



HSRP の設定

Hot Standby Router Protocol (HSRP; ホットスタンバイ ルータ プロトコル) は、ファーストホップ IP ルータのフェールオーバーを透過的に実行できるように作成された First Hop Redundancy Protocol (FHRP; ファーストホップ冗長プロトコル) です。HSRP によるネットワークの高可用性は、イーサネットの IP ホスト、Fiber Distributed Data Interface (FDDI; ファイバ分散データ インターフェイス)、Bridge-Group Virtual Interface (BVI; ブリッジ グループ仮想インターフェイス)、LAN Emulation (LANE; LAN エミュレーション)、またはデフォルト ゲートウェイ IP アドレスを使用して設定されているトークンリング ネットワークでファーストホップ ルーティングの冗長性を確保することによって実現されます。HSRP は、アクティブ ルータとスタンバイ ルータを選択するために一連のルータで使用されます。一連のルータ インターフェイスでは、アクティブ ルータはパケットのルーティング用に選択されたルータであり、スタンバイ ルータは、アクティブ ルータに障害が発生したり、事前に設定した条件に一致したりしたときに処理を引き継ぐルータです。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。この章に記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「[HSRP の機能情報](#)」(P.67) を参照してください。

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

この章の構成

- 「[HSRP の制約事項](#)」(P.2)
- 「[HSRP の概要](#)」(P.2)
- 「[HSRP の設定方法](#)」(P.20)
- 「[HSRP の設定例](#)」(P.56)
- 「[その他の参考資料](#)」(P.65)

- 「HSRP の機能情報」 (P.67)
- 「用語集」 (P.72)

HSRP の制約事項

- HSRP は、マルチアクセス、マルチキャスト、またはブロードキャストに対応したイーサネット LAN で使用するように設計されており、既存のダイナミック プロトコルの代用として想定されているわけではありません。
- HSRP は、イーサネット、FDDI、BVI、LANE、またはトークン リングのインターフェイスで設定できます。各トークン リング インターフェイスは最大で 3 つのホット スタンバイ グループに対応し、グループ番号は 0、1、2 が割り当てられます。
- Lance イーサネット ハードウェアを使用する Cisco 2500 シリーズ、Cisco 3000 シリーズ、Cisco 4000 シリーズ、Cisco 4500 の各ルータは、1 つのイーサネット インターフェイス上の複数のホット スタンバイ グループをサポートしていません。PQUICC イーサネット ハードウェアを使用する Cisco 800 シリーズと Cisco 1600 シリーズは、1 つのイーサネット インターフェイス上の複数のホット スタンバイ グループをサポートしていません。1 つの回避策として、インターフェイス コンフィギュレーション コマンド **standby use-bia** を使用することができます。このコマンドは、事前に割り当てられた MAC アドレスではなく、インターフェイスのバーンドイン アドレスを仮想 MAC アドレスとして使用します。
- HSRP の Bidirectional Forwarding Detection (BFD; 双方向フォワーディング検出) サポートは、すべてのプラットフォームとインターフェイスで有効とは限りません。
- 同一の HSRP グループ番号または HSRP MAC アドレスを、同じメジャー インターフェイスの別々のサブインターフェイスで設定することはできません。



(注) この制限は、Cisco IOS Release 12.4(14)、12.4(15)T、12.2(33)SRB、12.2(33)SXH と、これらの Cisco IOS リリースの以降のリリースで解消されています。

- Enhanced Object Tracking (EOT; 拡張オブジェクト トラッキング) は、Stateful Switchover (SSO; ステートフル スイッチオーバー) 対応ではなく、SSO モードで HSRP と使用することはできません。

HSRP の概要

- 「HSRP の動作」 (P.3)
- 「HSRP バージョン 2 の設計」 (P.4)
- 「HSRP バージョン 2 の設計」 (P.4)
- 「HSRP の利点」 (P.6)
- 「HSRP グループとグループのアトリビュート」 (P.6)
- 「HSRP のプリエンプション」 (P.6)
- 「HSRP のプライオリティとプリエンプション」 (P.7)
- 「オブジェクト トラッキングが HSRP ルータのプライオリティに与える影響」 (P.7)
- 「HSRP のアドレス指定」 (P.7)
- 「HSRP 仮想 MAC アドレスと BIA MAC アドレス」 (P.8)

- 「HSRP タイマー」 (P.8)
- 「HSRP の MAC リフレッシュ間隔」 (P.9)
- 「HSRP のテキスト認証」 (P.9)
- 「HSRP MD5 認証」 (P.9)
- 「HSRP の IPv6 サポート」 (P.10)
- 「HSRP のメッセージとステート」 (P.10)
- 「HSRP と ARP」 (P.11)
- 「HSRP gratuitous ARP」 (P.11)
- 「HSRP のオブジェクト トラッキング」 (P.12)
- 「HSRP の ICMP リダイレクト サポート」 (P.12)
- 「HSRP グループ シャットダウン」 (P.15)
- 「HSRP の MPLS VPN サポート」 (P.16)
- 「HSRP 複数グループ最適化」 (P.16)
- 「HSRP - ISSU」 (P.17)
- 「SSO HSRP」 (P.17)
- 「HSRP の BFD ピアリング」 (P.18)
- 「HSRP MIB トラップ」 (P.19)

HSRP の動作

ほとんどの IP ホストには、デフォルト ゲートウェイとして設定された 1 台のルータの IP アドレスが指定されています。HSRP を使用すると、ルータの IP アドレスではなく、HSRP 仮想 IP アドレスがホストのデフォルト ゲートウェイとして設定されます。

HSRP は、ICMP Router Discovery Protocol (IRDP) などのルータ ディスカバリ プロトコルをサポートしないホストや、選択したルータがリロードしたときやオフになったときに新しいルータに切り替える機能を備えていないホストには特に有効です。また、既存の TCP セッションはフェールオーバーが発生しても存続するため、このプロトコルでは IP トラフィックをルーティングするためにネクストホップを動的に選択するホストの回復をさらに透過的に実行できます。

HSRP は、ネットワーク セグメントで設定されている場合、仮想 MAC アドレスと、HSRP を実行しているルータのグループで共有される IP アドレスを用意します。この HSRP ルータ グループのアドレスが**仮想 IP アドレス**と呼ばれます。グループのうちの 1 台がプロトコルによって選択され、アクティブルータになります。アクティブ ルータはグループの MAC アドレスを宛先とするパケットを受け取ってルーティングします。HSRP を実行している n 台のルータでは、 $n + 1$ 個の IP アドレスと MAC アドレスが割り当てられます。

指定されたアクティブ ルータの障害を HSRP が検出すると、選択されているスタンバイ ルータがホットスタンバイグループの MAC アドレスと IP アドレスの制御を引き継ぎます。このとき、新しいスタンバイ ルータも選択されます。

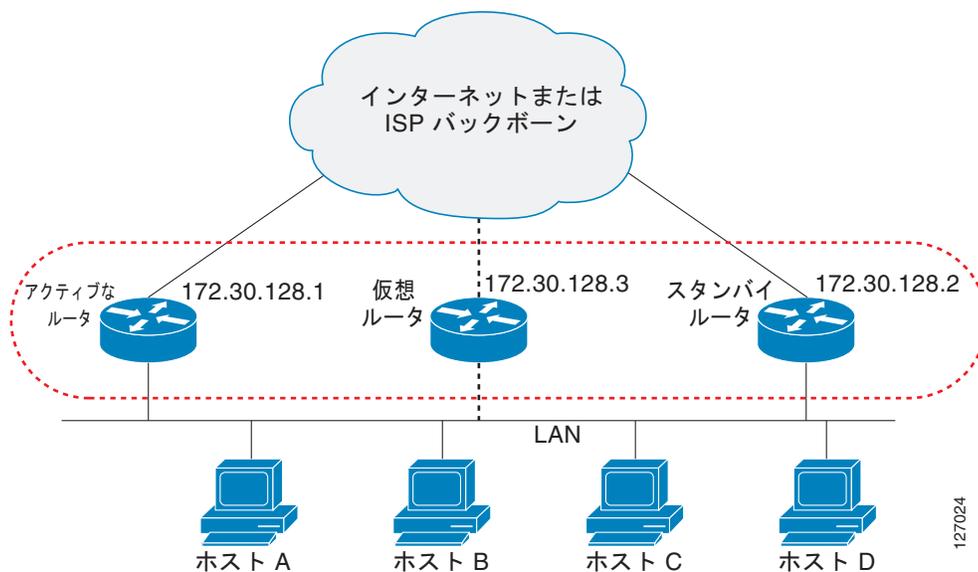
HSRP が設定されているルータのうち、どのルータをデフォルトのアクティブ ルータにするかを決定するために HSRP でプライオリティ メカニズムが使用されます。ルータをアクティブ ルータとして設定するためには、HSRP が設定された他のいずれのルータよりも高いプライオリティを割り当てます。デフォルトのプライオリティは 100 であるため、それを超えるプライオリティを 1 台のルータだけに割り当てれば、それがデフォルトのアクティブ ルータになります。

HSRP を実行しているルータは、User Datagram Protocol (UDP; ユーザ データグラム プロトコル) ベースのマルチキャスト hello メッセージを送信および受信して、ルータの障害を検出したり、アクティブ ルータとスタンバイ ルータを割り当てたりします。設定した時間内にアクティブ ルータが hello メッセージを送信できないと、プライオリティが最も高いスタンバイ ルータがアクティブ ルータになります。このようにパケット転送機能が別のルータに移行しても、ネットワークのいずれのホストにもまったく影響はありません。

複数のホット スタンバイ グループをインターフェイスに設定できるので、冗長ルータおよびロード シェアリングを余すところなく活用できるようになっています。

図 1 は、HSRP 用に構成されたネットワークを示しています。仮想 MAC アドレスおよび IP アドレスを共有することによって、複数台のルータが 1 台の仮想ルータとして機能します。仮想ルータは物理的には存在しませんが、互いのバックアップになるように設定されている複数のルータの共有のデフォルト ゲートウェイになります。LAN 上のホストは、アクティブ ルータの IP アドレスを使用して設定する必要はありません。その代わりに、仮想ルータの IP アドレス (仮想 IP アドレス) をデフォルト ゲートウェイとして使用して設定します。設定した時間内にアクティブ ルータが hello メッセージを送信できない場合、スタンバイ ルータが処理を引き継いで仮想アドレスに対応するアクティブ ルータになり、アクティブ ルータの役割を引き受けます。

図 1 HSRP のトポロジ



HSRP は Inter-Switch Link (ISL; スイッチ間リンク) でカプセル化を行うことによってサポートされます。『Cisco IOS LAN Switching Configuration Guide』(リリース 12.4) の「Configuring Routing Between VLAN」という章の「Virtual LANs」を参照してください。

HSRP バージョン 2 の設計

HSRP バージョン 2 は、バージョン 1 の次の問題が解消されるように設計されています。

- 以前は、ミリ秒のタイマー値はアドバタイズまたは検出されませんでした。HSRP バージョン 2 では、ミリ秒のタイマー値がアドバタイズおよび検出されます。この変更により、あらゆる状況での HSRP グループの安定性が確保されています。
- グループ番号の範囲が 0 ~ 255 に制限されていました。HSRP バージョン 2 では、グループ番号の範囲が 0 ~ 4095 に拡大されています。

- HSRP バージョン 2 では、管理性とトラブルシューティング機能が向上しています。HSRP バージョン 1 では、発信元 MAC アドレスが HSRP 仮想 MAC アドレスであったため、メッセージを送信した物理ルータをアクティブな HSRP hello メッセージから特定する方法がありませんでした。HSRP バージョン 2 のパケット形式には、メッセージの送信元を一意に特定するための 6 バイトの識別子フィールドが組み込まれています。通常は、インターフェイスの MAC アドレスがこのフィールドに格納されます。
- HSRP hello メッセージの送信にマルチキャスト アドレス 224.0.0.2 が使用されていました。このアドレスは、Cisco Group Management Protocol (CGMP; シスコ グループ管理プロトコル) の脱退処理と競合することがあります。

バージョン 1 は HSRP のデフォルトのバージョンです。

HSRP バージョン 2 は、新しい IP マルチキャスト アドレス 224.0.0.102 を使用して hello パケットを送信します。バージョン 1 で使用されるマルチキャスト アドレス 224.0.0.2 は使用されません。この新しいマルチキャスト アドレスにより、CGMP の脱退処理を HSRP と同時にイネーブルにすることができます。

