional Forwarding Detection（BFD）をサポートします。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 台のデバイス間の 1 つの BFD セッションだけです。

次の例では、**standbybfd** コマンドと **standbybfdall-interfaces** コマンドが表示されません。**bfdinterval** コマンドを使用して、BFD がデバイス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。**standbybfd** コマンドと **standbybfdall-interfaces** コマンドは、BFD がデバイスまたはインターフェイスで手動で無効にされている場合にのみ必要です。

デバイス A

```
DeviceA(config)# ip cef
DeviceA(config)# interface FastEthernet2/0
DeviceA(config-if)#  no shutdown
DeviceA(config-if)# ip address 10.0.0.2 255.0.0.0
DeviceA(config-if)# ip router-cache cef
DeviceA(config-if)# bfd interval 200 min_rx 200 multiplier 3
DeviceA(config-if)# standby 1 ip 10.0.0.11
DeviceA(config-if)# standby 1 preempt
DeviceA(config-if)# standby 1 priority 110
DeviceA(config-if)# standby 2 ip 10.0.0.12
DeviceA(config-if)# standby 2 preempt
DeviceA(config-if)# standby 2 priority 110
```

デバイス B

```
DeviceB(config)# interface FastEthernet2/0
DeviceB(config-if)# ip address 10.1.0.22 255.255.0.0
DeviceB(config-if)# no shutdown
DeviceB(config-if)# bfd interval 200 min_rx 200 multiplier 3
DeviceB(config-if)# standby 1 ip 10.0.0.11
DeviceB(config-if)# standby 1 preempt
DeviceB(config-if)# standby 1 priority 90
DeviceB(config-if)# standby 2 ip 10.0.0.12
DeviceB(config-if)# standby 2 preempt
DeviceB(config-if)# standby 2 priority 80
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』

関連項目	マニュアル タイトル
HSRP 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、使用に関する注意事項、および例	『*Cisco IOS First Hop redundancy Protocols Command Reference*』
HSRP for IPv6。	「HSRP for IPv6」のモジュール
HSRP のトラブルシューティング	『Hot Standby Router Protocol: Frequently Asked Questions』

標準

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

MIB

MIB	MIB のリンク
CISCO-HSRP-MIB CISCO-HSRP-EXT-MIB	選択したプラットフォーム、Cisco 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場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	Title
RFC 792	インターネット制御メッセージ プロトコル（*ICMP*）
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	Link
★枠で囲まれた Technical Assistance の場合★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。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。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

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *3* : ***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	15.2(1)S	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。 この機能により、次のコマンドが導入または変更されました。**debugstandbyeventsneighbor**、**showstandby**、**showstandbyneighbors**、**standbybfd**、**standbybfdall-interfaces**。

機能名	リリース	機能情報
FHRP - HSRP グループ シャットダウン	15.2(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。 **standbytrack** および **showstandby** の各コマンドがこの機能によって修正されました。
FHRP - HSRP 複数グループ最適化	15.2(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。 **standbyfollow** および **showstandby** 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。

機能名	リリース	機能情報
FHRP - HSRP の IPv6 サポート	15.2(1)S	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」のモジュールを参照してください。
HSRP - ISSU	15.2(1)S	HSRP--ISSU 機能により、HSRP で ISSU がサポートされています。 インサービス ソフトウェア アップグレード（ISSU）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、計画的なソフトウェア 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、パケット転送中に Cisco IOS ソフトウェアを変更できるため、ネットワークのアベイラビリティが向上し、計画的な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できます。ここでは、ISSU の概念について説明し、システムで ISSU を実行するための手順について説明します。 この機能の詳細については、『*Cisco IOS High Availability Configuration Guide*』の「Cisco IOS In Service Software Upgrade Process」のモジュール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。

機能名	リリース	機能情報
HSRP MD5 認証	15.2(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。 **showstandby** および **standbyauthentication** 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。
ICMP Redirect に対する HSRP サポート	15.2(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。 この機能により、次のコマンドが導入または変更されました。 **debugstandbyevent**、**debugstandbyeventsicmp**、**showstandby**、**standbyredirects**
HSRP の MPLS VPN サポート	15.2(1)S	HSRP のマルチプロトコル ラベル スイッチング（MPLS）バーチャル プライベート ネットワーク（VPN）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 つのプロバイダー エッジ（PE）ルータ間でイーサネット LAN が接続されている場合です。 この機能により、新規追加または変更されたコマンドはありません。

機能名	リリース	機能情報
HSRP バージョン 2	15.2(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 では HSRP バージョン1とは異なるパケットフォーマットを使用します。 **showstandby**、**standbyip**、**standbyversion** 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	15.2(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。 **debugstandbyevents** および **standbysso** 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：アドレス解決プロトコル（ARP）。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メディア アクセス コントロール（MAC）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。

アクティブ デバイス：仮想デバイス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デバイス。

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。

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。

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 デバイスのあるルータ グループを作成します。メインデバイスは、グループの他のデバイスによってモニタされます。メインデバイスに障害が発生すると、これらのスタンバイ HSRP デバイスのいずれかが、メイン デバイスとしての地位と 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、計画的なソフトウェア 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、パケット転送中に Cisco IOS ソフトウェアを変更できるため、ネットワークのアベイラビリティが向上し、計画的なソフトウェア アップグレードによるダウンタイムを短縮できます。

マスター グループ：アクティブ デバイスとスタンバイ デバイス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。

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：ルート プロセッサ。シャーシに搭載される、集中化されたコントロール ユニットの総称です。

RPR：Route Processor Redundancy。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。

スタンバイ グループ：HSRP に参加しているデバイスのうち、共同で仮想デバイスをエミュレートする一連のデバイス。

スタンバイ デバイス：HSRP グループのバックアップ デバイス。

スタンバイ RP：バックアップ RP。

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。

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.AC*xy* 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。

第 5 章

HSRP バージョン 2

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。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

HSRP バージョン 2 について

HSRP バージョン 2 の設計

HSRP バージョン 2 は、バージョン 1 の次の制限に対応するために設計されています。

- HSRP バージョン 1 では、ミリ秒のタイマー値はアドバタイズまたは学習されませんでした。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。
- HSRP バージョン 1 では、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、アクティブな HSRP hello メッセージを使用してメッセージを送信した物理デバイスを特定できませんでした。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。
- マルチキャスト アドレス 224.0.0.2 が HSRP hello メッセージを送信するために使用されます。このアドレスは、シスコ グループ管理プロトコル（CGMP）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 では、HSRP バージョン 1 で使用されていたマルチキャスト アドレス 224.0.0.2 の代わりに、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。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広がっても、インターフェイスが多くの HSRP グループをサポートするわけではありません。グループ番号範囲が拡大することにより、グループ番号がサブインターフェイスの VLAN 番号に一致するようになりました。

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 では HSRP バージョン 1 とは異なるパケット フォーマットを使用します。パケット フォーマットは Type-Length-Value（TLV）です。HSRP バージョン 1 のデバイスが受信した 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、ゲートウェイ ロード バランシング プロトコル（GLBP）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 の同じ制限が解消されます。GLBP の詳細については、『*Configuring GLBP*』を参照してください。

ジッター タイマー

ジッター タイマーは、HSRP で使用されます。これらはリアルタイムで機能し拡張するサービスで動作するタイマーに推奨されます。ジッター タイマーは、HSRP グループ操作のバンチングの可能性を減らすことによって HSRP とその他の FHRP プロトコルの信頼性を大幅に改善し、CPU とネットワーク トラフィックのスパイクを削減することを意図しています。HSRP の場合、特定のデバイスで最大 4,000 の運用グループを構成することができます。デバイスやネットワークへ

の負荷を分散するために、HSRP タイマーはジッターを使用します。特定のタイマー インスタンスでは、設定した値よりも最大20%多くかかる場合があります。たとえば、15秒に設定されているホールド時間の場合、実際のホールド時間は 18 秒かかることがあります。

HSRP では、Hello タイマー（Hello パケットを送信する）は負のジッターを持ち、ホールドダウンタイマー（ピア障害をチェックする）は正のジッターを持ちます。

HSRP バージョン 2 の設定方法

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 では HSRP バージョン 1 とは異なるパケット フォーマットを使用します。

（注）

- 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。どちらのバージョンも相互に排他的なので、インターフェイスはバージョン 1 およびバージョン 2 の両方を運用できません。しかし、同一デバイスの異なる物理インターフェイス上であれば、異なるバージョンを実行できます。バージョン 1 で認められるグループ番号範囲（0 ～ 255）を超えるグループを設定している場合は、バージョン 2 からバージョン 1 への変更はできません。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **interface***typenumber*
4. **ipaddress***ip-addressmask*
5. **standbyversion** {**1** | **2**}
6. **standby** [*group-number*] **ip** [*ip-address* [**secondary**]]
7. **end**
8. **showstandby**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化	特権 EXEC モードをイネーブルにします。

	コマンドまたはアクション	目的
	例： `Device> enable`	• パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# 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***typenumber* 例： `Device(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。
ステップ 4	**ipaddress***ip-addressmask* 例： `Device(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	**standbyversion** {**1** | **2**} 例： `Device(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： `Device(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 です。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： `Device(config-if)# end`	現在のコンフィギュレーションセッションを終了して、特権 EXEC モードに戻ります。
ステップ 8	**showstandby** 例： `Device# show standby`	（任意）HSRP 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）。

HSRP バージョン 2 の設定例

例：HSRP バージョン 2 の設定

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。

```
Device(config)# interface vlan 350
Device(config-if)# standby version 2
Device(config-if)# standby 350 priority 110
Device(config-if)# standby 350 preempt
Device(config-if)# standby 350 timers 5 15
Device(config-if)# standby 350 ip 172.20.100.10
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
HSRP 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、使用に関する注意事項、および例	『*Cisco IOS First Hop redundancy Protocols Command Reference*』
HSRP for IPv6。	「HSRP for IPv6」のモジュール
HSRP のトラブルシューティング	『Hot Standby Router Protocol: Frequently Asked Questions』

標準

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

MIB

MIB	MIB のリンク
CISCO-HSRP-MIB CISCO-HSRP-EXT-MIB	選択したプラットフォーム、Cisco 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場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	Title
RFC 792	インターネット制御メッセージ プロトコル（*ICMP*）
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	Link
★枠で囲まれた Technical Assistance の場合★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。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。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 バージョン 2 の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *4*：*HSRP* バージョン *2* の機能情報

機能名	リリース	機能情報
HSRP バージョン 2	Cisco IOS XE Release 2.1 Cisco IOS XE Release 3.5S Cisco IOS XE Release 3.9S	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 では HSRP バージョン 1 とは異なるパケットフォーマットを使用します。 Cisco IOS XE Release 3.5S では、Cisco ASR 903 ルータのサポートが追加されました。 **showstandby**、**standbyip**、**standbyversion** 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。

第 6 章

HSRP MD5 認証

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。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

HSRP MD5 認証に関する情報

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、デバイス A のプライオリティが 120 で、これがアクティブ デバイスであるとします。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、デバイス A はアクティブ デバイスとしての動作を停止します。デバイス 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、デバイス A はアクティブ デバイスのままです。

HSRP パケットが拒否されるのは、次のいずれかの場合です。

- 認証方式がデバイスと着信パケットの間で異なっている。
- テキスト認証文字列がデバイスと着信パケットで異なる。

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 認証を使用すると、別のプレーン テキスト認証方式よりもセキュリティを強化できます。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で直接指定するか、またはキー チェーンを使用して間接的に指定できます。

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、デバイス A のプライオリティが 120 で、これがアクティブ デバイスであるとします。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、デバイス A はアクティブ デバイスとしての動作を停止します。デバイス 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、デバイス A はアクティブ デバイスのままです。

HSRP パケットが拒否されるのは、次のいずれかの場合です。

- 認証方式がデバイスと着信パケットの間で異なっている。
- MD5 ダイジェストがデバイスと着信パケットで異なる。
- テキスト認証文字列がデバイスと着信パケットで異なる。

HSRP MD5 認証の設定方法

キー チェーンを使用した HSRP MD5 認証の設定

キー チェーンを使用して HSRP 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 チェーン設定に従って異なる時点で異なるキー 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. イネーブル化
2. **configureterminal**
3. **keychain***name-of-chain*
4. **key***key-id*
5. **key-string***string*
6. **exit**
7. **exit**
8. **interface***typenumber*
9. **ipaddress***ip-addressmask* [**secondary**]
10. **standby** [*group-number*] **priority***priority*
11. **standby** [*group-number*] **preempt** [**delay** {**minimum** | **reload** | **sync**} *seconds*]
12. **standby** [*group-number*] **authenticationmd5key-chain***key-chain-name*
13. **standby** [*group-number*] **ip** [*ip-address* [*secondary*]]
14. 通信する各デバイスに対してステップ 1 ～ 12 を繰り返します。
15. **end**
16. **showstandby**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： `Device# 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	**keychain***name-of-chain* 例： `Device(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、キー チェーン キー 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	**key***key-id* 例： `Device(config-keychain)# key 100`	キーチェーンの認証キーを識別し、キーチェーンキーコンフィギュレーション モードを開始します。 • *key-id* 引数の値には数値を指定する必要があります。
ステップ 5	**key-string***string* 例： `Device(config-keychain-key)# key-string mno172`	キーの認証文字列を指定します。 • *string* 引数の値は、1 ～ 80 文字の大文字または小文字の英数字を指定できます。最初の文字には数字を使用できません。
ステップ 6	**exit** 例： `Device(config-keychain-key)# exit`	キー チェーン キー 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： `Device(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***typenumber* 例： `Device(config)# interface GigabitEthernet 0/0/0`	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 9	**ipaddress***ip-addressmask* [**secondary**] 例： `Device(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。

	コマンドまたはアクション	目的
ステップ 10	**standby** [*group-number*] **priority***priority* 例： `Device(config-if)# standby 1 priority 110`	HSRP プライオリティを設定します。
ステップ 11	**standby** [*group-number*] **preempt** [**delay** {**minimum** | **reload** | **sync**} *seconds*] 例： `Device(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 12	**standby** [*group-number*] **authenticationmd5key-chain***key-chain-name* 例： `Device(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 で指定した名前に一致する必要があります。
ステップ 13	**standby** [*group-number*] **ip** [*ip-address* [*secondary*]] 例： `Device(config-if)# standby 1 ip 10.21.8.12`	HSRP をアクティブにします。
ステップ 14	通信する各デバイスに対してステップ 1 ～ 12 を繰り返します。	—
ステップ 15	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 16	**showstandby** 例： `Device# show standby`	（任意）HSRP 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. イネーブル化
2. **debugstandbyerrors**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**debugstandbyerrors** 例： `Device# 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。

例

次の例では、デバイス A には MD5 テキスト文字列認証が設定されていますが、デバイス B にはデフォルトのテキスト認証が設定されています。

```
Device# 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、デバイス A とデバイス B の両方に別々の MD5 認証文字列が設定されています。