HSRP バージョン 2 では、グループ番号の範囲が拡張され、0 ~ 4095 までの番号を使用できるようになったため、0000.0C9F.F000 ~ 0000.0C9F.FFFF の新しい MAC アドレス範囲を使用できます。グループ番号の範囲が拡張されたといっても、インターフェイスがそれほどの数の HSRP グループをサポートできる (サポートするはずである) というものではありません。グループ番号の範囲が拡張されたのは、グループ番号をサブインターフェイスの VLAN 番号に一致させることができるようにするためです。

各グループに新しい仮想 MAC アドレスが指定されるため、HSRP バージョンを変更するときは、各グループが再度初期化されます。

HSRP バージョン 2 のパケット形式は、バージョン 1 とは異なります。このパケット形式には、Type-Length-Value (TLV; タイプ、長さ、値) 形式が使用されています。HSRP バージョン 1 のルータが受信した HSRP バージョン 2 のパケットのタイプ フィールドは、HSRP バージョン 1 によってバージョン フィールドにマッピングされ、それ以降は無視されます。

また、Gateway Load Balancing Protocol (GLBP; ゲートウェイ ロード バランシング プロトコル) でも、HSRP バージョン 2 によって解消されている HSRP バージョン 1 の同じ問題が解消されます。GLBP の詳細については、『[Configuring GLBP](#)』を参照してください。

HSRP の設定の変更

Cisco IOS Release 12.2(33)SXI、12.4(24)T、12.2(33)SRE 以降のリリースでは、セカンダリ インターフェイスの IP アドレスのサブネットに一致する仮想 IP アドレスで HSRP グループを設定できます。

セカンダリ インターフェイスの IP アドレスと同じネットワーク ID で HSRP グループの仮想 IP アドレスを設定すると、HSRP メッセージの送信元アドレスは最適なインターフェイス アドレスに自動的に設定されます。この設定の変更により、次の設定が可能になっています。

```
interface Ethernet1/0
 ip address 192.168.1.1 255.255.255.0
 ip address 192.168.2.1 255.255.255.0 secondary
 standby 1 ip 192.168.1.254
 standby 1 priority 105
 standby 1 preempt
 standby 2 ip 192.168.2.254 !Same network ID as secondary interface
```

Cisco IOS Release 12.2(33)SXI、12.4(24)T、12.2(33)SRE よりも前のリリースでは、HSRP 仮想 IP アドレスのネットワーク ID がプライマリ インターフェイスのアドレスと同じ場合を除き、HSRP グループは INIT ステートのままです。

さらに、設定されているインターフェイス アドレスがないのに HSRP グループ アドレスを設定すると、次の警告メッセージが表示されます。

```
% Warning: address is not within a subnet on this interface
```

HSRP の利点

冗長性

HSRP には、実績があり、大規模ネットワークで広範に導入されている冗長性方式が採用されています。

高速なフェールオーバー

HSRP では、ファーストホップ ルータのフェールオーバーが、透過的かつ高速に実行されます。

プリエンブション

プリエンブションにより、スタンバイ ルータがアクティブになるのを一定時間遅らせることができます（この時間は設定可能です）。

認証

HSRP の Message Digest 5 (MD5; メッセージ ダイジェスト 5) アルゴリズム認証は、HSRP スピーキング 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

Command-Line Interface (CLI; コマンドライン インターフェイス) を使用して、グループの属性を次に適用できます。

- 1 つの HSRP グループ：インターフェイス コンフィギュレーション モードで実行され、1 つのグループに適用されます。
- インターフェイスのすべてのグループ：インターフェイス コンフィギュレーション モードで実行され、インターフェイスのすべてのグループに適用されます。
- すべてのインターフェイスのすべてのグループ：グローバル コンフィギュレーション モードで実行され、すべてのインターフェイスのすべてのグループに適用されます。

HSRP のプリエンブション

新規にリロードされたルータが HSRP アクティブ ルータになったとき、HSRP アクティブ ルータが既に存在していた場合は、HSRP のプリエンブションが機能していないように見えることがあります。この現象が発生する原因は、新しい HSRP アクティブ ルータが現在の HSRP アクティブ ルータから hello パケットを受信しておらず、プリエンブション設定が新しいルータの決定で考慮されないためです。

この現象は、インターフェイスが受信するパケットで遅延が発生することのある、Cisco 7600 シリーズのルータなどの一部の大規模なプラットフォームで発生する可能性があります。

通常は、すべての HSRP ルータを次のように設定することを推奨します。

```
standby delay minimum 30 reload 60
```

インターフェイス コンフィギュレーション コマンド **standby delay minimum reload** は、インターフェイスが起動した後、指定した時間が経過するまで HSRP グループの初期化を遅延します。

これは、HSRP プリエンプションによる遅延をイネーブルにするインターフェイス コンフィギュレーション コマンド **standby preempt delay** とは別のコマンドです。

HSRP のプライオリティとプリエンプション

プリエンプションを設定すると、プライオリティが最も高い HSRP ルータがすぐにアクティブ ルータになることができます。プライオリティの判定は、まず設定されているプライオリティ値で行われ、次に IP アドレスで行われます。値が同じ場合は、プライマリ IP アドレスが比較され、IP アドレスが高いほうが優先されます。いずれの場合も、値が高いほうがプライオリティが高くなります。ルータを設定するときにインターフェイス コンフィギュレーション コマンド **standby preempt** を使用しないと、そのルータは、他のすべてのルータよりもプライオリティが高い場合でもアクティブなルータになりません。

プライオリティが同じで、高い IP アドレスが設定されているスタンバイ ルータがアクティブ ルータに取って代わることはありません。

ルータは、最初に起動したとき、完全なルーティング テーブルを保持していません。プリエンプションの遅延を設定して、設定した時間にわたってプリエンプションを遅延することができます。この遅延により、ルータはアクティブ ルータになる前にルーティング テーブルを構築することができます。

プリエンプションがイネーブルになっていない場合、アクティブ ルータから **hello** メッセージを受け取っていないか、あるルータがアクティブ ルータに取って代わっているように見えることがあります。

オブジェクト トラッキングが HSRP ルータのプライオリティに与える影響

オブジェクト トラッキングが設定されている場合に、追跡対象のオブジェクトがダウンすると、デバイスのプライオリティはダイナミックに変化します。トラッキング プロセスは、追跡対象オブジェクトを定期的にポーリングし、値に変化がないかどうかを確認します。トラッキング対象のオブジェクトの変化は、すぐに HSRP に伝えられるか、指定した遅延時間が経過してから HSRP に伝えられます。オブジェクトの値は、アップまたはダウンとして報告されます。トラッキング可能なオブジェクトには、インターフェイスのライン プロトコル ステータスや IP ルートの到達可能性などがあります。指定したオブジェクトがダウンすると、HSRP プライオリティが引き下げられます。このとき、プライオリティの高いほうの HSRP ルータは、**standby preempt** が設定されていれば、アクティブ ルータになることができます。オブジェクト トラッキングの詳細については、「[HSRP のオブジェクト トラッキングの設定](#)」(P.26) を参照してください。

HSRP のアドレス指定

HSRP ルータが互いに通信するときは、HSRP hello パケットをやり取りします。このパケットは、UDP ポート 1985 の宛先 IP マルチキャスト アドレス 224.0.0.2 (すべてのルータとの通信に使用される予約済みのマルチキャスト アドレス) に送信されます。アクティブ ルータは、それ自身に設定されている IP アドレスと HSRP 仮想 MAC アドレスを hello パケットの送信元とし、スタンバイ ルータは、それ自身に設定されている IP アドレスとインターフェイス MAC アドレスを hello パケットの送信元とします。この MAC アドレスは、バーンドイン MAC アドレス (BIA) である場合も、そうでない場合もあります。

ホストは、HSRP 仮想 IP アドレスとしてデフォルト ゲートウェイを使用して設定されるため、HSRP 仮想 IP アドレスに関連付けられている MAC アドレスと通信する必要があります。この MAC アドレスは、0000.0C07.ACxy で構成される仮想 MAC アドレスです。この xy はそれぞれのインターフェイスに基づいた 16 進数の HSRP グループ番号です。たとえば、HSRP グループ 1 は 0000.0C07.AC01 という HSRP 仮想 MAC アドレスを使用します。隣接する LAN セグメントのホストは通常の Address Resolution Protocol (ARP; アドレス解決プロトコル) を使用して、対応する MAC アドレスを解決します。

トークンリングインターフェイスは、HSRP MAC アドレスに機能アドレスを使用します。機能アドレスは、使用できる唯一の汎用マルチキャストメカニズムです。使用可能なトークンリングの機能アドレスの数は限られており、大半は他の機能のために予約されています。HSRP で使用可能なアドレスは次の 3 つだけです。

- c000.0001.0000 (グループ 0)
- c000.0002.0000 (グループ 1)
- c000.0004.0000 (グループ 2)

したがって、インターフェイス コンフィギュレーション コマンド **standby use-bia** が設定されている場合を除き、トークンリングインターフェイスで設定できる HSRP グループは 3 つだけです。

HSRP バージョン 2 は、新しい IP マルチキャストアドレス 224.0.0.102 を使用して hello パケットを送信します。バージョン 1 で使用されるマルチキャストアドレス 224.0.0.2 は使用されません。この新しいマルチキャストアドレスにより、Cisco Group Management Protocol (CGMP; シスコグループ管理プロトコル) の脱退処理を HSRP と同時にイネーブルにすることができます。

HSRP バージョン 2 では、グループ番号の範囲が拡張され、0 ~ 4095 までの番号を使用できるようになったため、0000.0C9F.F000 ~ 0000.0C9F.FFFF の新しい MAC アドレス範囲を使用できます。

HSRP 仮想 MAC アドレスと BIA MAC アドレス

各 HSRP ルータの仮想 MAC アドレスはルータで自動的に生成されます。ただし、Advanced Peer-to-Peer Networking (APPN; 拡張分散ネットワーク機能) などの一部のネットワーク実装では、MAC アドレスを使用して、ルーティングのためのファーストホップを特定します。この場合、グループで **standby mac-address** コマンドを使用して仮想 MAC アドレスを指定できるようになっていなければならないことがよくあります。このようなプロトコルでは、仮想 IP アドレスは重要ではありません。

standby use-bia コマンドは、トークンリングインターフェイスの HSRP MAC アドレスに機能アドレスを使用するという制限を解消するために実装されています。このコマンドを使用すると、HSRP グループは HSRP 仮想 MAC アドレスではなく、インターフェイスの BIA MAC アドレスを使用できるようになります。HSRP が複数リングのソースルートブリッジング環境で実行されていて、異なるリングに HSRP ルータが存在する場合に、**standby use-bia** コマンドを設定すると、Routing Information Field (RIF; ルーティング情報フィールド) に関する混乱を防ぐことができます。

standby use-bia コマンドはインターフェイスに適用され、**standby mac-address** コマンドは HSRP グループに適用されます。

HSRP タイマー

各 HSRP ルータには、hello メッセージのタイミング管理に使用されるアクティブタイマー、スタンバイタイマー、hello タイマーの 3 つのタイマーがあります。タイマーが時間切れになると、ルータは新しい HSRP ステートに変化します。タイマー値が設定されていないルータやアクセスサーバは、アクティブルータやスタンバイルータからタイマー値を取得できます。アクティブルータに設定されているタイマーは、常に他のいずれのタイマー設定よりも優先されます。ホットスタンバイグループのすべてのルータは同じタイマー値を使用する必要があります。

HSRP バージョン 1 では、ミリ秒のタイマー値が使用されている場合を除き、アクティブでないルータはタイマー値をアクティブルータから取得します。ミリ秒のタイマー値が使用されている場合は、すべてのルータはミリ秒のタイマー値を使用して設定されていなければなりません。このルールは、hello 時間とホールド時間のどちらかがミリ秒単位で指定されている場合に当てはまります。この設定が必要なのは、HSRP hello パケットはタイマー値を秒単位でアドバタイズするためです。HSRP バージョン 2 には、この制限はありません。このバージョンではタイマー値がミリ秒単位でアドバタイズされます。

HSRP の MAC リフレッシュ間隔

HSRP が FDDI で動作している場合、ラーニングブリッジやスイッチの MAC キャッシュをリフレッシュするためにパケットを送信する間隔を変更することができます。FDDI インターフェイスの HSRP hello パケットが使用するのは MAC 仮想アドレスではなく Burned-In Address (BIA; バーンドインアドレス) です。リフレッシュ パケットは、スイッチやラーニングブリッジの MAC キャッシュを最新の状態に保ちます。また、複数グループのスレーブとして設定されている HSRP グループは定期的に hello メッセージを送信しないため、このような HSRP グループに対しても使用されます。

FDDI リングでのリフレッシュ間隔を延長または短縮して、帯域幅をさらに効率的に使用することができます。MAC リフレッシュ パケットが不要な場合 (FDDI を使用しているがラーニングブリッジやスイッチが存在しない場合) は、MAC リフレッシュ パケットが送信されないようにすることが可能です。

HSRP のテキスト認証

HSRP は、認証されていない HSRP メッセージを無視します。デフォルトの認証タイプはテキスト認証です。

HSRP 認証は、サービス拒絶攻撃を引き起こす偽の HSRP hello パケットから保護します。たとえば、ルータ A のプライオリティが 120 で、これがアクティブルータであるとします。あるホストが、プライオリティが 130 の偽の HSRP hello パケットを送信すると、ルータ A はアクティブルータとしての動作を停止します。ルータ A に偽の HSRP hello パケットを無視するような認証が設定されていれば、ルータ A はアクティブルータのままです。

HSRP パケットが拒否されるのは、次のいずれかの場合です。

- ルータと着信パケットの認証方式が異なる。
- ルータと着信パケットのテキスト認証文字列が異なる。

HSRP MD5 認証

HSRP MD5 認証の導入前、HSRP は単純なプレーン テキスト文字列でプロトコル パケットを認証していました。HSRP MD5 認証は、マルチキャスト HSRP プロトコル パケットの HSRP 部分の MD5 ダイジェストを生成するように拡張された認証方式です。この機能により、セキュリティが強化され、HSRP スプーフィング ソフトウェアの脅威に対する保護が得られます。

MD5 認証は、代替となるプレーン テキスト認証スキームよりも高いセキュリティを実現します。HSRP グループの各メンバーは秘密キーを使用して、発信パケットの一部となるキー付き MD5 ハッシュを生成できます。着信パケットからはキー付きハッシュが生成されますが、このハッシュと着信パケット内のハッシュが一致しない場合は、パケットは無視されます。

MD5 ハッシュのキーは、キー スtring を使用して設定に直接指定することもできますし、キーチェーンを通して間接的に提供することもできます。

HSRP には次の 2 つの認証方式があります。

- プレーン テキスト認証
- MD5 認証

HSRP 認証は、サービス拒絶攻撃を引き起こす偽の HSRP hello パケットから保護します。たとえば、ルータ A のプライオリティが 120 で、これがアクティブルータであるとします。あるホストが、プライオリティが 130 の偽の HSRP hello パケットを送信すると、ルータ A はアクティブルータとしての動作を停止します。ルータ A に偽の HSRP hello パケットを無視するような認証が設定されていれば、ルータ A はアクティブルータのままです。

HSRP パケットが拒否されるのは、次のいずれかの場合です。

- ルータと着信パケットの認証方式が異なる。
- ルータと着信パケットの MD5 ダイジェストが異なる。
- ルータと着信パケットのテキスト認証文字列が異なる。

HSRP の IPv6 サポート

ほとんどの IPv4 ホストでは、1 台のルータの IP アドレスがデフォルト ゲートウェイとして設定されています。HSRP を使用すると、ルータの IP アドレスではなく、HSRP 仮想 IP アドレスがホストのデフォルト ゲートウェイとして設定されます。2 つの HSRP グループを使用し、ある仮想 IP アドレスでホストの半分を設定し、別の仮想 IP アドレスで残りのホストを設定することによって、簡単なロードシェアリングが実現できます。

それに対して、IPv6 ホストは IPv6 ネイバー探索の Router Advertisement (RA; ルータ アドバタイズメント) メッセージを使用して、使用可能な IPv6 ルータを検出します。メッセージは定期的にマルチキャストされるほか、ホストから要求されることもあります。HSRP は IPv6 ホストに仮想ファーストホップのみを伝えるように設計されています。

HSRP IPv6 グループには、HSRP グループ番号から生成される仮想 MAC アドレスと、デフォルトで HSRP 仮想 MAC アドレスから生成される仮想 IPv6 リンクローカル アドレスがあります。HSRP IPv6 が使用する MAC アドレス範囲は 0005.73A0.0000 ~ 0005.73A0.0FFF です。HSRP グループがアクティブになっているときは、HSRP 仮想 IPv6 リンクローカル アドレスに RA が定期的に送信されます。HSRP グループがアクティブ ステートではなくなると、最後の RA が送信された後、定期的な RA の送信は停止します。

最後の RA が送信された後、インターフェイスのリンクローカル アドレスへの 定期的な RA の送信は停止しますが、インターフェイスには少なくとも 1 つの 仮想 IPv6 リンクローカル アドレスが設定されています。インターフェイスの IPv6 リンクローカル アドレスには、RA に関して挙げられているものを除き、制限は発生しません。他のプロトコルは、このアドレスに対するパケットの送信と受信を引き続き実行します。

HSRP が設定されているルータのうち、どのルータをデフォルトのアクティブ ルータにするかを決定するために HSRP でプライオリティ メカニズムが使用されます。ルータをアクティブ ルータとして設定するためには、HSRP が設定された他のいずれのルータよりも高いプライオリティを割り当てます。デフォルトのプライオリティは 100 であるため、それを超えるプライオリティを 1 台のルータだけに割り当てれば、それがデフォルトのアクティブ ルータになります。

詳細については、『Cisco IOS IPv6 Configuration Guide』の「[Configuring First Hop Redundancy Protocols in IPv6](#)」を参照してください。

HSRP のメッセージとステート

HSRP を使用して設定されているルータは、次の 3 種類のマルチキャスト メッセージをやり取りします。

- **hello** : hello メッセージは、ルータの HSRP プライオリティとステートに関する情報を他の HSRP ルータに伝達します。
- **coup** : スタンバイ ルータは、アクティブ ルータの機能を引き継ぐときに coup メッセージを送信します。
- **resign** : アクティブ ルータであるルータは、シャットダウンする直前や、もっとプライオリティの高いルータから hello メッセージまたは coup メッセージを受け取ったときに、このメッセージを送信します。

常に、HSRP を使用して設定されているルータは次のいずれかのステートになっています。

- **Active** : ルータはパケット転送機能を実行しています。
- **Standby** : ルータはアクティブ ルータに障害が発生した場合にパケット転送機能を引き継ぐことができる状態になっています。
- **Speak** : ルータは hello メッセージの送受信中です。
- **Listen** : ルータは hello メッセージの受信中です。
- **Learn** : ルータは、仮想 IP アドレスを特定しておらず、アクティブ ルータからの認証済みの hello メッセージをまだ受信していません。このステートでは、ルータはアクティブ ルータからのメッセージを引き続き待機します。
- **Init** または **Disabled** : ルータは HSRP に参加する準備ができていないか、参加できない状態です。対応するインターフェイスが起動されていない可能性があります。スヌーピングによって検出されたネットワークの他のルータで設定されている HSRP グループは、**Init** ステートであると表示されます。また、停止しているインターフェイスを使用してローカルで設定されているグループや、指定したインターフェイス IP アドレスを持たないグループも、**Init** ステートであると表示されます。

Cisco IOS Release 12.2(33)SXH 以降の Cisco IOS 12.2SX リリース、Cisco IOS Release 12.2(33)SRB 以降の Cisco IOS 12.2SR リリース、Cisco IOS Release 12.4(8) 以降の Cisco IOS 12.4 リリースでは、HSRP は、HSRP ステートの変化に関する syslog メッセージにログ レベル 5 を使用してイベントをログ記録し、ルータの syslog バッファがプライオリティの低いレベル 6 のメッセージでいっぱいにならないようにしています。

これらのリリースよりも前の Cisco IOS ソフトウェアは、HSRP ステートの変化に関する syslog メッセージにログ レベル 6 を使用します。

HSRP と ARP

HSRP は、ホストがプロキシ ARP に対応するように設定されているときも機能します。アクティブ HSRP ルータは、ローカル LAN に存在しないホストの ARP 要求を受信すると、仮想ルータの MAC アドレスを使用して応答します。このアクティブ ルータが使用不能になるか、リモート LAN への接続が失われると、アクティブ ルータになったルータが、仮想ルータ宛てにアドレス指定されたパケットを受信し、適切に転送します。インターフェイスがホットスタンバイ状態になっていない場合は、プロキシ ARP 応答は実行されません。

HSRP gratuitous ARP

HSRP gratuitous ARP 機能により、HSRP は ARP キャッシュ内のエントリが正しいことを確認し、1 つまたは複数のアクティブ HSRP グループから gratuitous ARP パケットを定期的送信するように設定されます。HSRP は、デフォルトでは HSRP グループのステートが **Active** に変化したときに、そのグループから gratuitous ARP パケットを 3 個送信します。最初の 1 個はグループがアクティブになったときに送信しますが、残りの 2 個が送信されるのは 2 秒後と 4 秒後です。

HSRP gratuitous ARP 機能によって HSRP の機能が拡張され、アクティブ HSRP グループから送信される gratuitous ARP パケットの数と頻度を設定できるようになっています。指定した間隔で特定の数の gratuitous ARP パケットが送信されるように設定するには、**standby arp gratuitous** コマンドをインターフェイス コンフィギュレーション モードで使用します。

アクティブなグループごとに 1 つの gratuitous ARP パケットを送信するように HSRP を設定するには、**standby send arp** コマンドを EXE モードで使用します。**standby send arp** コマンドが設定されると、HSRP は gratuitous ARP パケットを送信する前に ARP キャッシュのエントリが正しいことを確認します。ARP エントリが正しくない場合、HSRP は ARP エントリを再度追加します。スタティック ARP エントリやエイリアス ARP エントリは HSRP によって上書きされることはありません。

standby send arp コマンドを設定すると、CPU 利用率の高いプロセスや設定が開始される前にホストの ARP キャッシュが更新される状態になります。

適度にソフトウェア スイッチングされた IP トラフィックと大量の ARP トラフィックが一緒になって CPU 利用率が 50% を上回ると、ARP リフレッシュ要求が正常に実行されず、一部のアプリケーション サーバがデフォルト ゲートウェイの ARP エントリを失って、残りのネットワークと通信できなくなります。場合によっては、大規模なアクセス リストをイネーブル化するなどの操作によってホストからの ARP 要求が遅延して、ホストにデフォルト ゲートウェイがない状態が短時間発生することがあります。HSRP アクティブ ルータから定期的送信される gratuitous ARP パケットは、期限切れになる前にホストの ARP キャッシュをリフレッシュします。

HSRP のオブジェクト トラッキング

オブジェクト トラッキングにより、HSRP からトラッキング メカニズムが分離され、HSRP だけでなく、他のプロセスも使用可能な独立したトラッキング プロセスが別に生成されます。デバイスのプライオリティがオブジェクト トラッキング用に設定されているときに、トラッキング対象のオブジェクトがダウンすると、デバイスのプライオリティが動的に変更されることがあります。トラッキング可能なオブジェクトには、インターフェイスのライン プロトコル ステートや IP ルートの到達可能性などがあります。指定したオブジェクトがダウンすると、HSRP プライオリティが引き下げられます。

HSRP、Virtual Router Redundancy Protocol (VRRP; 仮想ルータ冗長プロトコル)、Gateway Load Balancing Protocol (GLBP; ゲートウェイ ロード バランシング プロトコル) などのクライアント プロセスは、オブジェクトのトラッキングを登録し、トラッキング対象オブジェクトのステートが変化したときに通知を得ることができるようになっています。

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

HSRP の ICMP リダイレクト サポート

ICMP は、ネットワーク層のインターネット プロトコルで、IP 処理に関連するエラーなどの情報をレポートするメッセージ パケットを生成します。ICMP はエラー パケットをホストに送信したり、リダイレクト パケットをホストに送信したりすることができます。

HSRP を実行しているときは、HSRP グループに属するルータのインターフェイス (または実際の) IP アドレスをホストが検出しないようにすることが重要です。ICMP によってホストがルータの実際の IP アドレスにリダイレクトされた場合、そのルータに後で障害が発生すると、そのホストからのパケットは失われます。

ICMP リダイレクト メッセージは、HSRP を使用して設定されているインターフェイスで自動的にイネーブルになります。この機能は、ネクストホップ IP アドレスが HSRP 仮想 IP アドレスに変更されることのある HSRP で発信 ICMP リダイレクト メッセージをフィルタリングすることによって効果を発揮します。