```
Device# 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. イネーブル化
2. **configureterminal**
3. **interface***typenumber*
4. **ipaddress***ip-addressmask* [**secondary**]
5. **standby** [*group-number*] **priority***priority*
6. **standby** [*group-number*] **preempt** [**delay** {**minimum** | **reload** | **sync**} *seconds*]
7. **standby** [*group-number*] **authenticationtext***string*
8. **standby** [*group-number*] **ip** [*ip-address* [**secondary**]]
9. 通信する各デバイスに対してステップ 1 ～ 8 を繰り返します。
10. **end**
11. **showstandby**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# 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***typenumber* 例： `Device(config)# interface GigabitEthernet 0/0/0`	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	**ipaddress***ip-addressmask* [**secondary**] 例： `Device(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。

	コマンドまたはアクション	目的
ステップ 5	**standby** [*group-number*] **priority***priority* 例： `Device(config-if)# standby 1 priority 110`	HSRP プライオリティを設定します。
ステップ 6	**standby** [*group-number*] **preempt** [**delay** {**minimum** | **reload** | **sync**} *seconds*] 例： `Device(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*] **authenticationtext***string* 例： `Device(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： `Device(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	通信する各デバイスに対してステップ 1 ～ 8 を繰り返します。	--
ステップ 10	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 11	**showstandby** 例： `Device# show standby`	（任意）HSRP 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 認証の設定例

例：キー ストリングを使用した HSRP MD5 認証の設定

```
Device(config)# interface GigabitEthernet 0/0/0
Device(config-if)# standby 1 priority 110
Device(config-if)# standby 1 preempt
Device(config-if)# standby 1 authentication md5 key-string 54321098452103ab timeout 30
Device(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、HSRP にはキー チェーン「hsrp1」が必要です。

```
Device(config)# key chain hsrp1
Device(config-keychain)# key 1
Device(config-keychain-key)# key-string 54321098452103ab
Device(config-keychain-key)# exit
Device(config)# interface GigabitEthernet 0/0/0
Device(config-if)# standby 1 priority 110
Device(config-if)# standby 1 preempt
Device(config-if)# standby 1 authentication md5 key-chain hsrp1
Device(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 認証の設定

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。

デバイス 1

```
Device(config)# key chain hsrp1
Device(config-keychain)# key 0
Device(config-keychain-key)# key-string 54321098452103ab
Device(config-keychain-key)# exit
Device(config)# interface GigabitEthernet 0/0/0
Device(config-if)# standby 1 authentication md5 key-chain hsrp1
Device(config-if)# standby 1 ip 10.21.0.10
```

デバイス 2

```
Device(config)# interface GigabitEthernet 0/0/0
Device(config-if)# standby 1 authentication md5 key-string 54321098452103ab
Device(config-if)# standby 1 ip 10.21.0.10
```

例：HSRP テキスト認証の設定

```
Device(config)# interface GigabitEthernet 0/0/0
Device(config-if)# standby 1 priority 110
Device(config-if)# standby 1 preempt
Device(config-if)# standby 1 authentication text company2
Device(config-if)# standby 1 ip 10.21.0.10
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
HSRP 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、使用に関する注意事項、および例	『*Cisco IOS First Hop redundancy Protocols Command Reference*』
HSRP for IPv6。	「HSRP for IPv6」のモジュール
HSRP のトラブルシューティング	『Hot Standby Router Protocol: Frequently Asked Questions』

標準

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

MIB

MIB	MIB のリンク
CISCO-HSRP-MIB CISCO-HSRP-EXT-MIB	選択したプラットフォーム、Cisco 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場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	Title
RFC 792	インターネット制御メッセージ プロトコル（*ICMP*）
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	Link
★枠で囲まれた Technical Assistance の場合★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。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。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 MD5 認証の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *5*：*HSRP MD5* 認証の機能情報

機能名	リリース	機能情報
HSRP MD5 認証	12.2(25)S 12.2(33)SRA 12.2(33)SXH 12.2(50)SY 12.3(2)T 15.0(1)S 15.0(1)SY Cisco IOS XE Release 2.1 Cisco IOS XE 3.1.0SG Cisco IOS XE Release 3.9S	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。 **showstandby** および **standbyauthentication** 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。

第 7 章

ICMP Redirect に対する HSRP サポート

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。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

ICMP リダイレクトの HSRP サポートについて

ICMP リダイレクト メッセージの HSRP サポート

デフォルトでは、Internet Control Message Protocol（ICMP）リダイレクト メッセージの HSRP フィルタリングは、HSRP が実行されているデバイスでイネーブルになっています。

ICMP は、エラーをレポートするためのメッセージ パケットや IP 処理に関連する他の情報を提供する、ネットワーク層インターネット プロトコルです。ICMP は、ホストにエラー パケットとリダイレクト パケットを送信できます。

HSRP を実行しているときは、HSRP グループに属するデバイス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 によってホストがデバイスの実際の IP アドレスにリダイレクトされた場合、そのデバイス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。

HSRP が設定されたインターフェイスでは、ICMP リダイレクト メッセージが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 デバイスへの ICMP リダイレクト

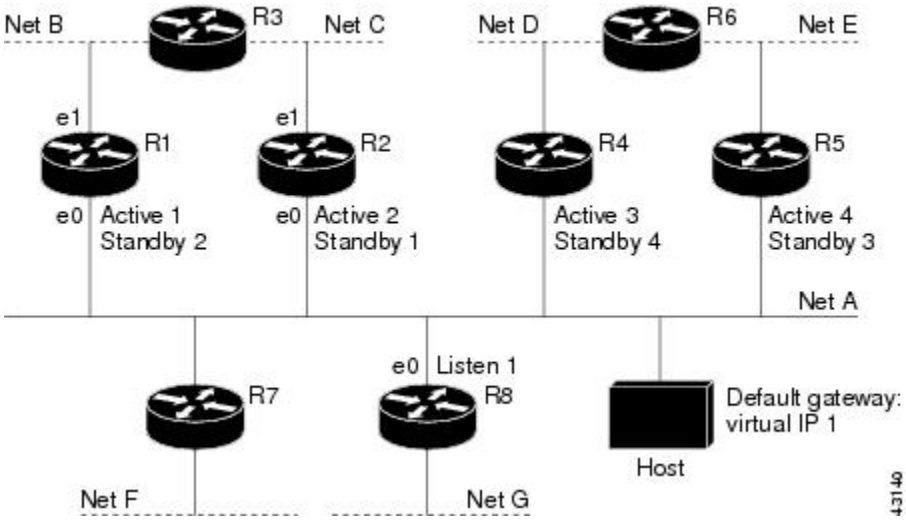
ネクストホップ IP アドレスは、そのネットワーク上のアクティブな HSRP デバイスのリストと比較され、一致が見つかると、実際のネクストホップ IP アドレスが対応する仮想 IP アドレスに置き換えられ、リダイレクト メッセージの続行が許可されます。

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デバイスが HSRP を実行していない場合だけです。パッシブ HSRP デバイスへのリダイレクトは許可されません（パッシブ HSRP デバイスとは、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デバイスです）。

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デバイスには、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 デバイス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 デバイスはネットワークの HSRP パケットをすべてスヌーピングして、アクティブ デバイスのリスト（仮想 IP アドレスと実際の IP アドレス）を管理します。

下の図に示されている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 6 : *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
```

デバイス R1 は、このパケットを受信し、デバイス 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、デバイス 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）。

デバイス 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、デバイス R1 の HSRP プロセスでデバイス R4 がグループ 3 のアクティブ HSRP デバイス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 ホップがデバイス 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。

2 つの変更されたフィールド（*）を示す変更された ICMP リダイレクト メッセージは次のようになります。

```
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 デバイスへの ICMP リダイレクト

パッシブ HSRP デバイスへの ICMP リダイレクトは許可されません。ホストが HSRP デバイスの実際の IP アドレスが検出されると、冗長性が失われる可能性があります。

「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」の図では、デバイス R8 へのリダイレクションは、R8 がパッシブ デバイスのため、許可されます。この場合、ホストからネット D へのパケットは、まずデバイス R1 に到着した後、デバイス 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 デバイス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 リダイレクションが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上のすべてのデバイスに、少なくとも 1 つのアクティブな HSRP グループが含まれている必要があります。

非 HSRP デバイスへの ICMP リダイレクト

ローカル インターフェイスで HSRP を実行していないデバイスへの ICMP リダイレクトは許可されます。非 HSRP デバイスの実際の 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。

「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」の図では、デバイス R7 へのリダイレクションは、R7 が HSRP を実行していないため、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、**nostandbyredirectunknown** コマンドを使用します。

パッシブ HSRP アドバタイズメント メッセージ

パッシブ HSRP デバイスは、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 デバイスが、ネットワークにある任意の HSRP デバイスの 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 デバイスに伝えます。

- アクティブ：インターフェイスには少なくとも 1 つのアクティブなグループがあります。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。
- 休止：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。
- パッシブ：インターフェイスには少なくとも 1 つの非アクティブなグループがあり、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。

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、**standbyredirecttimers** 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 デバイスが、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 デバイス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 **standbyuse-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 デバイス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。

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 デバイスは送信先 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。HSRP デバイスが複数の IP アドレスに同じ 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 アドレスを一意に判別することができなくなるので、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 **debugstandbyeventsicmp** 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 10.0.0.4 for dest 10.0.1.2
10:43:08: HSRP: could not uniquely determine IP address for mac 00d0.bbd3.bc22
```

ICMP リダイレクトの HSRP サポートの設定方法

ICMP リダイレクト メッセージの HSRP 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 が実行されているデバイス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、デバイス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. イネーブル化
2. **configureterminal**
3. **interface***typenumber*
4. **standbyredirect** [**timers***advertisementholddown*] [**unknown**]
5. **end**
6. **showstandbyredirect** [*ip-address*] [*interface-typeinterface-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	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# 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***typenumber* 例： `Device(config)# interface GigabitEthernet 0/0/0`	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	**standbyredirect** [**timers***advertisementholddown*] [**unknown**] 例： `Device(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

	コマンドまたはアクション	目的
		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： `Device(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 6	**showstandbyredirect** [*ip-address*] [*interface-typeinterface-number*] [**active**] [**passive**] [**timers**] 例： `Device# 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。

ICMP リダイレクトの HSRP サポートの設定例

例：ICMP リダイレクト メッセージの HSRP サポートの設定

デバイス 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

```
Device(config)# interface GigabitEthernet 0/0/0
Device(config-if)# ip address 10.0.0.10 255.0.0.0
Device(config-if)# standby redirect
Device(config-if)# standby 1 priority 120
Device(config-if)# standby 1 preempt delay minimum 20
Device(config-if)# standby 1 ip 10.0.0.1
Device(config-if)# standby 2 priority 105
Device(config-if)# standby 2 preempt delay minimum 20
Device(config-if)# standby 2 ip 10.0.0.2
```

デバイス 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

```
Device(config)# interface GigabitEthernet 0/0/0
Device(config-if)# ip address 10.0.0.11 255.0.0.0
Device(config-if)# standby redirect
Device(config-if)# standby 1 priority 105
Device(config-if)# standby 1 preempt delay minimum 20
Device(config-if)# standby 1 ip 10.0.0.1
Device(config-if)# standby 2 priority 120
Device(config-if)# standby 2 preempt delay minimum 20
Device(config-if)# standby 2 ip 10.0.0.2
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
HSRP 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、使用に関する注意事項、および例	『*Cisco IOS First Hop redundancy Protocols Command Reference*』
HSRP for IPv6。	「HSRP for IPv6」のモジュール
HSRP のトラブルシューティング	『Hot Standby Router Protocol: Frequently Asked Questions』

標準

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

MIB

MIB	MIB のリンク
CISCO-HSRP-MIB CISCO-HSRP-EXT-MIB	選択したプラットフォーム、Cisco 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場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	Title
RFC 792	インターネット制御メッセージ プロトコル（*ICMP*）

RFC	Title
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	Link
★枠で囲まれた Technical Assistance の場合★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。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。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

ICMP リダイレクトの HSRP サポートの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *6*：*ICMP* リダイレクトの *HSRP* サポートの機能情報

機能名	リリース	機能情報
ICMP Redirect に対する HSRP サポート	12.1(3)T 12.2(50)SY 15.0(1)S 15.0(1)SY Cisco IOS XE Release 2.1 Cisco IOS XE Release 3.9S	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。 この機能により、次のコマンドが導入または変更されました。 **debugstandbyevent**、**debugstandbyeventsicmp**、**showstandby**、**standbyredirects**

第 8 章

FHRP：HSRP 複数グループ最適化

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。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

FHRP に関する情報：複数グループの最適化

HSRP 複数グループ最適化

同じ物理インターフェイス上で、数百ものサブインターフェイスがそれぞれ独自の HSRP グループを持つ構成は、複数の HSRP グループのネゴシエーションとメンテナンスのプロセスが発生して、ネットワーク トラフィックと CPU 使用率に悪影響を与える可能性があります。

アクティブ デバイスとスタンバイ デバイス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デバイス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。

FHRP の設定方法：複数のグループの最適化

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、冗長デバイスを余すところなく活用できるようになります。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デバイスは、別のグループに対してスタンバイ ステートやリッスン ステートになることができます。

2 台のデバイスを使用している場合、デバイス 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、デバイス 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。図と設定例については、「例：ロード バランシング用の複数の HSRP グループの設定」を参照してください。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **interface***typenumber*
4. **ipaddress***ip-addressmask* [**secondary**]
5. **standby** [*group-number*] **priority***priority*
6. **standby** [*group-number*] **preempt** [**delay** {**minimum** | **reload** | **sync**} *delay*]
7. **standby** [*group-number*] **ip** [*ip-address*] **secondary**]
8. 同じデバイスでステップ 5 ～ 7 を繰り返して、別のスタンバイ グループのデバイス属性を設定します。
9. **exit**
10. もう 1 つのデバイスでステップ 3 ～ 9 を繰り返します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# 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***typenumber* 例： `Device(config)# interface GigabitEthernet 0/0/0`	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	**ipaddress***ip-addressmask* [**secondary**] 例： `Device(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： `Device(config-if)# standby 1 priority 110`	HSRP プライオリティを設定します。

	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** | **reload** | **sync**} *delay*] 例： `Device(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： `Device(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	同じデバイスでステップ 5 ～ 7 を繰り返して、別のスタンバイ グループのデバイス属性を設定します。	たとえば、デバイス A をグループ 1 のアクティブ デバイス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 デバイスまたはスタンバイ デバイスとして設定することができます。
ステップ 9	**exit** 例： `Device(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 つのデバイスでステップ 3 ～ 9 を繰り返します。	もう 1 つのデバイスで複数の 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

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。

standbyfollow 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。

standbymac-refresh*seconds* コマンドを使用して、HSRP クライアント グループの更新間隔を直接変更します。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。

（注）

- 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。