アクティブ HSRP ルータへの ICMP リダイレクト

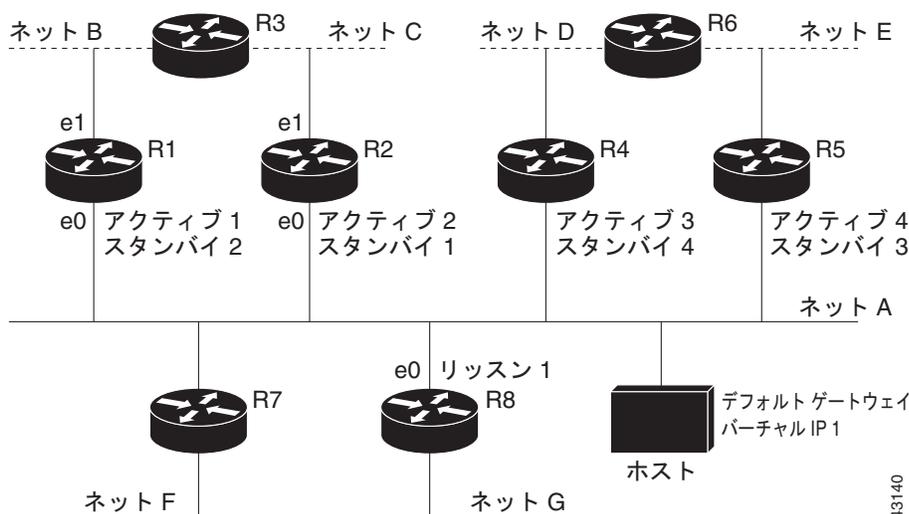
ネクストホップ IP アドレスは、そのネットワークのアクティブ HSRP ルータのリストと比較されます。一致が見つかり、実際のネクストホップ IP アドレスが、対応する仮想 IP アドレスに置き換えられ、リダイレクトメッセージの続行が許可されます。

一致が見つからない場合、ICMP リダイレクトメッセージが送信されるのは、新しいネクストホップ IP アドレスに対応するルータが HSRP を実行していない場合だけです。パッシブ HSRP ルータへのリダイレクトは許可されません（パッシブ HSRP ルータとは、HSRP を実行しているが、インターフェイスのアクティブ HSRP グループが存在しないルータです）。

最適に動作するためには、HSRP を実行しているネットワークの各ルータには、そのネットワークのインターフェイスのアクティブ HSRP グループが少なくとも 1 つ存在する必要があります。各 HSRP ルータが同じグループのメンバーである必要はありません。各 HSRP ルータはネットワークの HSRP パケットをすべてスヌーピングして、アクティブ ルータのリスト（仮想 IP アドレスと実際の IP アドレス）を管理します。

図 2 のネットワークに注目してください。このネットワークでは、HSRP ICMP リダイレクションフィルタがサポートされています。

図 2 HSRP ICMP リダイレクションフィルタをサポートするネットワーク



ホストは、ネット D の別のホストにパケットを送信する場合、まずパケットをデフォルトゲートウェイ（HSRP グループ 1 の仮想 IP アドレス）に送信します。

ホストから受信したパケットを次に示します。

```
dest MAC      = HSRP group 1 virtual MAC
source MAC    = Host MAC
dest IP       = host-on-netD IP
source IP     = Host IP
```

ルータ R1 は、このパケットを受信し、ルータ R4 のネット D へのパスのほうが適切であると判断したため、ルータ R4 の実際の IP アドレスにホストをリダイレクトするリダイレクトメッセージを送信する準備を行います（実際の IP アドレスのみが R1 のルーティングテーブルに含まれているため）。

ルータ R1 によって送信された最初の ICMP リダイレクトメッセージを次に示します。

```
dest MAC      = Host MAC
source MAC    = router R1 MAC
```

```

dest IP           = Host IP
source IP        = router R1 IP
gateway to use   = router R4 IP

```

このリダイレクトが発生する前、ルータ R1 の HSRP プロセスでルータ R4 がグループ 3 のアクティブ HSRP ルータであることが特定されるため、リダイレクト メッセージのネクストホップがルータ R4 の実際の IP アドレスからグループ 3 の仮想 IP アドレスに変更されます。さらに、リダイレクト メッセージを発生させた宛先 MAC アドレスから、ホストがグループ 1 の仮想 IP アドレスをゲートウェイとして使用したことが特定されるため、リダイレクト メッセージの送信元 IP アドレスがグループ 1 の仮想 IP アドレスに変更されます。

修正された ICMP リダイレクト メッセージでは、次の 2 つのフィールド (*) が修正されています。

```

dest MAC         = Host MAC
source MAC       = router R1 MAC
dest IP          = Host IP
source IP*       = HSRP group 1 virtual IP
gateway to use*  = HSRP group 3 virtual IP

```

2 回目の修正が必要な理由は、ホストが ICMP リダイレクト メッセージの送信元 IP アドレスを自身のデフォルト ゲートウェイと比較するためです。これらのアドレスが一致しない場合、ICMP リダイレクト メッセージは無視されます。この段階で、ホストのルーティング テーブルの構成は、デフォルト ゲートウェイ、グループ 1 の仮想 IP アドレス、グループ 3 の仮想 IP アドレスを通るネット D へのルートから成っています。

パッシブ HSRP ルータへの ICMP リダイレクト

パッシブ HSRP ルータへのリダイレクトは許可されません。ホストが HSRP ルータの実際の IP アドレスを検出した場合、冗長性が失われることがあります。

図 2 では、ルータ R8 はパッシブ HSRP ルータであるため、R8 へのリダイレクトは許可されません。この場合、ホストからネット D へのパケットは、まずルータ R1 に到着した後、ルータ R4 に転送されます（つまり、ネットワークを 2 回通過します）。

パッシブ HSRP ルータのあるネットワーク構成は、誤った構成と見なされます。HSRP ICMP リダイレクトが最適に動作するためには、ネットワークの HSRP を実行している各ルータに、少なくとも 1 つのアクティブ HSRP グループが存在していなければなりません。

非 HSRP ルータへの ICMP リダイレクト

ローカル インターフェイスで HSRP を実行していないルータへのリダイレクトは許可されます。非 HSRP ルータの実際の IP アドレスをホストが検出しても、冗長性が失われることはありません。

図 2 では、ルータ R7 は HSRP を実行していないので、R7 へのリダイレクトが許可されます。この場合、ネクストホップ IP アドレスは変更されません。送信元 IP アドレスは元のパケットの宛先 MAC アドレスに応じて変更されます。このリダイレクトの送信を停止するには、**no standby redirect unknown** コマンドを使用します。

パッシブ HSRP ルータのアドバタイズメント

パッシブ HSRP ルータは、HSRP アドバタイズメント メッセージの送信を定期的に行うほか、パッシブ ステートに入るときやパッシブ ステートから出るときに行います。したがって、すべての HSRP ルータが、ネットワークにある任意の HSRP ルータの HSRP グループのステートを判別できます。このアドバタイズメントは、次のように HSRP インターフェイスのステートをネットワークの他の HSRP ルータに伝えます。

- **Dormant** : インターフェイスには HSRP グループがありません。最後のグループが削除されるときに 1 つのアドバタイズメントが一度送信されます。
- **Passive** : インターフェイスには、非アクティブのグループが少なくとも 1 つありますが、アクティブなグループはありません。アドバタイズメントは定期的送信されます。
- **Active** : インターフェイスには、アクティブなグループが少なくとも 1 つあります。最初のグループがアクティブになるときに 1 つのアドバタイズメントが送信されます。

アドバタイズメントの間隔とホールドダウン時間の調整は、**standby redirect timers** コマンドを使用して行います。

送信されない ICMP リダイレクト

HSRP ルータが、リダイレクトを発生させたパケットを送信するときに、ホストが使用した IP アドレスを一意に特定できない場合、リダイレクトメッセージは送信されません。HSRP ルータは元のパケットの宛先 MAC アドレスを使用して、この IP アドレスの特定を行います。インターフェイス コンフィギュレーションコマンド **standby use-bia** の使用がインターフェイスで指定されているような特定の構成では、リダイレクトは送信できません。この場合、HSRP グループはその仮想 MAC アドレスとしてインターフェイス MAC アドレスを使用します。この時点では、HSRP ルータはホストのデフォルトゲートウェイが実際の IP アドレスであるか、インターフェイスでアクティブな HSRP 仮想 IP アドレスの 1 つであるかを特定することはできません。

Cisco 800 シリーズ、Cisco 1000 シリーズ、Cisco 1600 シリーズ、Cisco 2500 シリーズ、Cisco 3000 シリーズ、Cisco 4500 シリーズのルータでは、HSRP と ICMP リダイレクトを使用することはできません。これは、イーサネットコントローラが 1 つの MAC アドレスしかサポートしていないためです。

ICMP パケットの IP 送信元アドレスは、ICMP パケットを発生させたパケットでホストによって使用されているゲートウェイアドレスと一致している必要があります。一致していない場合、ホストは ICMP リダイレクトパケットを拒否します。HSRP ルータは送信先 MAC アドレスを使用してホストのゲートウェイ IP アドレスを特定します。その HSRP ルータが複数の IP アドレスに対して同じ MAC アドレスを使用している場合、ホストのゲートウェイ IP アドレスを一意に特定することは不可能であり、リダイレクトメッセージは送信されません。

次の出力サンプルは、ホストによって使用されているゲートウェイを HSRP ルータが一意に特定できない場合に **debug standby events icmp EXEC** コマンドを実行して得られたものです。

```
10:43:08: HSRP: ICMP redirect not sent to 20.0.0.4 for dest 30.0.0.2
10:43:08: HSRP: could not uniquely determine IP address for mac 00d0.bbd3.bc22
```

HSRP グループ シャットダウン

FHRP - HSRP グループ シャットダウン機能を使用すると、トラッキング対象のオブジェクトがダウンしたときに、HSRP グループのプライオリティを下げるのではなく、ディセーブルな状態になる（ステートが **Init** になる）ように HSRP グループを設定することができます。HSRP グループ シャットダウンを設定するには、**shutdown** キーワードとともに **standby track** コマンドを使用します。

あるオブジェクトが HSRP グループによってすでにトラッキングされている場合、HSRP グループ シャットダウン機能を使用するようにこのトラッキング設定を変更することはできません。先に、**no standby track** コマンドを使用してトラッキング設定を解除し、**shutdown** キーワードとともに **standby track** コマンドを使用してトラッキング設定を再度設定する必要があります。

次の例は、HSRP グループ シャットダウン機能が追加されるようにトラッキング対象のオブジェクトの設定を変更する方法を示しています。

```
no standby 1 track 101 decrement 10
standby 1 track 101 shutdown
```

HSRP の MPLS VPN サポート

HSRP の Multiprotocol Label Switching (MPLS; マルチプロトコル ラベル スイッチング) Virtual Private Network (VPN; バーチャル プライベート ネットワーク) インターフェイス サポートが役に立つのは、次のいずれかの状態で 2 つの Provider Edge (PE; プロバイダー エッジ) ルータ間でイーサネット LAN が接続されている場合です。

- Customer Edge (CE; カスタマー エッジ) ルータに HSRP 仮想 IP アドレスへのデフォルト ルートがある。
- 1 つまたは複数のホストで、HSRP 仮想 IP アドレスがデフォルト ゲートウェイとして設定されている。

各 VPN は 1 つまたは複数の VPN Routing and Forwarding (VRF; VPN ルーティングおよびフォワーディング) インスタンスに関連付けられています。VRF は次の要素で構成されています。

- IP ルーティング テーブル
- Cisco Express Forwarding (CEF; シスコ エクスプレス フォワーディング) テーブル
- CEF フォワーディング テーブルを使用する一連のインターフェイス
- ルーティング テーブルの情報を管理する一連のルールおよびルーティング プロトコル パラメータ

VPN ルーティング情報は、各 VRF の IP ルーティング テーブルと CEF テーブルに格納されています。各 VRF の一連のルーティング テーブルと CEF テーブルは別々に維持されます。これらのテーブルにより、VPN の外側に情報が転送されないようになっているほか、VPN の外側のバケットも VPN 内のルータに転送されないようになっています。

HSRP は、デフォルトのルーティング テーブル インスタンスを使用して ARP エントリと IP ハッシュ テーブル エントリ (エイリアス) を追加します。ただし、VRF フォワーディングがインターフェイスで設定されているときは別のルーティング テーブル インスタンスが使用されるため、HSRP 仮想 IP アドレスに対する ARP および ICMP のエコー要求は失敗します。

HSRP の MPLS VPN サポートにより、HSRP 仮想 IP アドレスがデフォルトのルーティング テーブルではなく、正しい IP ルーティング テーブルに確実に追加されます。

HSRP 複数グループ最適化

同じ物理インターフェイスに設定されるサブインターフェイスが増え続けて数百にもものぼり、各サブインターフェイスには固有の HSRP グループがある状態になっています。この複数の HSRP グループのネゴシエーションやメンテナンスは、ネットワーク トラフィックや CPU 使用率に悪影響を及ぼすことがあります。

アクティブ ルータとスタンバイ ルータを選出するために物理インターフェイスに必要なのは、1 つの HSRP グループだけです。このグループがマスター グループと呼ばれます。他の HSRP グループは、各サブインターフェイスに作成されたり、グループ名によってマスター グループとリンクされたりします。リンクされた HSRP グループは、クライアント グループまたはスレーブ グループと呼ばれます。

クライアント グループの HSRP グループ ステートは、マスター グループと同じです。また、クライアント グループはどの種類のルータ選出メカニズムにも参加しません。

クライアント グループは、スイッチやラーニング ブリッジの仮想 MAC アドレスをリフレッシュするために、定期的にメッセージを送信します。リフレッシュ メッセージが送信される頻度は、マスター グループから送信されるプロトコル選択メッセージに比べて、はるかに低いことがあります。

HSRP - ISSU

In-Service Software Upgrade (ISSU; インサービス ソフトウェア アップグレード) プロセスにより、パケット 転送を続行しながら、Cisco IOS ソフトウェアをアップデートまたは修正することができます。ほとんどのネットワークでは、予定されているソフトウェア アップグレードがダウンタイムの大きな原因になっています。ISSU を使用すると、パケット転送を続行しながら Cisco IOS ソフトウェアを修正できるので、ネットワークの可用性が向上し、予定されているソフトウェア アップグレードによるダウンタイムを短縮することができます。このマニュアルでは、ISSU の概念が説明されているほか、ISSU をシステムで実行するのに必要な手順が説明されています。

ISSU の詳細については、次の URL に掲載されている『Cisco IOS In Service Software Upgrade Process』を参照してください。

http://www.cisco.com/en/US/docs/ios/ha/configuration/guide/ha-inserv_updg.html

7600 シリーズ ルータでの ISSU の詳細については、次の URL に掲載されている『ISSU and eFSU on Cisco 7600 Series Routers』を参照してください。

<http://www.cisco.com/en/US/docs/routers/7600/ios/12.2SR/configuration/guide/efsuoovrw.html>

Cisco Catalyst 4500 シリーズのスイッチでの ISSU の詳細については、次の URL に掲載されている『Catalyst 4500 Series Switch Cisco IOS Software Configuration Guide, Release 12.2(31)SGA』の「Configuring the Cisco IOS In Service Software Upgrade Process」という章を参照してください。

<http://www.cisco.com/en/US/docs/switches/lan/catalyst4500/12.2/31sga/configuration/guide/issu.html>

SSO HSRP

SSO HSRP は、冗長な Route Processor (RP; ルート プロセッサ) を装備したルータが Stateful Switchover (SSO; ステートフル スイッチオーバー) 冗長モード用に設定されているときの HSRP の動作を変更します。ある RP がアクティブで、もう一方の RP がスタンバイになっているとき、アクティブ RP に障害が発生すると、SSO は処理を引き継ぐスタンバイ RP をイネーブルにします。

この機能を使用すると、HSRP の SSO 情報がスタンバイ RP に同期されるため、HSRP 仮想 IP アドレスを使用して送信されるトラフィックをスイッチオーバー中も引き続き転送できるほか、データの損失やパスの変更も発生しません。さらに、HSRP アクティブ ルータの両方の RP に障害が発生しても、スタンバイ状態の HSRP ルータが HSRP アクティブ ルータとして処理を引き継ぎます。

この機能は、動作の冗長モードが SSO に設定されている場合にデフォルトでイネーブルになっています。

デュアル ルート プロセッサの SSO とシスコ ノンストップ フォワーディング

SSO は、デュアル RP をサポートするネットワーキング デバイス (通常はエッジ デバイス) で機能します。1 台の RP をアクティブ プロセッサとして設定し、他の RP をスタンバイ プロセッサとして設定することで、RP 冗長化を実現します。また、RP 間の重要なステート情報を同期するため、ネットワーク ステート情報は RP 間でダイナミックに維持されます。

一般的に、SSO は Cisco NonStop Forwarding (NSF; ノンストップ フォワーディング) とともに使用されます。Cisco NSF を使用すると、ルーティング プロトコルに関する情報をスイッチオーバー後に復旧している間、データ パケットの転送を既知のルートに沿って続行できます。NSF を使用している場合、ユーザがサービスの停止に遭遇することはあまりありません。

HSRP と SSO の協調動作

SSO HSRP により、Cisco IOS HSRP サブシステム ソフトウェアはスタンバイ RP が装備されていることと、システムが SSO 冗長モードで設定されていることを検出できます。さらに、アクティブ RP に障害が発生しても、HSRP グループ自体には何の変化も発生せず、トラフィックは現在アクティブなゲートウェイ ルータを通じて引き続き転送されます。

この機能が登場する前は、アクティブ ルータのプライマリ RP に障害が発生すると、プライマリ RP は HSRP グループへの参加を停止し、HSRP アクティブ ルータとして処理を引き継ぐ、グループの別のルータをアクティブにしていました。

SSO HSRP は、RP のスイッチオーバーを通じて HSRP 仮想 IP アドレス宛てのトラフィックの転送パスを維持するために必要です。

エッジルータで SSO を設定すると、イーサネット トラフィックが HSRP スタンバイ ルータにスイッチ オーバーされなくても、イーサネット リンクのトラフィックは RP のフェールオーバー中も存続できます（プリエンブションが有効になっている場合は、その後、フェールバックされます）。



(注)

SSO が他の接続のトラフィック フローを保持しているときに HSRP トラフィックを冗長デバイスにスイッチする必要がある LAN セグメントがある場合は、**no standby sso** コマンドを使用して SSO HSRP をディセーブルにすることができます。

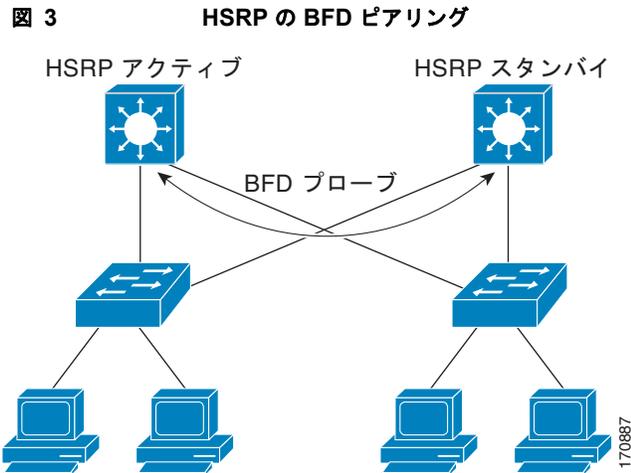
HSRP の BFD ピアリング

HSRP の BFD ピアリング機能により、HSRP グループ メンバーのヘルス モニタリング システムで BFD を使用できるようになりました。HSRP は、HSRP グループ メンバーのヘルス モニタリング システムの一部として BFD をサポートしています。BFD がないと、HSRP はマルチプロセス システムの 1 つのプロセスとして動作するため、ミリ秒の hello タイマーやホールド タイマーを使用して大量のグループに対応できるように適切なタイミングでスケジュールされることが保証されません。BFD は疑似プリエンブティブ プロセスとして動作するため、必要なときに実行されることが保証されます。複数の HSRP グループに早期フェールオーバー通知を実行できるのは、2 台のルータ間の 1 つの BFD セッションだけです。

この機能は、デフォルトでイネーブルにされています。HSRP スタンバイ ルータは、HSRP アクティブ ルータの実際の IP アドレスを HSRP hello メッセージから検出します。また、BFD クライアントとして登録し、アクティブ ルータが使用不能になった場合に通知するように要求します。

BFD は、インターフェイス、データ リンク、フォワーディング プレーンを含め、2 台の隣接ルータ間の転送パスの障害を検出する、オーバーヘッドが少なく、処理時間が短い方式です。また、BFD はインターフェイス レベルやルーティング プロトコル レベルでイネーブルにする検出プロトコルです。Cisco は、ルータ間の BFD ネイバーセッションをアクティブ化および維持するために 2 つのシステム間で BFD 制御パケットを送信する BFD 非同期モードをサポートしています。このため、BFD セッションを作成するためには、両方のシステム（または BFD ピア）で BFD を設定する必要があります。BFD がインターフェイスでイネーブルになっているとともに、HSRP 用にルータ レベルでイネーブルになっている場合、BFD セッションが作成されて、BFD タイマーがネゴシエートされ、ネゴシエートされた間隔で BFD ピアが互いに BFD 制御パケットの送信を開始します。

BFD による BFD ピアの障害検出が高速なのは、使用されているメディア タイプ、カプセル化、トポロジ、ルーティング プロトコル (BGP、EIGRP、HSRP、IS-IS、OSPF) が何であっても同じです。障害検出通知をローカル ルータのルーティング プロトコルにすばやく送信してルーティング テーブルの再計算プロセスを開始することによって、BFD はネットワーク全体のコンバージェンス時間を大幅に削減するのに役立っています。図 3 は、HSRP と BFD を実行している 2 台のルータのある単純なネットワークを示しています。



BFD の詳細については、次の URL にアクセスして『Cisco IOS IP Routing Configuration Guide』の「Bidirectional Forwarding Detection」を参照してください。

http://www.cisco.com/en/US/docs/ios/iproute/configuration/guide/irp_bfd.html

HSRP MIB トラップ

HSRP Management Information Base (MIB; 管理情報ベース) は、Simple Network Management Protocol (SNMP; 簡易ネットワーク管理プロトコル) の GET 操作をサポートしているため、ネットワーク デバイスはネットワークの HSRP グループに関するレポートをネットワーク管理ステーションから取得することができます。

HSRP MIB トラップのサポートのイネーブル化は CLI で行います。また MIB はレポートの取得に使用されます。各トラップは、ルータがアクティブ ステートやスタンバイ ステートになったり、それらのステートから移行したりしたときにネットワーク管理ステーションに通知します。CLI からエントリを設定すると、直ちに、MIB でのそのグループの RowStatus がアクティブ ステートになります。

Cisco IOS ソフトウェアがサポートしているのは読み取り専用の MIB で、SET 操作はサポートしていません。

この機能は次の 4 つの MIB テーブルをサポートしています。

- CISCO-HSRP-MIB.my で定義されている cHsrpGrpEntry テーブル
- CISCO-HSRP-EXT-MIB.my で定義されている cHsrpExtIfTrackedEntry、cHsrpExtSecAddrEntry、cHsrpExtIfEntry

cHsrpGrpEntry テーブルは、各 HSRP グループの情報から構成されており、その他のテーブルは CISCO-HSRP-EXT-MIB.my で定義されている HSRP の Cisco 拡張で構成されています。

HSRP の設定方法

- 「HSRP のイネーブル化」 (P.20) (必須)
- 「インターフェイスでの HSRP の初期化の遅延」 (P.22) (任意)
- 「HSRP のプライオリティとプリエンプションの設定」 (P.24) (必須)
- 「HSRP のオブジェクト トラッキングの設定」 (P.26) (任意)
- 「キー スtringを使用した HSRP MD5 認証の設定」 (P.28) (任意)
- 「キー チェーンを使用した HSRP MD5 認証の設定」 (P.30) (任意)
- 「HSRP MD5 認証のトラブルシューティング」 (P.32) (任意)
- 「HSRP テキスト認証の設定」 (P.33) (任意)
- 「HSRP タイマーの設定」 (P.35) (任意)
- 「HSRP MAC リフレッシュ インターバルの設定」 (P.36) (任意)
- 「ロード バランシング用の複数の HSRP グループの設定」 (P.37) (任意)
- 「HSRP 複数グループ最適化による CPU およびネットワークのパフォーマンスの向上」 (P.39) (任意)
- 「HSRP の ICMP リダイレクト サポートのイネーブル化」 (P.41) (任意)
- 「HSRP 仮想 MAC アドレスまたは BIA MAC アドレスの設定」 (P.42) (任意)
- 「HSRP グループへの IP 冗長性クライアントのリンク」 (P.43) (任意)
- 「HSRP バージョン 2 への変更」 (P.45) (任意)
- 「SSO 対応 HSRP のイネーブル化」 (P.47) (任意)
- 「SSO 対応 HSRP の検証」 (P.48) (任意)
- 「HSRP MIB トラップのイネーブル化」 (P.49) (任意)
- 「HSRP BFD ピアリングの設定」 (P.51) (任意)
- 「HSRP gratuitous ARP の設定」 (P.54) (任意)

HSRP のイネーブル化

ここでは、HSRP をイネーブルにする作業を行います。

インターフェイス コンフィギュレーション コマンド **standby ip** は、設定されているインターフェイスで HSRP をアクティブ化します。指定されている IP アドレスがある場合は、そのアドレスがホット スタンバイ グループの仮想 IP アドレスとして使用されます。指定したルータが HSRP によって選出されるようにするには、グループの少なくとも 1 台のルータに仮想 IP アドレスを設定する必要があります。このアドレスはグループの他のルータによって検出されます。