```
Device(config-if)# standby 1 priority 110
%Warning: This setting has no effect while following another group.
Device(config-if)# standby 1 timers 5 15
    % Warning: This setting has no effect while following another group.
Device(config-if)# standby 1 preempt delay minimum 300
    % Warning: This setting has no effect while following another group.
```

はじめる前に

「ロード バランシング用の複数の HSRP グループの設定」セクションのステップを使用して、HSRP グループのマスター グループを設定します。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **interface***typenumber*
4. **ipaddress***ip-addressmask* [**secondary**]
5. **standbymac-refresh***seconds*
6. **standby***group-number***follow***group-name*
7. **exit**
8. 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	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# 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***typenumber* 例： `Device(config)# interface GigabitEthernet 0/0/0`	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	**ipaddress***ip-addressmask* [**secondary**] 例： `Device(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	**standbymac-refresh***seconds* 例： `Device(config-if)# standby mac-refresh 30`	HSRP クライアント グループの更新間隔を設定します。
ステップ 6	**standby***group-number***follow***group-name* 例： `Device(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 7	**exit** 例： `Device(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 8	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。

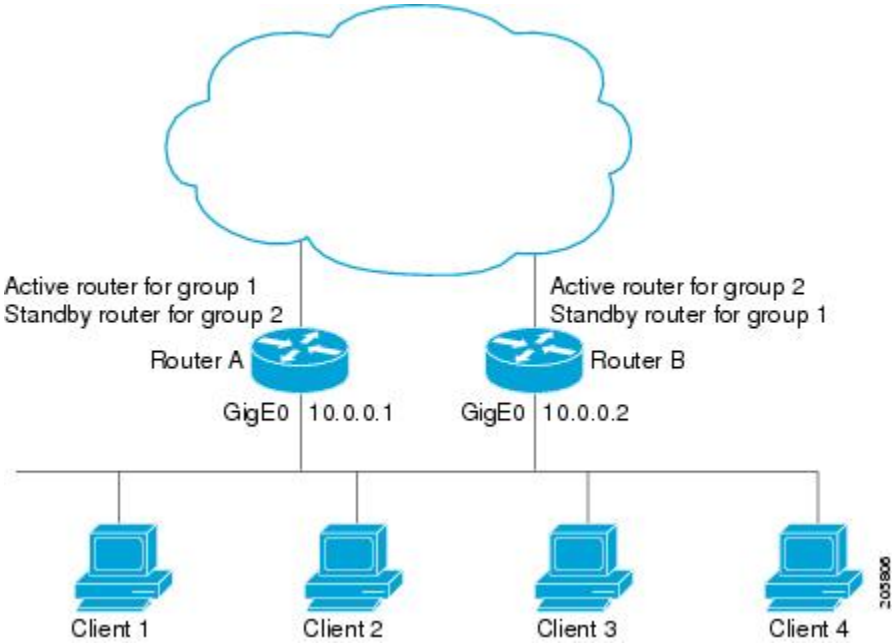
FHRP の設定例：複数グループ最適化

例：ロード バランシング用の複数の HSRP グループの設定

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。下の図では、半分のクライアントがルータ A に設定されており、もう半分はルータ B に設定されています。ルータ A およびルータ B の設定により、合計 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 に最高のプライオリティが割り当てられているので、ルータ A がデフォルトのアクティブ ルータになり、ルータ B がスタンバイ ルータとなります。

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。通常の運用では、2 つのルータが IP トラフィック負荷を分散します。いずれかのルータが使用できなくなると、もう一方のルータがアクティブになり、使用できない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 **standbypreempt** が必要です。

図 *7*：*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
!
Router(config)# interface GigabitEthernet 0/0/0
Router(config-if)# ip address 10.0.0.1 255.255.255.0
Router(config-if)# standby 1 priority 110
Router(config-if)# standby 1 preempt
Router(config-if)# standby 1 ip 10.0.0.3
Router(config-if)# standby 2 preempt
Router(config-if)# standby 2 ip 10.0.0.4
```

ルータ B の設定

```
Router(config)# hostname RouterB
!
Router(config)# interface GigabitEthernet 0/0/0
```

```
Router(config-if)# ip address 10.0.0.2 255.255.255.0
Router(config-if)# standby 1 preempt
Router(config-if)# standby 1 ip 10.0.0.3
Router(config-if)# standby 2 priority 110
Router(config-if)# standby 2 preempt
Router(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。

```
Device(config)# interface GigabitEthernet 0/0/0
Device(config-if)# no shutdown
Device(config-if)# standby mac-refresh 30
! Client Hello message interval
!
Device(config)# interface GigabitEthernet 0/0/1
Device(config-if)# no shutdown
Device(config-if)# ip vrf forwarding VRF2
Device(config-if)# ip address 10.0.0.100 255.255.0.0
Device(config-if)# standby 1 ip 10.0.0.254
Device(config-if)# standby 1 priority 110
Device(config-if)# standby 1 preempt
Device(config-if)# standby 1 name HSRP1
!Server group
!
Device(config)# interface GigabitEthernet 0/0/2
Device(config-if)# no shutdown
Device(config-if)# ip vrf forwarding VRF3
Device(config-if)# ip address 10.0.0.100 255.255.0.0
Device(config-if)# standby 2 ip 10.0.0.254
Device(config-if)# standby 2 follow HSRP1
! Client group
!
Device(config)# interface GigabitEthernet 0/0/3
Device(config-if)# no shutdown
Device(config-if)# ip vrf forwarding VRF4
Device(config-if)# ip address 10.0.0.100 255.255.0.0
Device(config-if)# standby 2 ip 10.0.0.254
Device(config-if)# standby 2 follow HSRP1
! Client group
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
HSRP 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、使用に関する注意事項、および例	『*Cisco IOS First Hop redundancy Protocols Command Reference*』
HSRP for IPv6。	「HSRP for IPv6」のモジュール

関連項目	マニュアル タイトル
HSRP のトラブルシューティング	『Hot Standby Router Protocol: Frequently Asked Questions』

標準

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

MIB

MIB	MIB のリンク
CISCO-HSRP-MIB CISCO-HSRP-EXT-MIB	選択したプラットフォーム、Cisco 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場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	Title
RFC 792	インターネット制御メッセージ プロトコル（*ICMP*）
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	Link
★枠で囲まれた Technical Assistance の場合★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。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。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

FHRP の機能情報：HSRP 複数グループ最適化

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *7*：***FHRP - HSRP*** 複数グループ最適化の機能情報

機能名	リリース	機能情報
FHRP - HSRP 複数グループ最適化	12.4(6)T 12.2(33)SRB 12.2(33)SXI 12.2(50)SY 15.0(1)S 15.0(1)SY Cisco IOS XE Release 2.1	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 デバイスとスタンバイ デバイス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。 **standbyfollow** および **showstandby** 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。

第 9 章

『FHRP - HSRP Group Shutdown』

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。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

FHRP に関する情報：HSRP グループ シャットダウン

オブジェクト トラッキングが HSRP デバイスのプライオリティに及ぼす影響

デバイスがオブジェクト トラッキング対応として設定されていて、なおかつトラッキング対象のオブジェクトがダウンした場合、デバイスのプライオリティはダイナミックに変更されます。トラッキング プロセスは定期的に、トラッキング対象オブジェクトをポーリングし、値の変更を確認します。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。よりプライオリティの高いHSRPデバイスは、**standbypreempt** コマンドが設定されている場合にはアクティブなデバイスになることができます。

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。デバイスがオブジェクト トラッキング対応として設定されていて、なおかつトラッキング対象のオブジェクトがダウンした場合、デバイスのプライオリティはダイナミックに変更されます。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。

HSRP、仮想ルータ冗長プロトコル（VRRP）、Gateway Load Balancing Protocol（GLBP）などのクライアントプロセスで、トラッキング オブジェクトに対する興味を登録し、追跡対象オブジェクトの状態が変化したときに通知を受け取るようにすることができます。

オブジェクト トラッキングの詳細については、『Configuring Enhanced Object Tracking』を参照してください。

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 **standbytrack** 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、**nostandbytrack** 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 **standbytrack** 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。

FHRP の設定方法：HSRP グループのシャットダウン

HSRP 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。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **track***object-number***interface***typenumber* {**line-protocol** | **iprouting**}
4. **exit**
5. **interface***typenumber*
6. **standby** [*group-number*] **track***object-number* [**decrement***priority-decrement*] [**shutdown**]
7. **standby** [*group-number*] **ip** [*ip-address* [**secondary**]]
8. **end**
9. **showtrack** [*object-number* | **brief**] [**interface** [**brief**] | **iproute** [**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	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# 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***object-number***interface***typenumber* {**line-protocol** | **iprouting**} 例： `Device(config)# track 100 interface GigabitEthernet 0/0/0 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： `Device(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	**interface***typenumber* 例： `Device(config)# interface GigabitEthernet 0/0/0`	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 6	**standby** [*group-number*] **track***object-number* [**decrement***priority-decrement*] [**shutdown**] 例： `Device(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、デバイス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。 • トラッキング対象のオブジェクトがダウンしたときにデバイスの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。

	コマンドまたはアクション	目的
		（注） 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、**nostandbytrack** 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 **standbytrack** 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。
ステップ 7	**standby** [*group-number*] **ip** [*ip-address* [**secondary**]] 例： `Device(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 8	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 9	**showtrack** [*object-number* | **brief**] [**interface** [**brief**] | **iproute** [**brief**] | **resolution** | **timers**] 例： `Device# 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

（注） 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、受信側のデバイスの 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。

（注） あるグループのデバイスのキー ストリングを変更する場合、アクティブ デバイスを最後に変更して、HSRP ステートが変化しないようにします。アクティブ デバイスのキー ストリングの変更は、アクティブでないデバイスの後、インターフェイス コンフィギュレーション コマンド **standytimers** 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、アクティブでないデバイスでアクティブ デバイスのタイムアウトが発生することがなくなります。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **terminalinterface***typenumber*
4. **ipaddress***ip-addressmask* [**secondary**]
5. **standby** [*group-number*] **priority***priority*
6. **standby** [*group-number*] **preempt** [**delay** {**minimum** | **reload** | **sync**} *seconds*]
7. **standby** [*group-number*] **authenticationmd5key-string** [**0** | **7**] *key* [**timeout***seconds*]
8. **standby** [*group-number*] **ip** [*ip-address*] [**secondary**]]
9. 通信する各デバイスに対してステップ 1 ～ 8 を繰り返します。
10. **end**
11. **showstandby**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# 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	**terminalinterface***typenumber* 例： `Device(config)# interface GigabitEthernet 0/0/0`	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。

	コマンドまたはアクション	目的
ステップ 4	**ipaddress***ip-addressmask* [**secondary**] 例： `Device(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： `Device(config-if)# standby 1 priority 110`	HSRP プライオリティを設定します。
ステップ 6	**standby** [*group-number*] **preempt** [**delay** {**minimum** | **reload** | **sync**} *seconds*] 例： `Device(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*] **authenticationmd5key-string** [**0** | **7**] *key* [**timeout***seconds*] 例： `Device(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* 引数の長さは、最大 64 文字です。16 文字以上を使用することをお勧めします。 • *key* 引数にはプレフィッ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。**servicepassword-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場合、key-string 認証キーは自動的に暗号化されます。 • **timeout** 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： `Device(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	通信する各デバイスに対してステップ 1 ～ 8 を繰り返します。	—

	コマンドまたはアクション	目的
ステップ 10	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 11	**showstandby** 例： `Device# show standby`	（任意）HSRP 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）。

FHRP の設定例：HSRP グループのシャットダウン

例：HSRP オブジェクト トラッキングの設定

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。ギガビット イーサネット インターフェイス 0/0/0 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、デバイス A はデバイス B よりもプライオリティが高いので、デバイス A が HSRP アクティブ デバイスになります。ただし、デバイス 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デバイス B がアクティブ デバイス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。

デバイス A の設定

```
Device(config)# track 100 interface serial 1/0/0 ip routing
!
Device(config)# interface GigabitEthernet 0/0/0
Device(config-if)# ip address 10.1.0.21 255.255.0.0
Device(config-if)# standby 1 preempt
Device(config-if)# standby 1 priority 110
Device(config-if)# standby 1 track 100 decrement 10
Device(config-if)# standby 1 ip 10.1.0.1
```

デバイス B の設定

```
Device(config)# track 100 interface serial 1/0/0 ip routing
!
```

```
Device(config)# interface GigabitEthernet 0/0/0
Device(config-if)# ip address 10.1.0.22 255.255.0.0
Device(config-if)# standby 1 preempt
Device(config-if)# standby 1 priority 105
Device(config-if)# standby 1 track 100 decrement 10
Device(config-if)# standby 1 ip 10.1.0.1
```

例：HSRP グループ シャットダウンの設定

次の例では、トラッキング プロセスはギガビット イーサネット インターフェイス 0/0/0 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。ギガビット イーサネット インターフェイス 0/0/1 の HSRP は、ギガビット イーサネット インターフェイス 0/0/0 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。ギガビット イーサネット インターフェイス 0/0/0 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。

両方のギガビット イーサネット インターフェイスが動作している場合は、デバイス A はデバイス B よりもプライオリティが高いので、デバイス A が HSRP アクティブ デバイスになります。ただし、デバイス A のギガビット イーサネット インターフェイス 0/0/0 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デバイス B がアクティブ デバイス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。

デバイス A の設定

```
Device(config)# track 100 interface GigabitEthernet 0/0/0 ip routing
!
Device(config)# interface GigabitEthernet 0/0/1
Device(config-if)# ip address 10.1.0.21 255.255.0.0
Device(config-if)# standby 1 ip 10.1.0.1
Device(config-if)# standby 1 preempt
Device(config-if)# standby 1 priority 110
Device(config-if)# standby 1 track 100 shutdown
```

デバイス B の設定

```
Device(config)# track 100 interface GigabitEthernet 0/0/0 ip routing
!
Device(config)# interface GigabitEthernet 0/0/1
Device(config-if)# ip address 10.1.0.22 255.255.0.0
Device(config-if)# standby 1 ip 10.1.0.1
Device(config-if)# standby 1 preempt
Device(config-if)# standby 1 priority 105
Device(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、**nostandbytrack** 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 **standbytrack** 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。

```
Device(config)# no standby 1 track 100 decrement 10
Device(config)# standby 1 track 100 shutdown
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
HSRP 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、使用に関する注意事項、および例	『*Cisco IOS First Hop redundancy Protocols Command Reference*』
HSRP for IPv6。	「HSRP for IPv6」のモジュール
HSRP のトラブルシューティング	『Hot Standby Router Protocol: Frequently Asked Questions』

標準

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

MIB

MIB	MIB のリンク
CISCO-HSRP-MIB CISCO-HSRP-EXT-MIB	選択したプラットフォーム、Cisco 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場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	Title
RFC 792	インターネット制御メッセージ プロトコル（*ICMP*）

RFC	Title
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	Link
★枠で囲まれた Technical Assistance の場合★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。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。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

FHRP の機能情報：HSRP グループ シャットダウン

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *8*：*FHRP - HSRP* グループ シャットダウンの機能情報

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 12.2(50)SY 15.0(1)S 15.0(1)SY Cisco IOS XE Release 2.1	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。 **standbytrack** および **showstandby** の各コマンドがこの機能によって修正されました。

第 10 章

SSO HSRP

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。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

SSO HSRP の制約事項

- 拡張オブジェクト トラッキング（EOT）は、ステートフルスイッチオーバー（SSO）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。

SSO HSRP について

SSO HSRP

SSO HSRP は、冗長なルート プロセッサ（RP）を装備したデバイスがステートフル スイッチオーバー（SSO）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 デバイスの両方の RP に障害が発生しても、スタンバイ状態の HSRP デバイスが HSRP アクティブ デバイス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 Cisco 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 ノンストップ フォワーディング（NSF）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 機能により、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 デバイスを通じて引き続き転送されます。

SSO HSRP 機能が登場する前は、アクティブ デバイスのプライマリ 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 スイッチとして処理を引き継ぐ、グループの別のスイッチ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 デバイスで 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 デバイスにスイッチ 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、**nostandbysso** 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。

SSO HSRP の設定方法

SSO 対応 HSRP のイネーブル化

SSO 対応 HSRP 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、**nostandbysso** 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. イネーブル化
2. **configureterminal**
3. 冗長性
4. **modesso**
5. **exit**
6. **nostandbysso**
7. **standbysso**
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	**イネーブル化** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# 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	**冗長性** 例： `Device(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	**modesso** 例： `Device(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。 • 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： `Device(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。
ステップ 6	**nostandbysso** 例： `Device(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	**standbysso** 例： `Device(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： `Device(config)# end`	現在のコンフィギュレーションセッションを終了して、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. **showstandby**
2. **debugstandbyeventsha**

手順の詳細

ステップ 1 **showstandby**

showstandby 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。

例：

```
Device# show standby

GigabitEthernet0/0/0 - Group 1
 State is Active (standby RP)
 Virtual IP address is 10.1.0.7
 Active virtual MAC address is unknown
  Local virtual MAC address is 000a.f3fd.5001 (bia)
 Hello time 1 sec, hold time 3 sec
 Authentication text “authword”
 Preemption enabled
 Active router is unknown
 Standby router is unknown
 Priority 110 (configured 120)
  Track object 1 state Down decrement 10
 Group name is “name1” (cfgd)
```

ステップ 2 **debugstandbyeventsha**

debugstandbyeventsha 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。

例：

```
Device# debug standby events ha

!Active RP
*Apr 27 04:13:47.755: HSRP: Gi0/0/1 Grp 101 RF Encode state Listen into sync buffer
*Apr 27 04:13:47.855: HSRP: CF Sync send ok
*Apr 27 04:13:57.755: HSRP: Gi0/0/1 Grp 101 RF Encode state Speak into sync buffer
*Apr 27 04:13:57.855: HSRP: CF Sync send ok
*Apr 27 04:14:07.755: HSRP: Gi0/0/1 Grp 101 RF Encode state Standby into sync buffer
*Apr 27 04:14:07.755: HSRP: Gi0/0/1 Grp 101 RF Encode state Active into sync buffer
*Apr 27 04:14:07.863: HSRP: CF Sync send ok
*Apr 27 04:14:07.867: HSRP: CF Sync send ok
!Standby RP
*Apr 27 04:11:21.011: HSRP: RF CF client 32, entity 0 got msg len 24
```

```
*Apr 27 04:11:21.011: HSRP: Gi0/0/1 Grp 101 RF sync state Init -> Listen
*Apr 27 04:11:31.011: HSRP: RF CF client 32, entity 0 got msg len 24
*Apr 27 04:11:31.011: HSRP: Gi0/0/1 Grp 101 RF sync state Listen -> Speak
*Apr 27 04:11:41.071: HSRP: RF CF client 32, entity 0 got msg len 24
*Apr 27 04:11:41.071: HSRP: RF CF client 32, entity 0 got msg len 24
*Apr 27 04:11:41.071: HSRP: Gi0/0/1 Grp 101 RF sync state Speak -> Standby
*Apr 27 04:11:41.071: HSRP: Gi0/0/1 Grp 101 RF sync state Standby -> Active
```

SSO HSRP の設定例

例：SSO 対応 HSRP のイネーブル化

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。

```
Device(config)# redundancy
Device(config-red)# mode sso
```

nostandbysso コマンドを使用して SSO HSRP をディセーブルにすると、次の図に示すように、再度イネーブルにできます。

```
Device(config)# interface GigabitEthernet 1/0/0
Device(config-if)# ip address 10.1.1.1 255.255.0.0
Device(config-if)# standby priority 200
Device(config-if)# standby preempt
Device(config-if)# standby sso
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
HSRP 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、使用に関する注意事項、および例	『*Cisco IOS First Hop redundancy Protocols Command Reference*』
HSRP for IPv6。	「HSRP for IPv6」のモジュール
HSRP のトラブルシューティング	『Hot Standby Router Protocol: Frequently Asked Questions』

標準

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

MIB

MIB	MIB のリンク
CISCO-HSRP-MIB CISCO-HSRP-EXT-MIB	選択したプラットフォーム、Cisco 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場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	Title
RFC 792	インターネット制御メッセージ プロトコル（*ICMP*）
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	Link
★枠で囲まれた Technical Assistance の場合★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。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。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

SSO - HSRP の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *9*：*SSO - HSRP* の機能情報

機能名	リリース	機能情報
SSO：HSRP	12.2(25)S 12.2(33)SRA 12.2(33)SXH 12.2(50)SY 15.0(1)S 15.0(1)SY Cisco IOS XE Release 2.1 Cisco IOS XE 3.1.0SG	SSO - HSRP 機能により、冗長 RP のあるデバイスが 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。 **debugstandbyevents** および **standbysso** 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。

第 11 章

HSRP - ISSU

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。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

HSRP に関する情報：ISSU

HSRP - ISSU

インサービス ソフトウェア アップグレード（ISSU）プロセスにより、パケット 転送を続行しながら、Cisco 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、計画的なソフトウェア 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、パケット転送中に Cisco ソフトウェアを変更できるため、ネットワークのアベイラビリティが向上し、計画的なソフトウェア アップグレードによるダウンタイムを短縮できます。

ISSU の詳細については、『*Cisco IOS In Service Software Upgrade Process*』の「*High Availability Configuration Guide*」を参照してください。

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
HSRP 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、使用に関する注意事項、および例	『*Cisco IOS First Hop redundancy Protocols Command Reference*』
HSRP for IPv6。	「HSRP for IPv6」のモジュール
HSRP のトラブルシューティング	『Hot Standby Router Protocol: Frequently Asked Questions』

標準

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

MIB

MIB	MIB のリンク
CISCO-HSRP-MIB CISCO-HSRP-EXT-MIB	選択したプラットフォーム、Cisco 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場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	Title
RFC 792	インターネット制御メッセージ プロトコル（*ICMP*）
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	Link
★枠で囲まれた Technical Assistance の場合★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。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。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 - ISSU の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *10*：*HSRP - ISSU* の機能情報

機能名	リリース	機能情報
HSRP - ISSU	12.2(31)SGA 12.2(33)SRB1 15.0(1)S Cisco IOS XE Release 2.1 Cisco IOS XE 3.1.0SG	HSRP - インサービス ソフトウェア アップグレード（ISSU）機能により、HSRP で ISSU がサポートされています。 インサービス ソフトウェア アップグレード（ISSU）プロセスにより、パケット 転送を続行しながら、Cisco 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、計画的なソフトウェア 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、パケット転送中に Cisco ソフトウェアを変更できるため、ネットワークのアベイラビリティが向上し、計画的なソフトウェア アップグレードによるダウンタイムを短縮できます。ここでは、ISSU の概念について説明し、システムで ISSU を実行するための手順について説明します。 この機能の詳細については、『*Cisco IOS High Availability Configuration Guide*』の「Cisco IOS In Service Software Upgrade Process」のモジュール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。

第 12 章

FHRP：HSRP MIB

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。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

FHRP に関する情報：HSRP MIB

HSRP MIB トラップ

HSRP MIB は、簡易ネットワーク管理プロトコル（SNMP）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、デバイスがアクティブ 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 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
- CISCO-HSRP-EXT-MIB.my で定義されている cHsrpExtSecAddrEntry
- CISCO-HSRP-EXT-MIB.my で定義されている cHsrpExtIfEntry

cHsrpGrpEntry テーブルは、RFC 2281 の「*Cisco Hot Standby Router Protocol*」で定義されているすべてのグループ情報で構成されています。他のテーブルは、CISCO-HSRP-EXT-MIB.my で定義されている、RFC 2281 へのシスコの拡張で構成されています。

FHRP の設定方法：HSRP MIB

HSRP MIB トラップのイネーブル化

手順の概要

1. イネーブル化
2. **configureterminal**
3. **snmp-serverenabletrapshsrp**
4. **snmp-serverhost***hostcommunity-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	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： `Device# 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-serverenabletrapshsrp** 例： `Device(config)# snmp-server enable traps hsrp`	SNMP トラップ、SNMPインフォーム、HSRP 通知をデバイスが送信できるようにします。
ステップ 4	**snmp-serverhost***hostcommunity-string***hsrp** 例： `Device(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。

FHRP の設定例：HSRP MIB

例：HSRP MIB トラップのイネーブル化

次の例は、HSRP を 2 台のデバイスで設定し、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 台のデバイスがアクティブ デバイスとして優先されます。アクティブ デバイスとしてデバイスを設定するには、デバイスを高い優先順位に設定し、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 デバイスはプライマリ デバイスと呼ばれます。2 台目のデバイスはバックアップ デバイスと呼ばれます。

デバイス A

```
Device(config)# interface GigabitEthernet 0/0/0
Device(config-if)# ip address 10.1.1.1 255.255.0.0
Device(config-if)# standby priority 200
Device(config-if)# standby preempt
Device(config-if)# standby ip 10.1.1.3
Device(config-if)# exit
Device(config)# snmp-server enable traps hsrp
Device(config)# snmp-server host yourhost.cisco.com public hsrp
```

デバイス B

```
Device(config)#interface GigabitEthernet 1/0/0
Device(config-if)# ip address 10.1.1.2 255.255.0.0
```

```
Device(config-if)#  standby priority 101
Device(config-if)# standby ip 10.1.1.3
Device(config-if)# exit
Device(config)# snmp-server enable traps hsrp
Device(config)# snmp-server host myhost.cisco.com public hsrp
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
HSRP 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、使用に関する注意事項、および例	『*Cisco IOS First Hop redundancy Protocols Command Reference*』
HSRP for IPv6。	「HSRP for IPv6」のモジュール
HSRP のトラブルシューティング	『Hot Standby Router Protocol: Frequently Asked Questions』

標準

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

MIB

MIB	MIB のリンク
CISCO-HSRP-MIB CISCO-HSRP-EXT-MIB	選択したプラットフォーム、Cisco 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場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	Title
RFC 792	インターネット制御メッセージ プロトコル（*ICMP*）
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	Link
★枠で囲まれた Technical Assistance の場合★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。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。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

FHRP の機能情報：HSRP-MIB

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *11*：*FHRP* の機能情報：*HSRP-MIB*

機能名	リリース	機能情報
FHRP - HSRP - MIB	12.0(3)T 12.0(12)S Cisco IOS XE Release 2.1	FHRP - HSRP - MIB 機能により、CISCO - HRSP - MIB がサポートされています。

第 13 章

HSRP の MPLS VPN サポート

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。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

HSRP の MPLS VPN サポートについて

HSRP の MPLS VPN サポート

HSRP のマルチプロトコル ラベル スイッチング（MPLS）VPN 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 つのプロバイダー エッジ（PE）デバイス間でイーサネット LAN が接続されている場合です。

- カスタマー エッジ（CE）デバイスに 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 つ以上の VPN ルーティングおよび転送（VRF）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 テーブル
- Cisco Express Forwarding 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 テーブルおよび CEF テーブルに格納されます。各 VRF カスタマーに対して、別個の一連のルーティング テーブルおよび Cisco Express Forwarding テーブルが維持されます。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 内のデバイス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。

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
HSRP 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、使用に関する注意事項、および例	『*Cisco IOS First Hop redundancy Protocols Command Reference*』
HSRP for IPv6。	「HSRP for IPv6」のモジュール
HSRP のトラブルシューティング	『Hot Standby Router Protocol: Frequently Asked Questions』

標準

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

MIB

MIB	MIB のリンク
CISCO-HSRP-MIB CISCO-HSRP-EXT-MIB	選択したプラットフォーム、Cisco 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場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	Title
RFC 792	インターネット制御メッセージ プロトコル（*ICMP*）
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	Link
★枠で囲まれた Technical Assistance の場合★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。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。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

MPLS VPN の HSRP サポートの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *12*：*MPLS VPN* の *HSRP* サポートの機能情報

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 12.2(50)SY 15.0(1)S 15.0(1)SY Cisco IOS XE Release 2.1	HSRP のマルチプロトコル ラベル スイッチング（MPLS）バーチャル プライベート ネットワーク（VPN）インターフェイス サポートが役に立つのは、特定の状況で 2 つのプロバイダー エッジ（PE）デバイス間でイーサネット LAN が接続されている場合です。 この機能により、新規追加または変更されたコマンドはありません。

第 14 章

『Configuring VRRP』

仮想ルータ冗長プロトコル（VRRP）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 に接続された 1 つ以上の他のルータと連係して 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。

この章では、VRRP に関する概念と、ネットワーク上での VRRP 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。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

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 ブロードキャスト対応イーサネット LAN で使用するため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、ブリッジグループ仮想インターフェイス（BVI）、およびギガビット イーサネット インターフェイス、マルチプロトコル ラベル スイッチング（MPLS）バーチャルプライベート ネットワーク（VPN）、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、**bridgeforward-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、**vrrptimersadvertise** コマンドを使用します。

VRRP の概要

VRRP の動作

LAN クライアントが特定のリモート接続先に対して、どのルータをファーストホップにすべきかを判断するには、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。ダイナミック ルータ ディスカバリの例を示します。

- プロキシ ARP：クライアントはアドレス解決プロトコル（ARP）を使用して到達すべき宛先を取得します。ルータは独自の MAC アドレスで ARP 要求に応答します。
- ルーティング プロトコル：クライアントはダイナミック ルーティング プロトコルのアップデートを（ルーティング情報プロトコル（RIP）などから）受信し、独自のルーティングテーブルを形成します。
- ICMP Router Discovery Protocol（IRDP）クライアント：クライアントはインターネット制御メッセージ プロトコル（ICMP）ルータ ディスカバリ クライアントを実行します。