前提条件

認証、タイマー、プライオリティ、プリエンプションなど、HSRP で多くのアトリビュートを設定できません。先にアトリビュートを設定してから、HSRP グループをイネーブルにするのが最も効率的な方法です。

この方法では、他のルータでの認証エラー メッセージや予期しないステートの変化が発生しません。これらの現象は、グループを先にイネーブルにし、他の設定を入力するまでに十分に長い遅延 (1 つまたは 2 つのホールド タイム) があつた場合に発生することがあります。

常に HSRP IP アドレスを指定することを推奨します。

手順の概要

1. `enable`
2. `configure terminal`
3. `interface type number`
4. `ip address ip-address mask`
5. `standby [group-number] ip [ip-address [secondary]]`
6. `end`
7. `show standby [all] [brief]`
8. `show standby type number [group-number | all] [brief]`

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<code>enable</code> 例： Router> enable	特権 EXEC モードをイネーブルにします。 <ul style="list-style-type: none">• プロンプトが表示されたら、パスワードを入力します。
ステップ 2	<code>configure terminal</code> 例： Router# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	<code>interface type number</code> 例： Router(config)# interface ethernet 0	インターフェイス タイプを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	<code>ip address ip-address mask</code> 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	<code>standby [group-number] ip [ip-address [secondary]]</code> 例： Router(config-if)# standby 1 ip 172.16.6.100	HSRP をアクティブにします。 <ul style="list-style-type: none">• グループ番号は、指定しなければデフォルト値の 0 に設定されます。グループ番号の範囲は、HSRP バージョン 1 の場合は 0 ~ 255 で、HSRP バージョン 2 の場合は 0 ~ 4095 です。• <code>ip-address</code> は仮想ルータの仮想 IP アドレスです。指定したルータが HSRP によって選出されるようにするには、グループの少なくとも 1 台のルータに仮想 IP アドレスを設定する必要があります。このアドレスはグループの他のルータによって検出されます。
ステップ 6	<code>end</code> 例： Router(config-if)# end	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 7	<code>show standby [all] [brief]</code> 例： Router# show standby	(任意) HSRP に関する情報を表示します。 • このコマンドを実行すると、各グループの情報が表示されます。 all オプションを付けると、検出されたグループおよび standby ip コマンドが設定されていないグループが表示されます。
ステップ 8	<code>show standby type number [group-number all] [brief]</code> 例： Router# show standby ethernet 0	(任意) 特定のグループまたはインターフェイスの HSRP 関連の情報が表示されます。

インターフェイスでの HSRP の初期化の遅延

`standby delay` コマンドを使用して、インターフェイスのリロード後や起動後の HSRP の初期化を遅延します。この設定を行うと、インターフェイス起動イベントの後にインターフェイスやルータの状態が安定する時間を確保して、HSRP のステートが不安定になるのを防ぐことができます。

手順の概要

1. `enable`
2. `configure terminal`
3. `interface type number`
4. `ip address ip-address mask`
5. `standby delay minimum min-seconds reload reload-seconds`
6. `standby [group-number] ip [ip-address [secondary]]`
7. `end`
8. `show standby delay [type number]`

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<code>enable</code> 例： Router> enable	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	<code>configure terminal</code> 例： Router# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	<code>interface type number</code> 例： Router(config)# interface Ethernet0/1	インターフェイス タイプを設定し、インターフェイス コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	<pre>ip address ip-address mask</pre> <p>例： Router(config-if)# ip address 10.0.0.1 255.255.255.0</p>	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	<pre>standby delay minimum min-seconds reload reload-seconds</pre> <p>例： Router(config-if)# standby delay minimum 30 reload 60</p>	<p>(任意) HSRP グループの初期化までの遅延時間を設定します。</p> <ul style="list-style-type: none"> <i>min-seconds</i> 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。 <i>reload-seconds</i> の値は、ルータのリロード後に遅延する時間です。この遅延時間は、ルータがリロードした後の最初のインターフェイス起動イベントにのみ適用されます。 <p>(注) <i>min-seconds</i> および <i>reload-seconds</i> の値は、それぞれ 30 と 60 に設定することを推奨します。</p>
ステップ 6	<pre>standby [group-number] ip [ip-address [secondary]]</pre> <p>例： Router(config-if)# standby 1 ip 10.0.0.3 255.255.255.0</p>	HSRP をアクティブにします。
ステップ 7	<pre>end</pre> <p>例： Router(config-if)# end</p>	特権 EXEC モードに戻ります。
ステップ 8	<pre>show standby delay [type number]</pre> <p>例： Router# show standby delay</p>	(任意) HSRP の遅延時間に関する情報を表示します。

トラブルシューティングのヒント

standby timers コマンドをミリ秒単位で設定する場合や、スイッチの VLAN インターフェイスで HSRP を設定する場合は、**standby delay minimum reload** コマンドを使用することを推奨します。

HSRP のプライオリティとプリエンプションの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip address** *ip-address mask*
5. **standby** [*group-number*] **priority** *priority*
6. **standby** [*group-number*] **preempt** [**delay** {**minimum** *delay* | **reload** *delay* | **sync** *delay*}]
7. **standby** [*group-number*] **ip** [*ip-address* [**secondary**]]
8. **end**
9. **show standby** [**all**] [**brief**]
10. **show standby type number** [*group-number* | **all**] [**brief**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	enable 例： Router> enable	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	configure terminal 例： Router# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	interface <i>type number</i> 例： Router(config)# interface Ethernet0/1	インターフェイス タイプを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	ip address <i>ip-address mask</i> 例： Router(config-if)# ip address 10.0.0.1 255.255.255.0	インターフェイスの IP アドレスを指定します。
ステップ 5	standby [<i>group-number</i>] priority <i>priority</i> 例： Router(config-if)# standby 1 priority 110	HSRP のプライオリティを設定します。 • デフォルトのプライオリティは 100 です。

	コマンドまたはアクション	目的
ステップ 6	<pre>standby [group-number] preempt [delay {minimum delay reload delay sync delay}]</pre> <p>例： Router(config-if)# standby 1 preempt delay minimum 380</p>	<p>HSRP のプリエンプションとプリエンプション遅延を設定します。</p> <ul style="list-style-type: none"> デフォルトの遅延時間は 0 秒です。つまり、ルータは最優位になれる場合、すぐに最優位になります。デフォルトでは、後で起動したルータはスタンバイ ルータになります。
ステップ 7	<pre>standby [group-number] ip [ip-address [secondary]]</pre> <p>例： Router(config-if)# standby 1 ip 10.0.0.3 255.255.255.0</p>	<p>HSRP をアクティブにします。</p>
ステップ 8	<pre>end</pre> <p>例： Router(config-if)# end</p>	<p>特権 EXEC モードに戻ります。</p>
ステップ 9	<pre>show standby [all] [brief]</pre> <p>例： Router# show standby</p>	<p>(任意) HSRP に関する情報を表示します。</p> <ul style="list-style-type: none"> このコマンドを実行すると、各グループの情報が表示されます。all オプションを付けると、検出されたグループおよび standby ip コマンドが設定されていないグループが表示されます。
ステップ 10	<pre>show standby type number [group-number all] [brief]</pre> <p>例： Router# show standby ethernet 0/1</p>	<p>(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。</p>

HSRP のオブジェクト トラッキングの設定

ここでは、オブジェクトをトラッキングし、そのステートに基づいて HSRP のプライオリティを変更するように HSRP を設定する作業を行います。

トラッキング対象の各オブジェクトは、トラッキング CLI で指定した一意の番号で識別されます。クライアント プロセスは、この番号を使用して特定のオブジェクトを追跡します。

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

手順の概要

1. **enable**
2. **configure terminal**
3. **track object-number interface type number {line-protocol | ip routing}**
4. **exit**
5. **interface type number**
6. **standby [group-number] track object-number [decrement priority-decrement]**
7. **standby [group-number] track object-number shutdown**
8. **standby [group-number] ip [ip-address [secondary]]**
9. **end**
10. **show track [object-number | brief] [interface [brief] | ip route [brief] | resolution | timers]**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	enable 例： Router> enable	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	configure terminal 例： Router# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	track object-number interface type number {line-protocol ip routing} 例： Router(config)# track 100 interface serial2/0 line-protocol	インターフェイスをトラッキングされるように設定し、トラッキング コンフィギュレーション モードを開始します。
ステップ 4	exit 例： Router(config-track)# exit	グローバル コンフィギュレーション モードに戻ります。

	コマンドまたはアクション	目的
ステップ 5	<pre>interface type number</pre> <p>例： Router(config)# interface ethernet 2</p>	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	<pre>standby [group-number] track object-number [decrement priority-decrement]</pre> <p>例： Router(config-if)# standby 1 track 100 decrement 20</p>	<p>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。</p> <ul style="list-style-type: none"> デフォルトでは、トラッキング対象のオブジェクトがダウンすると、ルータのプライオリティは 10 だけ引き下げられます。デフォルトの動作を変更するには、キーワードと引数の組み合わせの decrement priority-decrement を使用します。 トラッキング対象の複数のオブジェクトがダウンした場合、priority-decrement の値が設定されていれば、設定されているプライオリティの減分値が累積されます。トラッキング対象のオブジェクトがダウンした場合、どのオブジェクトにもプライオリティの減分値が設定されていなければ、デフォルトの減分値は 10 で、累積されます。
ステップ 7	<pre>standby [group-number] track object-number shutdown</pre> <p>例： Router(config-if)# standby 1 track 100 shutdown</p>	<p>(任意) オブジェクトをトラッキングし、トラッキング対象のオブジェクトがダウンしたときに HSRP グループをディセーブルにするように HSRP を設定します。</p> <ul style="list-style-type: none"> トラッキング対象のオブジェクトがダウンしたときにルータの HSRP グループをディセーブルにするには、shutdown キーワードを使用します。
ステップ 8	<pre>standby [group-number] ip [ip-address [secondary]]</pre> <p>例： Router(config-if)# standby 1 ip 10.10.10.0</p>	<p>HSRP をアクティブにします。</p> <ul style="list-style-type: none"> デフォルトのグループ番号は 0 です。グループ番号の範囲は、HSRP バージョン 1 の場合は 0 ~ 255 で、HSRP バージョン 2 の場合は 0 ~ 4095 です。
ステップ 9	<pre>end</pre> <p>例： Router(config-if)# end</p>	特権 EXEC モードに戻ります。
ステップ 10	<pre>show track [object-number brief] [interface [brief] ip route [brief] resolution timers]</pre> <p>例： Router# show track 100 interface</p>	トラッキング情報を表示します。

キー ストリングを使用した HSRP MD5 認証の設定

制約事項

HSRP グループにテキスト認証と MD5 認証を併用することはできません。MD5 認証が設定されている場合、受信側のルータの MD5 認証がイネーブルになっていれば、HSRP Hello メッセージのテキスト認証フィールドは転送時にすべてゼロに設定され、受信時に無視されます。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip address** *ip-address mask* [**secondary**]
5. **standby** [*group-number*] **priority** *priority*
6. **standby** [*group-number*] **preempt** [**delay** {*minimum delay* | *reload delay* | *sync delay*}]
7. **standby** [*group-number*] **authentication md5** **key-string** [**0** | **7**] *key* [*timeout seconds*]
8. **standby** [*group-number*] **ip** [*ip-address* [**secondary**]]
9. 通信するルータごとにステップ 1 ～ 8 を繰り返します。
10. **end**
11. **show standby**

手順の詳細

	コマンド	目的
ステップ 1	enable 例： Router> enable	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	configure terminal 例： Router# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	interface <i>type number</i> 例： Router(config)# interface Ethernet0/1	インターフェイス タイプを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	ip address <i>ip-address mask</i> [secondary] 例： Router(config-if)# ip address 10.0.0.1 255.255.255.0	インターフェイスのプライマリ IP アドレスまたはセカンダリ IP アドレスを指定します。