ダイナミック ディスカバリ プロトコルには、LAN クライアントにおいて、設定および処理のオーバーヘッドが発生するという短所があります。また、ルータが機能を停止したときに、別のルータへの切り替え処理が遅くなる可能性があります。

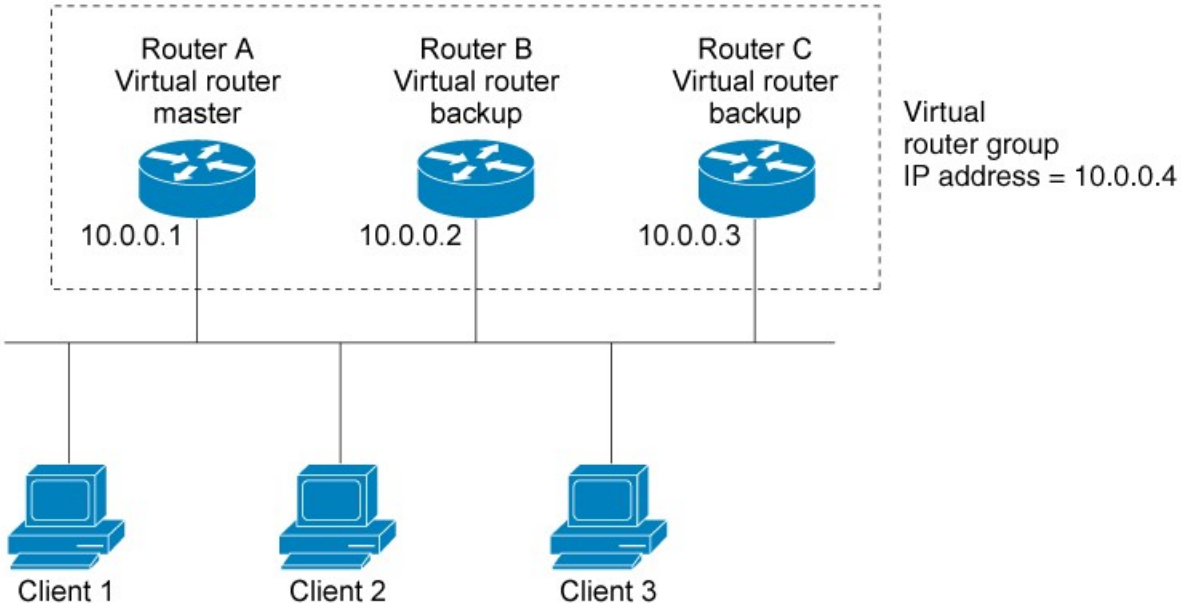
ダイナミック ディスカバリ プロトコルの代わりに、クライアント上でデフォルト ルータをスタティックに設定することもできます。このアプローチでは、クライアントの設定と処理は簡略化されますが、単一障害点が生じます。デフォルト ゲートウェイで障害が発生した場合、LAN クライアントの通信はローカル IP ネットワーク セグメントに限定され、ネットワークの他の部分から切り離されます。

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 を使用すると、ルータのグループを 1 つの仮想ルータにすることができます。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。

下の図は、VRRP が設定された LAN トポロジを示しています。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 *8*：基本的な *VRRP* トポロジ



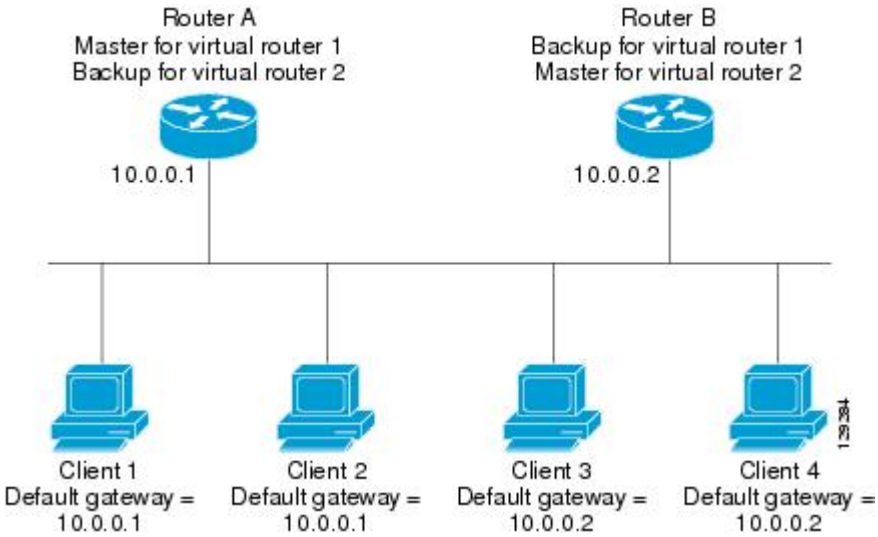
仮想ルータはルータ A の物理イーサネット インターフェイスの IP アドレスを使用するため、ルータ A は仮想ルータ マスターのロールを担い、「IP アドレス所有者」とも呼ばれます。ルータ A は、仮想ルータ マスターとして、仮想ルータの IP アドレスを管理し、この IP アドレスに送信されたパケットの転送を行います。クライアント 1 ～ 3 には、デフォルト ゲートウェイの IP アドレス 10.0.0.1 が設定されています。

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、再び仮想ルータ マスターになります。VRRP ルータの役割と、仮想ルータ マスターに障害が発生するとどうなるかについての詳細は、「VRRP ルータのプライオリティおよびプリエンプション」のセクションを参照してください。

下の図に示す 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 *9*：ロード シェアリングおよび冗長構成の *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、「複数の仮想ルータのサポート」のセクション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 マスターです。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 2 にはデフォルト ゲートウェイの IP アドレス 10.0.0.1 が設定されています。

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 マスターです。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 4 にはデフォルト ゲートウェイの IP アドレス 10.0.0.2 が設定されています。

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

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 のメッセージ ダイジェスト 5（MD5）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、VRRP アドバタイズメント専用のインターネット割り当て番号局（IANA）標準マルチキャストアドレス（224.0.0.18）を使用します。このアドレッシング方式によって、マルチキャストを提供するルータ数が最小限になり、テスト機器でセグメント上の VRRP パケットを正確に識別できるようになります。IANA では VRRP に IP プロトコル番号 112 を割り当てていました。

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

- ルータの処理能力
- ルータのメモリの能力
- 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 ルータのプライオリティおよびプリエンプション

VRRP 冗長性スキームの重要な一面に、VRRP 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。

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 アドレスのオーナーである場合には、このルータが仮想マスター ルータとして機能します。

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、LAN トポロジのマスター仮想ルータであるルータ A が機能を停止した場合、選択プロセスが実行されて、仮想ルータ バックアップ B または C が引き継ぐかどうかが決定されます。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設定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 の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 に従った VRRP プロトコルはミリ秒タイマーをサポートしていませんが、シスコ ルータでは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 **showvrrp** 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。ホットスタンバイ ルータ プロトコル（HSRP）、ゲートウェイ ロード バランシング プロトコル（GLBP）、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。

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。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 プロセスは定期的に、トラッキング対象オブジェクトをポーリングし、値の変更を確認します。トラッキング対象オブジェクトの変更は、すぐに、または指定された遅延後に、対象のクライアント プロセスに通知されます。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。

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ことができます。

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 デバイス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、仮想デバイスのプライオリティを増加（または減少）させます。

VRRP オブジェクト トラッキングがデバイスのプライオリティに及ぼす影響

デバイスがオブジェクト トラッキング対応として設定されていて、なおかつトラッキング対象のオブジェクトがダウンした場合、デバイスのプライオリティはダイナミックに変更されます。トラッキング プロセスは定期的に、トラッキング対象オブジェクトをポーリングし、値の変更を確認します。トラッキング対象のオブジェクトの変化は、すぐに VRRP に伝えられるか、指定した遅延時間が経過してから VRRP 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、VRRP プライオリティが引き下げられます。その場合、**vrrppreempt** 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 デバイスが仮想デバイス 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」のセクションを参照してください。

インサービス ソフトウェア アップグレード：VRRP

VRRP はインサービス ソフトウェア アップグレード（ISSU）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ルート プロセッサ（RP）またはラインカード上で異なるバージョンの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、『*High Availability Configuration Guide*』の「In Service Software Upgrade Process」を参照してください。

ステートフル スイッチオーバーの VRRP サポート

ステートフル スイッチオーバー機能の VRRP サポートの導入に伴い、VRRP は SSO を認識します。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、VRRP 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 **novrrpsso** 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。

VRRP の設定方法

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. イネーブル化
2. **configureterminal**
3. **interface***typenumber*
4. **ipaddress***ip-addressmask*
5. **vrrp***group***description***text*
6. **vrrp***group***priority***level*
7. **vrrp***group***preempt** [**delayminimum***seconds*]
8. **vrrp***group***timerslearn**
9. **exit**
10. **novrrpsso**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 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***typenumber* 例： `Router(config)# interface GigabitEthernet 0/0/0`	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 4	**ipaddress***ip-addressmask* 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** [**delayminimum***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***timerslearn** 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 9	**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。

	コマンドまたはアクション	目的
ステップ 10	**novrrpsso** 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. イネーブル化
2. **configureterminal**
3. **interface***typenumber*
4. **ipaddress***ip-addressmask*
5. **vrrp***group***ip***ip-address* [**secondary**]
6. **end**
7. **showvrrp** [**brief**] | *group*]
8. **showvrrpinterface***typenumber* [**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	イネーブル化 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 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***typenumber* 例： `Router(config)# interface GigabitEthernet 0/0/0`	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。

	コマンドまたはアクション	目的
ステップ 4	**ipaddress***ip-addressmask* 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***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 アドレスの指定後は、**secondary** キーワードを指定して **vrrpip** コマンドを再び使用し、このグループでサポートする他の 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	**showvrrp** [**brief**] | *group*] 例： `Router# show vrrp 10`	（任意）ルータ上の 1 つまたはすべての VRRP グループについて、簡潔または詳細なステータスを表示します。
ステップ 8	**showvrrpinterface***typenumber* [**brief**] 例： `Router# show vrrp interface GigabitEthernet 0/0/0`	（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。

VRRP オブジェクト トラッキングの設定

（注） 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. イネーブル化
2. **configureterminal**
3. **track***object-number***interface***typenumber* {**line-protocol** | **iprouting**}
4. **interface***typenumber*
5. **vrrp***group***ip***ip-address*
6. **vrrp***group***priority***level*
7. **vrrp***group***track***object-number* [**decrement***priority*]
8. **end**
9. **showtrack** [*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	イネーブル化 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 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***typenumber* {**line-protocol** | **iprouting**} 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。 • このコマンドは、**vrrptrack** コマンドで使用されるインターフェイスと対応するオブジェクトの数を設定します。 • **line-protocol** キーワードを指定すると、インターフェイスがアップ状態かどうかが追跡されます。**iprouting** キーワードを指定すると、インターフェイス上で IP

	コマンドまたはアクション	目的
		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。 • **trackiproute** 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***typenumber* 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。
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	**showtrack** [*object-number*] 例： `Router# show track 1`	トラッキング情報を表示します。

VRRP テキスト認証の設定

はじめる前に

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、受信側のルータの MD5 認証がイネーブルになっていれば、VRRP 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. イネーブル化
2. **configureterminal**
3. **terminalinterface***typenumber*
4. **ipaddress***ip-addressmask* [**secondary**]
5. **vrrp***group***authenticationtext***text-string*
6. **vrrp***group***ip***ip-address*
7. 通信する各ルータに対してステップ 1 ～ 6 を繰り返します。
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	イネーブル化 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 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	**terminalinterface***typenumber* 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。

	コマンドまたはアクション	目的
ステップ 4	**ipaddress***ip-addressmask* [**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***authenticationtext***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	通信する各ルータに対してステップ 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。

VRRP の設定例

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。

コンフィギュレーションにおいて、各グループのプロパティは次のとおりです。

- 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 120 で、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です。
- グループ 5：
  - ルータ B はプライオリティ 200 で、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です。
- グループ 100：
  - ルータ A は、IP アドレスが上位（10.1.0.2）なので、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の 1 秒です。
  - プリエンプションはディセーブルです。

ルータ A

```
Router(config)# interface GigabitEthernet 1/0/0
Router(config-if)# ip address 10.1.0.2 255.0.0.0
Router(config-if)# vrrp 1 priority 120
Router(config-if)# vrrp 1 authentication cisco
Router(config-if)# vrrp 1 timers advertise 3
Router(config-if)# vrrp 1 timers learn
Router(config-if)# vrrp 1 ip 10.1.0.10
Router(config-if)# vrrp 5 priority 100
Router(config-if)# vrrp 5 timers advertise 30
Router(config-if)# vrrp 5 timers learn
Router(config-if)# vrrp 5 ip 10.1.0.50
Router(config-if)# vrrp 100 timers learn
Router(config-if)# no vrrp 100 preempt
Router(config-if)# vrrp 100 ip 10.1.0.100
Router(config-if)# no shutdown
```

ルータ B

```
Router(config)# interface GigabitEthernet 1/0/0
Router(config-if)# ip address 10.1.0.1 255.0.0.0
Router(config-if)# vrrp 1 priority 100
Router(config-if)# vrrp 1 authentication cisco
Router(config-if)# vrrp 1 timers advertise 3
Router(config-if)# vrrp 1 timers learn
Router(config-if)# vrrp 1 ip 10.1.0.10
Router(config-if)# vrrp 5 priority 200
Router(config-if)# vrrp 5 timers advertise 30
Router(config-if)# vrrp 5 timers learn
```

```
Router(config-if)# vrrp 5 ip 10.1.0.50
Router(config-if)# vrrp 100 timers learn
Router(config-if)# no vrrp 100 preempt
Router(config-if)# vrrp 100 ip 10.1.0.100
Router(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 だけ引き下げられます。

```
Router(config)# track 1 interface Serial 0/1 line-protocol
Router(config-track)# exit
Router(config)# interface Ethernet 1/0
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

次の例は、「例：VRRP オブジェクト トラッキング」セクションに示した構成を確認します。

```
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：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 GigabitEthernet 0/0/0
Router(config)# 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：VRRP MIB トラップ

```
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

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
VRRP コマンド	『*Cisco IOS IP Application Services Command Reference*』
オブジェクト トラッキング	拡張オブジェクト トラッキングの設定
ホット スタンバイ ルーティング プロトコル（HSRP）	『Configuring HSRP』
In Service Software Upgrade（ISSU）	『*High Availability Configuration Guide*』の「In Service Software Upgrade Process」
ゲートウェイ ロード バランシング プロトコル（GLBP）	『Configuring GLBP』
『Stateful Switchover』	『*High Availability Configuration Guide*』の「Stateful Switchover」のセクション

標準

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

MIB

MIB	MIB のリンク
VRRP MIB	選択したプラットフォーム、Cisco 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場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	Title
RFC 2338	『Virtual Router Redundancy Protocol』
RFC 2787	Virtual Router Redundancy Protocol の管理対象オブジェクトの定義
RFC 3768	仮想ルータ冗長プロトコル（VRRP）

シスコのテクニカル サポート

説明	Link
★枠で囲まれた Technical Assistance の場合★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。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。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

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *13*：*VRRP* の機能情報

機能名	リリース	機能の設定情報
ISSU と VRRP	15.2(1)S 15.3(1)S	VRRP はインサービス ソフトウェア アップグレード（ISSU）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ルートプロセッサ（RP）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。 この機能により、新規追加または変更されたコマンドはありません。

機能名	リリース	機能の設定情報
SSO と VRRP	15.2(1)S 15.3(1)S	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。 **debugvrrpha**、**vrrpsso**、**showvrrp** 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。
『Virtual Router Redundancy Protocol』	15.2(1)S 15.3(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。 次のコマンドは、この機能によって導入されました。 **debugvrrpall**、**debugvrrperror**、**debugvrrpevents**、**debugvrrppackets**、**debugvrrpstate**、**showvrrp**、**showvrrpinterface**、**vrrpauthentication**、**vrrpdescription**、**vrrpip**、**vrrppreempt**、**vrrppriority**、**vrrptimersadvertise**、**vrrptimerslearn**

機能名	リリース	機能の設定情報
VRRP オブジェクト トラッキング	15.2(1)S 15.3(1)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。 コマンド **vrrptrack** がこの機能により導入されました。 コマンド **showtrack** がこの機能により変更されました。
VRRP MIB—RFC 2787		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。 コマンド **vrrpshutdown** がこの機能により導入されました。 **snmp-serverenabletraps** および **snmp-serverhost** の各コマンドがこの機能により変更されました。
FHRP—VRF 対応 VRRP		FHRP—VRF 対応 VRRP 機能は、MPLS VPN で VRRP サポートを有効にします。 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。

用語集

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。

VRRP ルータ：VRRP を実行しているルータ。

第 15 章

VRRPv3 プロトコルのサポート

Virtual Router Redundancy Protocol（VRRP）は、デバイスのグループを使用して単一の仮想デバイスを形成し、冗長性を実現することができます。これにより、仮想デバイスをデフォルト 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。デバイスのグループを表す仮想デバイスは、「VRRP グループ」とも呼ばれます。VRRP バージョン 3（v3）のプロトコル サポート機能は、VRRP バージョン 2（v2）が IPv4 アドレスしかサポートしていないのに対し、IPv4 と IPv6 アドレスをサポートするための機能を提供します。このモジュールでは、VRRPv3 に関連する概念と、ネットワーク内で VRRP グループを作成してカスタマイズする方法について説明します。VRRPv3 プロトコル サポートを使用する利点は次のとおりです。

- マルチベンダー環境での相互運用性。
- VRRPv3 は、VRRPv2 が IPv4 アドレスしかサポートしていないのに対し、IPv4 と IPv6 アドレスの使用をサポートしています。
- VRRS 経路によるスケーラビリティの向上。

（注） このモジュールでは、VRRP と VRRPv3 は同じ意味で使用されています。

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。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

VRRPv3 プロトコルのサポートの制限事項

- VRRPv3 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。VRRPv3 は、マルチアクセス、マルチキャスト、または ブロードキャスト対応イーサネット LAN で使用するために設計されています。
- VRRPv3 は、イーサネット、ファストイーサネット、ブリッジグループ仮想インターフェイス（BVI）、およびギガビット イーサネット インターフェイス、マルチプロトコル ラベル スイッチング（MPLS）バーチャル プライベート ネットワーク（VPN）、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、VRRPv3 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より短く設定する必要があります。VRRPv3 アドバタイズ タイマーの時間を BVI インターフェイスでの転送遅延時間以上の値に設定すると、最近初期化された BVI インターフェイス上にある VRRP デバイスが無条件にマスター ロールを引き継げなくなります。BVI インターフェイスでの転送遅延を設定するには、**bridgeforward-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、**vrrptimersadvertise** コマンドを使用します。
- VRRPv3 は、ステートフル スイッチオーバー（SSO）をサポートしていません。
- VRRP が VRRS 経路の冗長インターフェイスと同じネットワーク パス上で動作する場合にのみ、完全なネットワークの冗長性を実現できます。完全な冗長性のために、次の制約事項が適用されます。
  - VRRS 経路は、親 VRRP グループと異なる物理インターフェイスを共有したり、親 VRRP グループと異なる物理インターフェイスを持つサブインターフェイス上で設定することはできません。
  - VRRS 経路は、関連付けられた VLAN が親 VRRP グループが設定された VLAN と同じトランクを共有していない限り、スイッチ仮想インターフェイス（SVI）に設定することはできません。

VRRPv3 プロトコル サポートについて

VRRPv3 の利点

IPv4 と IPv6 のサポート

VRRPv3 は、VRRPv2 が IPv4 アドレスしかサポートしていないのに対し、IPv4 と IPv6 アドレス ファミリをサポートしています。

（注） VRRPv3 が使用中の場合、VRRPv2 は使用できません。VRRPv3 を設定可能にするには、**fhrpversionvrrpv3** コマンドをグローバル コンフィギュレーション モードで使用する必要があります

冗長性

VRRP により、複数のデバイスをデフォルト ゲートウェイ デバイス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 クライアントとのトラフィックを複数のデバイスで共有するように VRRP を設定できるため、利用可能なデバイス間でより公平にトラフィックの負荷を共有できます。

複数の仮想デバイス

VRRP はデバイスの物理インターフェイス上で（拡張の制限に従って）最大 255 の仮想デバイス（VRRP グループ）をサポートします。複数の仮想デバイス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。拡張環境では、VRRS 経路は VRRP 制御グループと組み合わせて使用する必要があります。

複数の IP アドレス

仮想デバイスは、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。

（注） VRRP グループでセカンダリ IP アドレスを使用するには、プライマリ アドレスを同じグループで設定する必要があります。

プリエンプション

VRRP の冗長性スキームにより、仮想デバイス 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デバイスバックアップが、機能を停止した仮想デバイスマスターを引き継ぐようにできます。

（注） 優先度の低いマスター デバイスのプリエンプションは、オプションの遅延を使用してイネーブルにできます。

アドバタイズメント プロトコル

VRRP は、VRRP アドバタイズメント専用のインターネット割り当て番号局（IANA）標準マルチキャスト アドレスを使用します。IPv4 では、マルチキャスト アドレスは 224.0.0.18 です。IPv6 では、マルチキャスト アドレスは FF02:0:0:0:0:0:0:12 です。このアドレッシング方式によって、マルチキャストを提供するデバイス数が最小限になり、テスト機器でセグメント上の VRRP パケットを正確に識別できるようになります。IANA では VRRP に IP プロトコル番号 112 を割り当てていました。

VRRP デバイスのプライオリティおよびプリエンプション

VRRP 冗長性スキームの重要な一面に、VRRP デバイス プライオリティがあります。プライオリティにより、各 VRRP デバイスが実行する役割と、仮想マスター デバイス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。

VRRP デバイス仮想デバイスの IP アドレスと物理インターフェイスの IP アドレスのオーナーである場合には、このデバイスが仮想マスター デバイスとして機能します。

VRRP デバイスが仮想バックアップ デバイスとして機能するかどうかや、仮想マスター デバイスが機能を停止した場合に仮想マスター デバイスを引き継ぐ順序も、プライオリティによって決定されます。各仮想バックアップ デバイスのプライオリティは、**priority** コマンドを使用して 1 ～ 254 の値に設定できます（**vrrpaddress-family** コマンドを使用して VRRP 設定モードに入り、**priority** オプションにアクセスします）。

たとえば、LAN トポロジのマスター仮想デバイスであるデバイス A が機能を停止した場合、選択プロセスが実行されて、仮想デバイス バックアップ B または C が引き継ぐかどうかが決定されます。デバイス B とデバイス 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デバイス B が仮想デバイス マスターになります。デバイス B とデバイス 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デバイス バックアップが選択されて仮想デバイス マスターになります。

デフォルトでは、プリエンプティブ設定はイネーブルになっています。この場合、仮想マスター デバイスになるように選択されている仮想バックアップ デバイスの中で、より高いプライオリティが設定されている仮想バックアップ デバイスが仮想マスターデバイスになります。このプリエンプティブ設定は、**no preempt** コマンドを使用して無効にできます（**vrrpaddress-family** コマンドを使用して VRRP 設定モードに入り、**no preempt** コマンドを入力します）。プリエンプションがディセーブルになっている場合は、元の仮想マスター デバイスが回復して再びマスターになる

まで、仮想マスターデバイスになるように選択されている仮想バックアップデバイスがマスターの役割を実行します。

（注） 優先度の低いマスター デバイスのプリエンプションは、オプションの遅延を使用してイネーブルにできます。

VRRP の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、（VRRP グループ設定に基づいて）IPv4 または IPv6 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適切なマルチキャスト アドレスに送信されます。IPv4 では、マルチキャスト アドレスは 224.0.0.18 です。IPv6 では、マルチキャスト アドレスは FF02:0:0:0:0:0:0:12 です。アドバタイズメントは、デフォルトでは 1 秒に 1 回送信されますが、この間隔は設定可能です。

シスコ ルータでは、VRRPv2 からの変更点であるミリ秒タイマーが設定できます。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 **showvrrp** 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。ミリ秒の値は望ましい状況でのみ動作します。ミリ秒のタイマー値の使用は、VRRPv3 も含めてサポートしている限り、サードパーティ ベンダーと互換性があります。タイマー値は 100 ～ 40000 ミリ秒の範囲で指定できます。

VRRPv3 プロトコル サポートの設定方法

IPv6 VRRP リンク ローカル アドレス

IPv6 の VRRPv3 では、グループを動作可能にするため、プライマリ仮想リンクローカル IPv6 アドレスが設定されている必要があります。プライマリ リンク ローカル IPv6 アドレスがグループに確立されると、セカンダリ グローバル アドレスを追加できます。

デバイス上の VRRPv3 のイネーブル化

デバイス上で VRRPv3 をイネーブルにするには、次のタスクを実行します。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **fhrpversionvrrpv3**
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	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# 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	**fhrpversionvrrpv3** 例： `Device(config)# fhrp version vrrp v3`	VRRPv3 および VRRS を設定する機能をイネーブルにします。 （注） VRRPv3 が使用中の場合、VRRPv2 は使用できません。
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

VRRP グループの作成とカスタマイズ

VRRP グループを作成するには、次の手順を実行します。ステップ 6 ～ 14 はそのグループのカスタマイズ オプションで、これらは省略可能です。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **fhrpversionvrrpv3**
4. **interface***typenumber*
5. **vrrp***group-id***address-family** {**ipv4** | **ipv6**}
6. **address***ip-address* [**primary** | **secondary**]
7. **description***group-description*
8. **match-address**
9. **preemptdelayminimum***seconds*
10. **priority***priority-level*
11. **timersadvertise***interval*
12. **vrrpv2**
13. **vrrsleader***vrrs-leader-name*
14. シャットダウン
15. **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	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# 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	**fhrpversionvrrpv3** 例： `Device(config)# fhrp version vrrp v3`	VRRPv3 および VRRS を設定する機能をイネーブルにします。 （注） VRRPv3 が使用中の場合、VRRPv2 は使用できません。
ステップ 4	**interface***typenumber* 例： `Device(config)# interface GigabitEthernet 0/0/0`	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。

	コマンドまたはアクション	目的
ステップ 5	**vrrp***group-id***address-family** {**ipv4** | **ipv6**} 例： `Device(config-if)# vrrp 3 address-family ipv4`	VRRP グループを作成し、VRRP 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	**address***ip-address* [**primary** | **secondary**] 例： `Device(config-if-vrrp)# address 100.0.1.10 primary`	VRRP グループのプライマリ アドレスまたはセカンダリ アドレスを指定します。 （注） IPv6 の VRRPv3 では、グループを動作可能にするため、プライマリ仮想リンクローカル IPv6 アドレスが設定されている必要があります。プライマリ リンク ローカル IPv6 アドレスがグループに確立されると、セカンダリ グローバルアドレスを追加できます。
ステップ 7	**description***group-description* 例： `Device(config-if-vrrp)# description group 3`	（任意）VRRP グループの説明を指定します。
ステップ 8	**match-address** 例： `Device(config-if-vrrp)# match-address`	（任意）アドバタイズメント パケットのセカンダリ アドレスを設定したアドレスと照合します。 • セカンダリアドレスの照合は、デフォルトで有効になっています。
ステップ 9	**preemptdelayminimum***seconds* 例： `Device(config-if-vrrp)# preempt delay minimum 30`	（任意）プライオリティの低いマスター デバイスのプリエンプションをオプションの延期期間でイネーブルにします。 • プリエンプションはデフォルトでイネーブルです。
ステップ 10	**priority***priority-level* 例： `Device(config-if-vrrp)# priority 3`	（任意）VRRP グループのプライオリティを指定します。 • VRRP グループの優先度はデフォルトで 100 です。
ステップ 11	**timersadvertise***interval* 例： `Device(config-if-vrrp)# timers advertise 1000`	（任意）アドバタイズメント タイマーをミリ秒で設定します。 • アドバタイズメントタイマーはデフォルトで1000ミリ秒に設定されています。

	コマンドまたはアクション	目的
ステップ 12	**vrrpv2** 例： `Device(config-if-vrrp)# vrrpv2`	（任意）VRRPv2 のみをサポートするデバイスと相互運用するため、VRRPv2 のサポートを同時にイネーブルにします。 • VRRPv2 はデフォルトで無効になっています。
ステップ 13	**vrrsleader***vrrs-leader-name* 例： `Device(config-if-vrrp)# vrrs leader leader-1`	（任意）VRRS に登録され、フォロワーに使用されるリーダーの名前を指定します。 • 登録済みの VRRS 名はデフォルトで使用不可になっています。
ステップ 14	シャットダウン 例： `Device(config-if-vrrp)# shutdown`	（任意）VRRP グループの VRRP 設定をディセーブルにします。 • VRRP の設定は、VRRP グループに対してはデフォルトでイネーブルになっています。
ステップ 15	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