	コマンド	目的
ステップ 5	<pre>standby [group-number] priority priority</pre> <p>例： Router(config-if)# standby 1 priority 110</p>	HSRP のプライオリティを設定します。
ステップ 6	<pre>standby [group-number] preempt [delay {minimum delay reload delay sync delay}]</pre> <p>例： Router(config-if)# standby 1 preempt</p>	HSRP のプリエンブションを設定します。
ステップ 7	<pre>standby [group-number] aut hentication md5 key-string [0 7] key [timeout seconds]</pre> <p>例： Router(config-if)# standby 1 authentication md5 key-string d00b4r987654321a timeout 30</p>	<p>HSRP MD5 認証の認証文字列を設定します。</p> <ul style="list-style-type: none"> • <i>key</i> 引数には最大 64 文字を設定できます。16 文字以上を使用することを推奨します。 • <i>key</i> 引数にはプレフィクスを指定しません。0 を指定すると、キーは暗号化されないことを示します。 • 7 を指定するとキーは暗号化されます。service password-encryption グローバル コンフィギュレーション コマンドがイネーブルになっていると、key-string 認証キーは自動的に暗号化されます。 • タイムアウト値は、古いキー ストリングが受け入れられ、新しいキーを使用してグループ内のすべてのルータを設定できる時間です。
ステップ 8	<pre>standby [group-number] ip [ip-address [secondary]]</pre> <p>例： Router(config-if)# standby 1 ip 10.0.0.3</p>	HSRP をアクティブにします。
ステップ 9	通信するルータごとにステップ 1～8 を繰り返します。	—
ステップ 10	<pre>end</pre> <p>例： Router(config-if)# end</p>	特権 EXEC モードに戻ります。
ステップ 11	<pre>show standby</pre> <p>例： Router# show standby</p>	<p>(任意) HSRP に関する情報を表示します。</p> <ul style="list-style-type: none"> • このコマンドを使用して、設定を確認します。キー ストリングまたはキー チェーンが表示されます (設定されている場合)。

トラブルシューティングのヒント

あるグループのルータのキー ストリングを変更する場合、アクティブ ルータを最後に変更して、HSRP ステートが変化しないようにします。アクティブ ルータのキー ストリングの変更は、アクティブでないルータの後、インターフェイス コンフィギュレーション コマンド **standby timers** によって指定されているホールド時間 1 回分の時間が経過する前に行われなければなりません。この手順により、アクティブでないルータでアクティブ ルータのタイムアウトが発生することがなくなります。

キーチェーンを使用した HSRP MD5 認証の設定

キーチェーンを使用すると、キーチェーンの設定に基づき、場合に応じて異なるキー・ストリングを使用できます。HSRP は適切なキーチェーンを照会し、特定のキーチェーンに対して現在アクティブになっているキーとキー ID を取得します。

手順の概要

1. **enable**
2. **configure terminal**
3. **key chain name-of-chain**
4. **key key-id**
5. **key-string string**
6. **exit**
7. **interface type number**
8. **ip address ip-address mask [secondary]**
9. **standby [group-number] priority priority**
10. **standby [group-number] preempt [delay {minimum delay | reload delay | sync delay}]**
11. **standby [group-number] authentication md5 key-chain key-chain-name**
12. **standby [group-number] ip [ip-address [secondary]]**
13. 通信するルータごとにステップ 1 ～ 12 を繰り返します。
14. **end**
15. **show standby**

手順の詳細

	コマンド	目的
ステップ 1	enable 例： Router> enable	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	configure terminal 例： Router# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	key chain name-of-chain 例： Router(config)# key chain hsrpl	ルーティング プロトコルの認証をイネーブルにし、認証キーのグループを識別します。
ステップ 4	key key-id 例： Router(config-keychain)# key 100	キーチェーンの認証キーを識別します。 • <i>key-id</i> は、数値で指定する必要があります。

	コマンド	目的
ステップ 5	key-string <i>string</i> 例： Router(config-keychain-key) # key-string mnol172	キーの認証文字列を指定します。 <ul style="list-style-type: none"> <i>string</i> には、1 ~ 80 文字の大文字と小文字の英数字を指定できます。ただし、最初の文字を数値にすることはできません。
ステップ 6	exit 例： Router(config-keychain-key) # exit	グローバル コンフィギュレーション モードに戻ります。
ステップ 7	interface <i>type number</i> 例： Router(config)# interface Ethernet0/1	インターフェイス タイプを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 8	ip address <i>ip-address mask</i> [secondary] 例： Router(config-if)# ip address 10.21.8.32 255.255.255.0	インターフェイスのプライマリ IP アドレスまたはセカンダリ IP アドレスを指定します。
ステップ 9	standby [<i>group-number</i>] priority <i>priority</i> 例： Router(config-if)# standby 1 priority 110	HSRP のプライオリティを設定します。
ステップ 10	standby [<i>group-number</i>] preempt [delay { minimum <i>delay</i> reload <i>delay</i> sync <i>delay</i> }] 例： Router(config-if)# standby 1 preempt	HSRP のプリエンプションを設定します。
ステップ 11	standby [<i>group-number</i>] aut hentication md5 key-chain <i>key-chain-name</i> 例： Router(config-if)# standby 1 authentication md5 key-chain hsrp1	HSRP MD5 認証の認証 MD5 キー チェーンを設定します。 <ul style="list-style-type: none"> キー チェーン名は、ステップ 3 で指定した名前と一致する必要があります。
ステップ 12	standby [<i>group-number</i>] ip [ip-address [secondary]] 例： Router(config-if)# standby 1 ip 10.21.8.12	HSRP をアクティブにします。

	コマンド	目的
ステップ 13	通信するルータごとにステップ 1 ~ 12 を繰り返します。	—
ステップ 14	<code>end</code> 例： Router(config-if)# end	特権 EXEC モードに戻ります。
ステップ 15	<code>show standby</code> 例： Router# show standby	(任意) HSRP に関する情報を表示します。 • このコマンドを使用して、設定を確認します。キー スtring または キー チェーンが表示されます (設定されている場合)。

HSRP MD5 認証のトラブルシューティング

ここでは、HSRP MD5 認証が正しく機能しない場合に行う作業を説明します。

手順の概要

1. `enable`
2. `debug standby errors`

手順の詳細

	コマンド	目的
ステップ 1	<code>enable</code> 例： Router> enable	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	<code>debug standby errors</code> 例： Router# debug standby errors	HSRP 関連のエラー メッセージを表示します。 • エラー メッセージは、認証に失敗したパケットごとに表示されるため、このコマンドを使用するときは注意してください。 • 2 台のルータで認証が実行されないときに表示されるエラー メッセージの例については、「例」を参照してください。

例

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

```
Router# debug standby errors
```

```
A:Jun 16 12:14:50.337:HSRP:Et0/1 Grp 0 Auth failed for Hello pkt from 10.21.0.5, MD5
confgd but no tlv
B:Jun 16 12:16:34.287:HSRP:Et0/1 Grp 0 Auth failed for Hello pkt from 10.21.0.4, Text auth failed
```

次の例では、ルータ A とルータ B の両方に別々の MD5 認証文字列が設定されています。

```
Router# debug standby errors
```

```
A:Jun 16 12:19:26.335:HSRP:Et0/1 Grp 0 Auth failed for Hello pkt from 10.21.0.5, MD5 auth failed
B:Jun 16 12:18:46.280:HSRP:Et0/1 Grp 0 Auth failed for Hello pkt from 10.21.0.4, MD5 auth failed
```

HSRP テキスト認証の設定

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip address** *ip-address mask* [**secondary**]
5. **standby** [*group-number*] **priority** *priority*
6. **standby** [*group-number*] **preempt** [**delay** {*minimum delay* | **reload** *delay* | **sync** *delay*}]
7. **standby** [*group-number*] **authentication text** *string*
8. **standby** [*group-number*] **ip** [*ip-address* [**secondary**]]
9. 通信するルータごとにステップ 1 ~ 8 を繰り返します。
10. **end**
11. **show standby**

手順の詳細

	コマンド	目的
ステップ 1	enable 例： Router> enable	特権 EXEC モードなど、高位の権限レベルをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	configure terminal 例： Router# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	interface <i>type number</i> 例： Router(config)# interface Ethernet0/1	インターフェイス タイプを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	ip address <i>ip-address mask</i> [secondary] 例： Router(config-if)# ip address 10.0.0.1 255.255.255.0	インターフェイスのプライマリ IP アドレスまたはセカンダリ IP アドレスを指定します。
ステップ 5	standby [<i>group-number</i>] priority <i>priority</i> 例： Router(config-if)# standby 1 priority 110	HSRP のプライオリティを設定します。

	コマンド	目的
ステップ 6	<pre>standby [group-number] preempt [delay {minimum delay reload delay sync delay}]</pre> <p>例： Router(config-if)# standby 1 preempt</p>	HSRP のプリエンプションを設定します。
ステップ 7	<pre>standby [group-number] aut hentication text string</pre> <p>例： Router(config-if)# standby 1 authentication text authentication1</p>	HSRP テキスト認証の認証文字列を設定します。 <ul style="list-style-type: none"> デフォルトの文字列は「cisco」です。
ステップ 8	<pre>standby [group-number] ip [ip-address [secondary]]</pre> <p>例： Router(config-if)# standby 1 ip 10.0.0.3</p>	HSRP をアクティブにします。
ステップ 9	通信するルータごとにステップ 1 ~ 8 を繰り返します。	—
ステップ 10	<pre>end</pre> <p>例： Router(config-if)# end</p>	特権 EXEC モードに戻ります。
ステップ 11	<pre>show standby</pre> <p>例： Router# show standby</p>	(任意) HSRP に関する情報を表示します。 <ul style="list-style-type: none"> このコマンドを使用して、設定を確認します。キー ストリングまたはキー チェーンが表示されます (設定されている場合)。

HSRP タイマーの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **interface type number**
4. **ip address ip-address mask [secondary]**
5. **standby [group-number] timers [msec] hellotime [msec] holdtime**
6. **standby [group-number] ip [ip-address [secondary]]**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	enable 例： Router> enable	特権 EXEC モードをイネーブルにします。 <ul style="list-style-type: none"> • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	configure terminal 例： Router# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	interface type number 例： Router(config)# interface Ethernet0/1	インターフェイス タイプを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	ip address ip-address mask [secondary] 例： Router(config-if)# ip address 10.0.0.1 255.255.255.0	インターフェイスのプライマリ IP アドレスまたはセカンダリ IP アドレスを指定します。
ステップ 5	standby mac-refresh seconds 例： Router(config-if)# standby mac-refresh 100	HSRP が FDDI で動作している場合に、MAC キャッシュをリフレッシュするためにパケットが送信される間隔を変更します。 <ul style="list-style-type: none"> • このコマンドは、FDDI で動作している HSRP にのみ適用されます。
ステップ 6	standby [group-number] ip [ip-address [secondary]] 例： Router(config-if)# standby 1 ip 10.0.0.3	HSRP をアクティブにします。

トラブルシューティングのヒント

hellotime と holdtime の最小値は、それぞれ 250 ミリ秒、800 ミリ秒に設定することを推奨します。

standby delay コマンドを使用すると、HSRP が初期化される前に、インターフェイスを完全に起動することが可能です。

HSRP MAC リフレッシュ インターバルの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **interface type number**
4. **ip address ip-address mask [secondary]**
5. **standby mac-refresh seconds**
6. **standby [group-number] ip [ip-address [secondary]]**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	enable 例： Router> enable	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	configure terminal 例： Router# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	interface type number 例： Router(config)# interface Ethernet0/1	インターフェイス タイプを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	ip address ip-address mask [secondary] 例： Router(config-if)# ip address 10.0.0.1 255.255.255.0	インターフェイスのプライマリ IP アドレスまたはセカンダリ IP アドレスを指定します。
ステップ 5	standby mac-refresh seconds 例： Router(config-if)# standby mac-refresh 100	HSRP が FDDI で動作している場合に、MAC キャッシュをリフレッシュするためにパケットが送信される間隔を変更します。 • このコマンドは、FDDI で動作している HSRP にのみ適用されます。
ステップ 6	standby [group-number] ip [ip-address [secondary]] 例： Router(config-if)# standby 1 ip 10.0.0.3	HSRP をアクティブにします。

ロード バランシング用の複数の HSRP グループの設定

ここでは、ロード バランシングのために複数の HSRP グループを設定する作業を行います。

HSRP グループを複数にすると、ネットワークで冗長性を確保し、ロード シェアリングを実現できるほか、冗長ルータを余すところなく活用できるようになります。各ルータは、1つの HSRP グループにトラフィックをアクティブに転送する一方、別のグループに対してスタンバイ ステートやリスン ステートになることができます。