FHRP クライアントの初期化前の遅延時間の設定

インターフェイス上のすべての FHRP クライアントの初期化の前に遅延期間を設定するには、次のタスクを実行します。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **fhrpversionvrrpv3**
4. **interface***typenumber*
5. **fhrpdelay** {[**minimum**] [**reload**] *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	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# 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	**fhrpversionvrrpv3** 例： `Device(config)# fhrp version vrrp v3`	VRRPv3 および VRRS を設定する機能をイネーブルにします。 （注） VRRPv3 が使用中の場合、VRRPv2 は使用できません。
ステップ 4	**interface***typenumber* 例： `Device(config)# interface GigabitEthernet 0/0/0`	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 5	**fhrpdelay** {[**minimum**] [**reload**] *seconds*} 例： `Device(config-if)# fhrp delay minimum 5`	インターフェイスの起動後に、FHRP クライアントの初期化の遅延期間を指定します。 • 範囲は 0 ～ 3600 秒です。
ステップ 6	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

VRRPv3 プロトコル サポートの設定例

例：デバイス上の VRRPv3 のイネーブル化

次の例は、デバイスで VRRPv3 をイネーブルにする方法を示しています。

```
Device> enable
Device# configure terminal
Device(config)# fhrp version vrrp v3
Device(config-if-vrrp)# end
```

例：VRRP グループの作成とカスタマイズ

次に、VRRP グループを作成およびカスタマイズする例を示します。

```
Device> enable
Device# configure terminal
Device(config)# fhrp version vrrp v3
Device(config)# interface gigabitethernet0/0
Device(config-if)# vrrp 3 address-family ipv4
Device(config-if-vrrp)# address 100.0.1.10 primary
Device(config-if-vrrp)# description group 3
Device(config-if-vrrp)# match-address
Device(config-if-vrrp)# preempt delay minimum 30
Device(config-if-vrrp)# end
```

（注） 上記の例では、グローバル コンフィギュレーション モードで **fhrpversionvrrpv3** コマンドが使用されています。

例：FHRP クライアントの初期化前の遅延時間の設定

次の例は、FHRP クライアントの初期化前の遅延時間の設定方法を示しています。

```
Device> enable
Device# configure terminal
Device(config)# fhrp version vrrp v3
Device(config)# interface gigabitethernet0/0
Device(config-if)# fhrp delay minimum 5
Device(config-if-vrrp)# end
```

（注） 上記の例では、インターフェイスが表示されてから FHRP クライアントの初期化に 5 秒間の遅延時間が指定されています。遅延時間は 0 ～ 3600 秒の範囲で指定できます。

例：VRRP ステータス、設定、および統計情報の詳細

以下は、VRRP グループのステータス、設定、および統計情報の詳細の出力例です。

```
Device> enable
Device# show vrrp detail

 Ethernet0/0 - Group 1 - Address-Family IPv4

 State is MASTER
 State duration 3.707 secs
 Virtual IP address is 1.0.0.10
 Virtual MAC address is 0000.5E00.0101
 Advertisement interval is 1000 msec
 Preemption enabled
 Priority is 100
 Master Router is 1.0.0.1 (local), priority is 100
 Master Advertisement interval is 1000 msec (expires in 686 msec)
 Master Down interval is unknown
 State is MASTER
 State duration 3.707 secs
 VRRPv3 Advertisements: sent 5 (errors 0) - rcvd 0
 VRRPv2 Advertisements: sent 0 (errors 0) - rcvd 0
 Group Discarded Packets: 0
   VRRPv2 incompatibility: 0
   IP Address Owner conflicts: 0
   Invalid address count: 0
   IP address configuration mismatch : 0
   Invalid Advert Interval: 0
   Adverts received in Init state: 0
   Invalid group other reason: 0
 Group State transition:
   Init to master: 0
   Init to backup: 1 (Last change Mon Jul 30 16:42:01.856)
   Backup to master: 1 (Last change Mon Jul 30 16:42:05.469)
   Master to backup: 0
   Master to init: 0
   Backup to init: 0

Device# exit
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Master Commands List, All Releases』
FHRP コマンド	『First Hop Redundancy Protocols Command Reference』
VRRPv2 の設定	『*Configuring VRRP*』

標準および RFC

標準/RFC	Title
RFC5798	『*Virtual Router Redundancy Protocol*』

シスコのテクニカル サポート

説明	Link
★枠で囲まれた Technical Assistance の場合★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。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。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

VRRPv3 プロトコルのサポートの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *14*：*VRRPv3* プロトコルのサポートの機能情報

機能名	リリース	機能情報
VRRPv3 プロトコルのサポート	Cisco IOS XE Release 3.8S	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。VRRPv3 プロトコルのサポート機能は、IPv4 と IPv6 アドレスをサポートするための機能を提供します。 **fhrpdelay**、**showvrrp**、**vrrpaddress-family** の各コマンドが導入または修正されました。

用語集

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。仮想ルータは、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。

VRRP ルータ：VRRP を実行しているルータ。

第 16 章

VRRPv3：オブジェクト トラッキングの統合

Virtual Router Redundancy Protocol（VRRP）は、デバイスのグループを使用して単一の仮想デバイスを形成し、冗長性を実現することができます。これにより、仮想デバイスをデフォルト 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。デバイスのグループを表す仮想デバイスは、「VRRP グループ」とも呼ばれます。VRRPv3：オブジェクト トラッキングの統合機能は、オブジェクトの動作を追跡し、変更の通知を受け取れるようにします。このモジュールでは、オブジェクト トラッキング（特に IPv6 オブジェクトのトラッキング）が VRRP バージョン 3（VRRPv3）にどのように統合されるかを説明し、VRRPv3 グループを使用して IPv6 オブジェクトを追跡する方法について説明します。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」のセクションを参照してください。

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。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

VRRPv3 に関する情報：オブジェクト トラッキングの統合

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。ホットスタンバイ ルータ プロトコル（HSRP）、ゲートウェイ ロード バランシング プロトコル（GLBP）、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。

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。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 プロセスは定期的に、トラッキング対象オブジェクトをポーリングし、値の変更を確認します。トラッキング対象オブジェクトの変更は、すぐに、または指定された遅延後に、対象のクライアント プロセスに通知されます。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。

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ことができます。

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 デバイス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、仮想デバイスのプライオリティを増加（または減少）させます。

VRRP オブジェクト トラッキングがデバイスのプライオリティに及ぼす影響

デバイスがオブジェクト トラッキング対応として設定されていて、なおかつトラッキング対象のオブジェクトがダウンした場合、デバイスのプライオリティはダイナミックに変更されます。トラッキング プロセスは定期的に、トラッキング対象オブジェクトをポーリングし、値の変更を確認します。トラッキング対象のオブジェクトの変化は、すぐに VRRP に伝えられるか、指定した遅延時間が経過してから VRRP 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、VRRP プライオリティが引き下げられます。その場合、**vrrppreempt** 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 デバイスが仮想デバイス 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」のセクションを参照してください。

VRRPv3 の設定方法：オブジェクト トラッキングの統合

VRRPv3 を使用した IPv6 オブジェクトのトラッキング

手順の概要

1. **fhrpversionvrrpv3**
2. **interface***typenumber*
3. **vrrp***group-id***address-family ipv6**
4. **track***object-number* **decrement***number*
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	**fhrpversionvrrpv3** 例： `Device(config)# fhrp version vrrp v3`	Virtual Router Redundancy Protocol version 3（VRRPv3）と Virtual Router Redundancy Service（VRRS）をデバイスに設定できるようにします。 （注） VRRPv3 が使用中の場合、VRRPv2 は使用できません。
ステップ 2	**interface***typenumber* 例： `Device(config)# interface GigabitEthernet 0/0/0`	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 3	**vrrp***group-id***address-family ipv6** 例： `Device(config-if)# vrrp 1 address-family ipv6`	IPv6 用に VRRP グループを作成し、VRRP 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	**track***object-number* **decrement***number* 例： `Device(config-if-vrrp)# track 1 decrement 20`	VRRPv3 グループを使用して IPv6 オブジェクトのステートを追跡するようにトラッキング プロセスを設定します。イーサネット インターフェイス 0/0 の VRRP は、VRRPv3 グループで IPv6 オブジェク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 VRRPv3 の IPv6 オブジェクト ステートがダウンにな

	コマンドまたはアクション	目的
		ると、VRRP グループのプライオリティは 20 だけ引き下げられます。
ステップ 5	**end** 例： `Device(config-if-vrrp)# end`	特権 EXEC モードに戻ります。

VRRPv3 の設定例：オブジェクト トラッキングの統合

例：VRRPv3 を使用した IPv6 オブジェクトのトラッキング

次の例では、トラッキング プロセスは、VRRPv3 グループを使用して IPv6 オブジェクトのステートを追跡するように設定されています。ギガビットイーサネットインターフェイス 0/0/0 の VRRP は、VRRPv3 グループで IPv6 オブジェク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 VRRPv3 の IPv6 オブジェクト 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 20 だけ引き下げられます。

```
Device(config)# fhrp version vrrp v3
Device(config)# interface GigabitEthernet 0/0/0
Device(config-if)# vrrp 1 address-family ipv6
Device(config-if-vrrp)# track 1 decrement 20
```

例：VRRP IPv6 オブジェクト トラッキングの確認

```
Device# show vrrp

Ethernet0/0 - Group 1 - Address-Family IPv4
  State is BACKUP
  State duration 1 mins 41.856 secs
  Virtual IP address is 172.24.1.253
  Virtual MAC address is 0000.5E00.0101
  Advertisement interval is 1000 msec
  Preemption enabled
  Priority is 80 (configured 100)
    Track object 1 state Down decrement 20
  Master Router is 172.24.1.2, priority is 100
  Master Advertisement interval is 1000 msec (learned)
  Master Down interval is 3609 msec (expires in 3297 msec)

Device# show track ipv6 route brief

Track Type        Instance                  Parameter        State Last Change
601   ipv6 route  3172::1/32                metric threshold Down  00:08:55
602   ipv6 route  3192:ABCD::1/64           metric threshold Down  00:08:55
603   ipv6 route  3108:ABCD::CDEF:1/96      metric threshold Down  00:08:55
604   ipv6 route  3162::EF01/16             metric threshold Down  00:08:55
```

```
605   ipv6 route  3289::2/64                metric threshold Down  00:08:55
606   ipv6 route  3888::1200/64             metric threshold Down  00:08:55
607   ipv6 route  7001::AAAA/64             metric threshold Down  00:08:55
608   ipv6 route  9999::BBBB/64             metric threshold Down  00:08:55
611   ipv6 route  1111::1111/64             reachability     Down  00:08:55
612   ipv6 route  2222:3333::4444/64        reachability     Down  00:08:55
613   ipv6 route  5555::5555/64             reachability     Down  00:08:55
614   ipv6 route  3192::1/128               reachability     Down  00:08:55
```

VRRPv3 に関する追加情報：オブジェクト トラッキングの統合

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
HSRP 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、使用に関する注意事項、および例	『*Cisco IOS First Hop Redundancy Protocols Command Reference*』
HSRP のトラブルシューティング	『*Hot Standby Router Protocol: Frequently Asked Questions*』

RFC

RFC	Title
RFC 792	インターネット制御メッセージ プロトコル（*ICMP*）
RFC 1828	『*IP Authentication Using Keyed MD5*』
RFC 5798	『*Virtual Router Redundancy Protocol*』

シスコのテクニカル サポート

説明	Link
★枠で囲まれた Technical Assistance の場合★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。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。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

VRRPv3 の機能情報：オブジェクト トラッキングの統合

表 *15*：*VRRPv3* の機能情報：オブジェクト トラッキングの統合

機能名	リリース	機能情報
VRRPv3：オブジェクト トラッキングの統合	Cisco IOS XE Release 3.10S	VRRPv3：オブジェクト トラッキングの統合機能を使用すると、VRRPv3 グループを使用してオブジェクトを追跡できます。 **fhrpversionvrrpv3**、**showvrrp**、**track (VRRP)** 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。

第 17 章

Virtual Router Redundancy Service

Virtual Router Redundancy Service（VRRS）は、Virtual Router Redundancy Protocol (VRRP)、VRRS 経路、およびオプションの VRRS クライアント間にマルチクライアント情報の抽象化と管理サービスを提供します。VRRS マルチクライアント サービスは、複数の First Hop Redundancy Protocol（FHRP）を抽象化し、FHRP の状態の理想的なビューを提供することで、VRRP との一貫したインターフェイスを提供します。VRRS はデータの更新を管理して、関連するクライアントを 1 か所で登録し、指定された VRRP グループに関する更新を受信できるようにします。

VRRP は VRRP ステータス情報を VRRS 経路および登録済みのすべての VRRS クライアントにプッシュするサーバとして機能します。経路とクライアントは、VRRP から提供されたすべての重要情報に関するステータスを取得します。たとえば、現在と以前の冗長状態、アクティブ状態と非アクティブ状態の レイヤ 2 および レイヤ 3 アドレス、さらに場合によってはネットワーク内の他の冗長ゲートウェイに関する情報などです。拡張されたファースト ホップ ゲートウェイの冗長性を拡張されたインターフェイス環境全体に提供するため、経路はこの情報を使用します。VRRS クライアントもこの情報を使用して、ステートレスおよびステートフル冗長情報をクライアントとプロトコルに提供します。

（注） このモジュールでは、VRRP と VRRPv3 は同じ意味で使用されています。

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。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

VRRS の制約事項

- VRRS プラグインは VRRP グループで設定されていないが、それが従う VRRP グループと物理インターフェイスを共有するサブインターフェイスで設定する必要があります。
- VRRP バージョン 2（VRRPv2）は、ギガビット イーサネット インターフェイスでのみ設定できます。
- VRRS は現在、VRRP バージョン 3（VRRPv3）と使用する場合にのみ使用できます。

VRRS について

VRRS の概要

VRRS は VRRP のスケーラビリティを改善します。VRRS は、VRRP をモニタすることで、VRRS 経路とアプリケーション（VRRS クライアント）にステートレスな冗長性サービスを提供します。VRRS は VRRP の現在の状態のデータベースを提供し、VRRS が通信する VRRS 経路とクライアントに「プッシュ」データ サービスを提供します。VRRP は VRRS サーバとして機能します。VRRS クライアントは、VRRP 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 プロセスまたはアプリケーションです。VRRS 経路は、VRRS データベース情報を使用して、拡張インターフェイス環境全体に拡張ファーストホップ ゲートウェイの冗長性を提供する特殊な VRRS クライアントです。

VRRS 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。VRRP グループに VRRS クライアントをリンクすると、ステートレスまたはステートフル フェールオーバーが実装可能になるように、VRRS でクライアント アプリケーションにサービスを提供できるようにするメカニズムが提供されます。ステートレス フェールオーバーは、状態の同期がないフェールオーバーです。ステートフル フェールオーバーでは、フェールオーバーが発生したときに運用データが失われないように障害の前に所定バックアップとの通信が必要になります。

VRRS 経路はクライアントと同様に動作しますが、VRRS アーキテクチャと統合されます。ユーザが何百ものインターフェイス間で 1 つの仮想アドレスを設定できるようにすることで、ファーストホップ ゲートウェイの冗長性を拡張する方法が提供されます。VRRS経路の「仮想ゲートウェイ」の状態は、FHRP VRRS サーバの状態によります。

VRRP での VRRS の使用

VRRP は VRRS にサーバ サポートを提供します。VRRP サーバは、内部の更新が発生すると、状態とステータス情報をVRRSにプッシュします。VRRSは、サーバの更新を受信すると、内部データベースを更新し、共有名に関連付けられた各VRRSクライアントにプッシュ通知を送信します。クライアントは、グループに関連付けられたプロトコル状態、仮想MAC（vMAC）アドレス、および仮想IPアドレス情報に関心を持っています。クライアントと VRRP グループ間のアソシエーション名は文字名文字列です。VRRS で提供された情報により、クライアントは関連付けられている VRRP グループの状態に依存するさまざまなアクティビティを実行することができます。

VRRPは、現在の状態（マスター、バックアップ、または非動作時の初期状態（INIT））をVRRSに通知します。VRRP状態は経路またはクライアントに渡されます。VRRPグループは、VRRSをアクティベートするために名前を使って設定する必要があります。経路またはクライアントは、VRRS でバインドするために同じ名前で設定する必要があります。

VRRP グループ名は、VRRP グループと同じ名前を持つ VRRS の一部として設定されている任意のクライアントを関連付けます。

VRRS サーバとクライアント

VRRP は VRRS サーバとして機能します。経路およびクライアントは、VRRP サーバの状態で機能します。VRRPグループの状態が変化すると、VRRS経路とクライアントの動作（インターフェイスのシャット ダウン、アカウンティング ログの追加などのタスクの実行）がVRRSから受信した状態により変化します。

VRRS 経路と VRRS Pathway Manager

VRRS 経路

VRRS経路は、イーサネットインターフェイス（物理インターフェイス、サブインターフェイス、またはスイッチ仮想インターフェイス（SVI）など）で次の機能を使用して IPv4 または IPv6 トラフィック転送作業を行うエンティティとして定義されます。

- MACdb を使用したハードウェア ドライバへの vMAC アドレスの挿入と削除。
- IPv4 および IPv6 API を使用した仮想 IP（vIP）の挿入と削除。
- vIP とインターフェイス バーンドイン アドレス（BIA）MAC とを関連付けるためのプロビジョニング。

- vMAC アドレスとインターフェイスが所有する vIP とを関連付けるためのプロビジョニング。
- Address Resolution Protocol（ARP）または Neighbor Discovery Protocol を使用した LAN 上での vMAC と vIP のアソシエーションの維持。
- 接続されたレイヤ 2 デバイスのスイッチング キャッシュ（Content-Addressable Memory（CAM））を LAN 上に維持。
- ハイ アベイラビリティ モジュールでのすべてのデータと経路の状態のチェックポイント。

経路は、VRRS Pathway L2 Controller または VRRS Pathway L3 Controller のいずれかとのアソシエーションを使用して、上記の機能の一部を提供します。

VRRS Pathway Manager

VRRS Pathway Manager は、次の機能を提供します。

- 1 つ以上の VRRS 経路インスタンスと単一のデータベース名エントリとの間にアソシエーションを作成します。
- VRRS からのプッシュに応じて、関連する登録済み経路に、設定と状態情報をプッシュします。
- ユーザにデバッグと出力の表示を提供します。出力は VRRS Pathway Manager の状態と設定に関連しています。
- Online Insertion and Removal（OIR）に対応しており、OIR イベントの影響を受ける可能性がある経路を管理します。
- Virtual Routing and Forwarding（VRF）に対応しており、VRF イベントの影響を受ける可能性がある経路を管理します。

VRRS の設定方法

VRRPv3 制御グループの設定

VRRP 制御グループを設定するには、次の作業を実行します。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **fhrpversionvrrpv3**
4. **interface***typenumber*
5. **ip address***ip-addressmask*
6. **vrrp***group-id***address-family** {**ipv4** | **ipv6**}
7. **address***ip-address* [**primary** | **secondary**]
8. **vrrsleader***vrrs-leader-name*
9. **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	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# 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	**fhrpversionvrrpv3** 例： `Device(config)# fhrp version vrrp v3`	VRRPv3 および VRRS を設定する機能をイネーブルにします。 （注） VRRPv3 が使用中の場合、VRRPv2 は使用できません。
ステップ 4	**interface***typenumber* 例： `Device(config)# interface vlan 40`	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-addressmask* 例： `Device(config-if)# ip address 209.165.200.230 255.255.255.224`	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 6	**vrrp***group-id***address-family** {**ipv4** | **ipv6**} 例： `Device(config-if)# vrrp 1 address-family ipv4`	VRRP グループを作成し、VRRP 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	**address***ip-address* [**primary** | **secondary**] 例： `Device(config-if-vrrp)# address 209.165.202.141`	VRRP グループのプライマリ アドレスまたはセカンダリ アドレスを指定します。
ステップ 8	**vrrsleader***vrrs-leader-name* 例： `Device(config-if-vrrp)# vrrs leader group1`	VRRS に登録するリーダーの名前を指定し、VRRP グループが VRRS 経路を制御できるようにします。 • 1 つの VRRP インスタンスで複数の VRRS グループを制御することも可能です。登録済みの VRRS 名はデフォルトで使用不可になっています。
ステップ 9	**end** 例： `Device(config-if-vrrp)# end`	特権 EXEC モードに戻ります。

VRRS 経路の設定

VRRP 経路を設定するには、次の作業を実行します。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **fhrpversionvrrpv3**
4. **interface***typenumber*
5. **ip address***ip-addressmask*
6. **vrrspathway***vrrs-leader-name*
7. **macaddress***mac-address*
8. **address***ip-address*
9. **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	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# 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	**fhrpversionvrrpv3** 例： `Device(config)# fhrp version vrrp v3`	VRRPv3 および VRRS を設定する機能をイネーブルにします。 （注） VRRPv3 が使用中の場合、VRRPv2 は使用できません。
ステップ 4	**interface***typenumber* 例： `Device(config)# interface vlan 42`	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-addressmask* 例： `Device(config-if)# ip address 209.165.201.25 255.255.255.224`	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	**vrrspathway***vrrs-leader-name* 例： `Device(config-if)# vrrs pathway group1`	VRRS グループの VRRS 経路を定義し、VRRS 経路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	**macaddress***mac-address* 例： `Device(config-if-vrrs-pw)# mac address fe24.fe24.fe24`	経路で使用される MAC アドレスを指定します。
ステップ 8	**address***ip-address* 例： `Device(config-if-vrrs-pw)# address`	経路の仮想 IP を定義します。 • （注） VRRP グループは、複数の経路を制御できます。

	コマンドまたはアクション	目的
	209.165.201.10	
ステップ 9	**end** 例： Device(config-if-vrrs-pw)# end	特権 EXEC モードに戻ります。 • （注） 追加の経路を設定するには、ステップ 1 ～ 9 を繰り返し行います。

VRRS の確認

VRRS の機能を確認するには、次のタスクを実行します。

（注） **show** コマンドは、特定の順序で入力する必要はありません。異なる経路ステートの **show vrrs pathway**（アクティブ、非アクティブ、および「受信不可」）を以下に示します。

手順の概要

1. イネーブル化
2. **show vrrs pathway**
3. **show vrrs pathway**
4. **show vrrs pathway**
5. **show vrrs server**

手順の詳細

ステップ 1 イネーブル化

特権 EXEC モードをイネーブルにします。

例：

```
Device> enable
```

ステップ 2 **show vrrs pathway**

タグ名「group1」を持ち、VRRP が VLAN インターフェイスでマスター ステートにあるアクティブな経路の VRRS 経路情報を表示します。

例：

```
Device# show vrrs pathway
```

```
Pathway ["group1"@Vlan42]
State is ACTIVE [VRRS push "ACTIVE"]
Virtual MAC is fe24.fe24.fe24 [Active] (0)
Address-family is v4
Options: Default Pathway=0, Owner Mode=0, Accept-Mode=1, Configured vMAC=1
Evaluation: No Shut=1, Connected=1, OIR=1, L2 Ready=1, L3 Ready=1, vMAC Ready=1,
vIP Ready=1
Virtual Address List: 209.165.201.10
```

ステップ 3 **show vrrs pathway**

タグ名「group1」を持ち、VRRP が イーサネット 0/1 インターフェイスでバックアップ ステートにある非アクティブな経路の VRRS 経路情報を表示します。

例：

```
Device# show vrrs pathway

Pathway ["group1"@Et0/1]
State is INACTIVE [VRRS push "BACKUP"]
Virtual MAC is 0101.0101.0101 [Reserved] (0)
Address-family is v4
Options: Default Pathway=0, Owner Mode=0, Accept-Mode=1, Configured vMAC=1
Evaluation: No Shut=1, Connected=1, OIR=1, L2 Ready=1, L3 Ready=1, vMAC Ready=1,
vIP Ready=1
Virtual Address List: 209.165.201.10
```

ステップ 4 **show vrrs pathway**

タグ名「group1」を持ち、VRRP が イーサネット 0/1 インターフェイスでバックアップ ステートにある「受信不可」経路の VRRS 経路情報を表示します。

例：

```
Device# show vrrs pathway

Pathway ["group1"@Et0/1]
State is NOT READY [VRRS push "INIT"]
Virtual MAC is 0101.0101.0101 [Reserved] (0)
Address-family is v4
Options: Default Pathway=0, Owner Mode=0, Accept-Mode=1, Configured vMAC=1
Evaluation: No Shut=1, Connected=1, OIR=1, L2 Ready=1, L3 Ready=1, vMAC Ready=1,
vIP Ready=1
Virtual Address List: 209.165.201.10
```

ステップ 5 **show vrrs server**

VRRS サーバ情報を表示します。

例：

```
Device# show vrrs pathway

Pathway ["group1"@Et0/1]
State is INACTIVE [VRRS push "BACKUP"]
Virtual MAC is 0101.0101.0101 [Reserved] (0)
Address-family is v4
Options: Default Pathway=0, Owner Mode=0, Accept-Mode=1, Configured vMAC=1
Evaluation: No Shut=1, Connected=1, OIR=1, L2 Ready=1, L3 Ready=1, vMAC Ready=1,
vIP Ready=1
```

```
Virtual Address List: 209.165.201.10
```

次の表で、サンプル出力の重要なフィールドについて説明します。

フィールド	説明
状態	インターフェイスの VRRS の現在のステート。表示されている値は「ACTIVE」、「INACTIVE」、「NOT READY」、または「BACKUP」のいずれかです。
Virtual MAC	インターフェイス用に予約されている仮想 MAC アドレス。
Address-family	IPv4 または IPv6 アドレス ファミリ。
Default Pathway	値が 1 であれば、経路が VRRP グループから暗黙的に作成されたことを示します。値が 0 であれば、経路が **vrrs pathway** コマンを使用して明示的に作成されたことを示します。
Owner Mode	値が 1 であれば、インターフェイス IP アドレスが指定されていることを示します。
Accept-Mode	値が 1 であれば、特定の仮想 IP アドレスへのトラフィックが受け入れられていることを示します。
Configured vMAC	値が 1 であれば、仮想 MAC アドレスが設定されていることを示します。
No Shut	値が 1 であれば、インターフェイスが no shutdown モードに設定されていることを示します。
接続済み	値が 1 であれば、VRRS 経路が VRRS グループに接続されていることを示しています。
OIR	値が 1 であれば、デバイスのインターフェイス ライン カードの Online Insertion and Removal（OIR）が完了していることを示しています。
L2 Ready	値が 1 であれば、レイヤ 2 インターフェイスがアップしていることを示します。
L3 Ready	値が 1 であれば、レイヤ 3 インターフェイスがアップしていることを示します。

フィールド	説明
vMAC Ready	値が 1 であれば、仮想 MAC アドレスがインターフェイスに割り当てられていることを示します。
vIP Ready	値が 1 であれば、仮想 IP アドレスがインターフェイスに割り当てられていることを示します。
Virtual Address List	仮想 IPv4 または IPv6 アドレスのアドレス一覧。
インターフェイス	経路が定義されるインターフェイスの名前。
vMAC	インターフェイスに割り当てられている仮想 MAC アドレス。
vIP Address	インターフェイスに割り当てられている仮想 IP アドレス。
Tags Connected	インターフェイスの経路に現在接続されている特定のタグ名。

VRRS の設定例

例：VRRPv3 制御グループの設定

次に、VRRPv3 制御グループを設定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# fhrp version vrrp v3
Device(config)# interface vlan 40
Device(config-if)# ip address 209.165.200.230 255.255.255.224
Device(config-if)# vrrp 1 address-family ipv4
Device(config-if-vrrp)# address 209.165.202.141
Device(config-if-vrrp)# vrrs leader group1
Device(config-if-vrrp)# end
```

（注） 上記の例では、グローバル コンフィギュレーション モードで **fhrpversionvrrpv3** コマンドが使用されています。

例：VRRS 経路の設定

次の例は、VRRS 経路を設定する方法を示しています。

```
Device> enable
Device# configure terminal
Device(config)# fhrp version vrrp v3
Device(config)# interface vlan 42
Device(config-if)# ip address 209.165.201.25 255.255.255.224
Device(config-if)# vrrs pathway group1
Device(config-if-vrrs-pw)# mac address fe24.fe24.fe24
Device(config-if-vrrs-pw)# address 209.165.201.10
Device(config-if-vrrs-pw)# end
```

（注） 上記の例では、グローバル コンフィギュレーション モードで **fhrpversionvrrpv3** コマンドが使用されています。

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Master Command List, All Releases』
FHRP コマンド	『First Hop Redundancy Protocols Command Reference』
VRRPv2 の設定	『*First Hop Redundancy Protocols Configuration Guide*』の「Configuring VRRP」モジュール
VRRPv3 プロトコルのサポート	『*First Hop Redundancy Protocols Configuration Guide*』の「VRRPv3 Protocol Support」モジュール

標準および RFC

標準/RFC	Title
RFC5798	『*Virtual Router Redundancy Protocol*』

シスコのテクニカル サポート

説明	Link
★枠で囲まれた Technical Assistance の場合★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。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。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

Virtual Router Redundancy Service の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *16*：***Virtual Router Redundancy Service*** の機能情報

機能名	リリース	機能情報
Virtual Router Redundancy Service	Cisco IOS XE Release 3.8S	VRRS 機能は、VRRP、VRRS 経路、およびオプションの VRRS クライアント間にマルチクライアント情報の抽象化と管理サービスを提供します。 次のコマンドが導入または修正されました。**debugvrrsall**、**debugvrrsdatabase**、**debugvrrslog**、**debugvrrspathway**、**showvrrs**。

索 引

S