2 台のルータを使用している場合、ルータ A はグループ 1 に対してアクティブと設定され、グループ 2 に対してスタンバイと設定されます。また、ルータ B はグループ 1 に対してスタンバイになり、グループ 2 に対してアクティブになります。LAN 上のホストの半数はグループ 1 の仮想 IP アドレスを使用して設定され、残りの半数はグループ 2 の仮想 IP アドレスを使用して設定されます。図および設定例については、「例：ロード バランシング用の複数の HSRP」(P.59) を参照してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface type number**
4. **ip address ip-address mask [secondary]**
5. **standby [group-number] priority priority**
6. **standby [group-number] preempt [delay {minimum delay | reload delay | sync delay}]**
7. **standby [group-number] ip [ip-address [secondary]]**
8. 同じルータでステップ 5 ~ 7 を繰り返して、別のスタンバイ グループのルータ アトリビュートを設定します。
9. **exit**
10. もう 1 つのルータで、ステップ 3 ~ 9 を繰り返して HSRP を設定します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	enable 例： Router> enable	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	configure terminal 例： Router# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	interface type number 例： Router(config)# interface Ethernet0/1	インターフェイス タイプを設定し、インターフェイス コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	<pre>ip address ip-address mask [secondary] 例： Router(config-if)# ip address 10.0.0.1 255.255.255.0</pre>	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	<pre>standby [group-number] priority priority 例： Router(config-if)# standby 1 priority 110</pre>	HSRP のプライオリティを設定します。
ステップ 6	<pre>standby [group-number] preempt [delay {minimum delay reload delay sync delay}] 例： Router(config-if)# standby 1 preempt</pre>	HSRP のプリエンプションを設定します。
ステップ 7	<pre>standby [group-number] ip [ip-address [secondary]] 例： Router(config-if)# standby 1 ip 10.0.0.3</pre>	HSRP をアクティブにします。
ステップ 8	同じルータでステップ 5～7 を繰り返して、別のスタンバイグループのルータアトリビュートを設定します。	たとえば、ルータ A をグループ 1 のアクティブルータとして設定するとともに、別のプライオリティおよびプリエンプションの値を使用して別の HSRP グループのアクティブルータまたはスタンバイルータとして設定することができます。
ステップ 9	<pre>exit 例： Router(config-if)# exit</pre>	グローバル コンフィギュレーション モードに戻ります。
ステップ 10	もう 1 つのルータでステップ 3～9 を繰り返します。	もう 1 つのルータで複数の HSRP を設定し、ロード バランシングをイネーブルにします。

HSRP 複数グループ最適化による CPU およびネットワークのパフォーマンスの向上

前の項の「[ロード バランシング用の複数の HSRP グループの設定](#)」の手順を行って HSRP マスターグループを設定してください。

ここでは、複数の HSRP クライアントグループを設定する作業を行います。

standby follow コマンドでは、別の HSRP グループのスレーブになるように HSRP グループを設定します。

HSRP クライアントグループがマスター HSRP に追従するときは短時間のランダムな遅延が発生するので、すべてのクライアントグループが同時に変化することはありません。

アクティブなクライアントグループは FDDI の MAC リフレッシュ メカニズムを使用して、マスターグループよりも長い間隔で hello パケットを送信します。デフォルトの間隔は 10 秒ですが、最大で 255 秒に設定することができます。

制約事項

- クライアントグループまたはスレーブグループは、マスターグループと同じ物理インターフェイス上に存在していなければなりません。
- クライアントグループは、追従しているグループからステータスを取得します。このため、クライアントグループは自身のタイマー設定、プライオリティ設定、プリエンプション設定を使用しません。これらの設定がクライアントグループに設定されている場合は、警告が表示されます。

```
Router(config-if)# standby 1 priority 110  
%Warning: This setting has no effect while following another group.
```

```
Router(config-if)# standby 1 timers 5 15  
% Warning: This setting has no effect while following another group.
```

```
Router(config-if)# standby 1 preempt delay minimum 300  
% Warning: This setting has no effect while following another group.
```

手順の概要

1. **enable**
2. **configure terminal**
3. **interface type number**
4. **ip address ip-address mask [secondary]**
5. **standby group-number follow group-name**
6. **exit**
7. ステップ 3 ~ 6 を繰り返して、さらに HSRP クライアントグループを設定します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	enable 例： Router> enable	特権 EXEC モードをイネーブにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	configure terminal 例： Router# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	interface type number 例： Router(config)# interface Ethernet0/1	インターフェイス タイプを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	ip address ip-address mask [secondary] 例： Router(config-if)# ip address 10.0.0.1 255.255.255.0	インターフェイスのプライマリ IP アドレスまたはセカンダリ IP アドレスを指定します。
ステップ 5	standby group-number follow group-name 例： Router(config-if)# standby 1 follow HSRP1	HSRP グループをクライアント グループとして設定します。
ステップ 6	exit 例： Router(config-if)# exit	グローバル コンフィギュレーション モードに戻ります。
ステップ 7	ステップ 3～6 を繰り返して、さらに HSRP クライアント グループを設定します。	複数の HSRP クライアント グループを設定します。

HSRP の ICMP リダイレクト サポートのイネーブル化

デフォルトでは、ICMP リダイレクト メッセージの HSRP フィルタリングは、HSRP が実行されているルータでイネーブルになっています。ここでは、この機能がディセーブルになっている場合に、ルータでこの機能を再度イネーブルにする作業を行います。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface type number**
4. **standby redirect [timers advertisement holddown] [unknown]**
5. **end**
6. **show standby redirect [ip-address] [interface-type interface-number] [active] [passive] [timers]**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	enable 例： Router> enable	特権 EXEC モードをイネーブルにします。 <ul style="list-style-type: none">• プロンプトが表示されたら、パスワードを入力します。
ステップ 2	configure terminal 例： Router# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	interface type number 例： Router(config)# interface Ethernet0/1	インターフェイス タイプを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	standby redirect [timers advertisement holddown] [unknown] 例： Router(config-if)# standby redirect	ICMP リダイレクト メッセージの HSRP フィルタリングをイネーブルにします。 <ul style="list-style-type: none">• このコマンドは、グローバル コンフィギュレーション モードで使用することもできます。この場合、ICMP リダイレクト メッセージの HSRP フィルタリングが、HSRP 用に設定されているすべてのインターフェイスでイネーブルになります。
ステップ 5	end 例： Router(config-if)# end	特権 EXEC モードに戻ります。
ステップ 6	show standby redirect [ip-address] [interface-type interface-number] [active] [passive] [timers] 例： Router# show standby redirect	(任意) HSRP を使用して設定されているインターフェイスの ICMP リダイレクト関連の情報を表示します。

HSRP 仮想 MAC アドレスまたは BIA MAC アドレスの設定

制約事項

standby use-bia コマンドと **standby mac-address** コマンドを同じ設定で使用することはできません。これらのコマンドは相互に排他的な関係にあります。

standby use-bia コマンドには次の欠点があります。

- あるルータがアクティブになると、その仮想 IP アドレスが別の MAC アドレスに移行されます。この新しいアクティブ ルータは、**gratuitous ARP** 応答を送信しますが、すべてのホスト実装で **gratuitous ARP** が正しく処理されるとは限りません。
- standby use-bia** コマンドを設定すると、プロキシ ARP を使用できなくなります。ルータで障害が発生してプロキシ ARP データベースが失われても、スタンバイ ルータはそれに対応できなくなります。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface type number**
4. **ip address ip-address mask [secondary]**
5. **standby [group-number] mac-address mac-address**
または
standby use-bia [scope interface]
6. **standby [group-number] ip [ip-address [secondary]]**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	enable 例： Router> enable	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	configure terminal 例： Router# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	interface type number 例： Router(config)# interface Ethernet0/1	インターフェイス タイプを設定し、インターフェイス コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	<pre>ip address ip-address mask [secondary]</pre> <p>例： Router(config-if)# ip address 172.16.6.5 255.255.255.0</p>	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	<pre>standby [group-number] mac-address mac-address または standby use-bia [scope interface]</pre> <p>例： Router(config-if)# standby 1 mac-address 5000.1000.1060 または</p> <p>例： Router(config-if)# standby use-bia</p>	<p>HSRP の仮想 MAC アドレスを指定します。</p> <ul style="list-style-type: none"> 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。 <p>または</p> <p>仮想 MAC アドレスとしてインターフェイスのバードイン アドレスを使用するように HSRP を設定します。</p> <ul style="list-style-type: none"> scope interface キーワードでは、コマンドの設定対象が、メジャー インターフェイスではなく、コマンドを入力したサブインターフェイスに限定されるように指定されます。
ステップ 6	<pre>standby [group-number] ip [ip-address [secondary]]</pre> <p>例： Router(config-if)# standby 1 ip 172.16.6.100</p>	HSRP をアクティブにします。

HSRP グループへの IP 冗長性クライアントのリンク

ここでは、IP 冗長性クライアントを HSRP グループにリンクする作業を行います。

HSRP により、IP ルーティングのステートレスな冗長性が実現されます。HSRP は、単独ではそれ自身のステートを管理することしかできません。HSRP グループに IP 冗長性クライアントをリンクすると、HSRP がクライアント アプリケーションにサービスを提供できるようになるため、このクライアント アプリケーションがステートフル フェールオーバーを実装できます。

IP 冗長性クライアントは、HSRP を使用して、グループのステートに応じてサービスやリソースを提供または抑制する他の Cisco IOS プロセスまたはアプリケーションです。

HSRP グループのデフォルトの名前は **hsrp-interface-group** であるため、グループ名の指定は省略可能です。たとえば、Ethernet0/0 のグループ 1 のデフォルトの名前は「hsrp-Et0/0-1」です。

前提条件

クライアント アプリケーションでは、**standby name** コマンドで設定したものと同名前を最初に指定する必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip address** *ip-address mask*
5. **standby** [*group-number*] **name** [*redundancy-name*]
6. **standby** [*group-number*] **ip** [*ip-address* [**secondary**]]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	enable 例： Router> enable	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	configure terminal 例： Router# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	interface <i>type number</i> 例： Router(config)# interface Ethernet0/1	インターフェイス タイプを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	ip address <i>ip-address mask</i> 例： Router(config-if)# ip address 10.0.0.1 255.255.255.0	インターフェイスの IP アドレスを指定します。
ステップ 5	standby [<i>group-number</i>] name [<i>redundancy-name</i>] 例： Router(config-if)# standby 1 name HSRP-1	スタンバイ グループの名前を設定します。 • HSRP グループのデフォルトの名前は hsrp-interface-group であるため、グループ名の指定は省略可能です。
ステップ 6	standby [<i>group-number</i>] ip [<i>ip-address</i> [secondary]] 例： Router(config-if)# standby 1 ip 10.0.0.11	HSRP をアクティブにします。

HSRP バージョン 2 への変更

HSRP バージョン 2 は、今後の機能拡張に備え、HSRP バージョン 1 よりも機能を拡張するために導入されました。HSRP バージョン 2 のパケット形式は、バージョン 1 とは異なります。

制約事項

- HSRP バージョン 2 は、LAN エミュレーションを実行している ATM インターフェイスでは使用できません。
- HSRP バージョン 2 は HSRP バージョン 1 と相互運用できません。バージョン 1 とバージョン 2 は相互に排他的な関係であるため、この両方を 1 つのインターフェイスで動作させることはできません。ただし、同じルータの別々の物理インターフェイスで、この別々のバージョンを実行することは可能です。バージョン 1 で許可されているグループ番号の範囲 (0 ~ 255) よりも上のグループが設定されている場合、バージョン 2 からバージョン 1 に変更することはできません。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface *type number***
4. **ip address *ip-address mask***
5. **standby version {1 | 2}**
6. **standby [*group-number*] ip [*ip-address* [**secondary**]]**
7. **end**
8. **show standby**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	enable 例： Router> enable	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	configure terminal 例： Router# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	interface <i>type number</i> 例： Router(config)# interface vlan 400	インターフェイス タイプを設定し、インターフェイス コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	<pre>ip address ip-address mask</pre> <p>例： Router(config-if)# ip address 10.10.28.1 255.255.255.0</p>	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	<pre>standby version {1 2}</pre> <p>例： Router(config-if)# standby version 2</p>	HSRP のバージョンを変更します。
ステップ 6	<pre>standby [group-number] ip [ip-address [secondary]]</pre> <p>例： Router(config-if)# standby 400 ip 10.10.28.5</p>	<p>HSRP をアクティブにします。</p> <ul style="list-style-type: none"> • HSRP バージョン 2 のグループ番号範囲は 0 ~ 4095 に拡張されています。HSRP バージョン 1 のグループ番号範囲は 0 ~ 255 です。
ステップ 7	<pre>end</pre> <p>例： Router(config-if)# end</p>	現在の設定セッションを終了し、特権 EXEC モードに戻ります。
ステップ 8	<pre>show standby</pre> <p>例： Router# show standby</p>	<p>(任意) HSRP に関する情報を表示します。</p> <ul style="list-style-type: none"> • HSRP バージョン 2 関連の情報が表示されます (設定されている場合)。

SSO 対応 HSRP のイネーブル化

この機能は、冗長モードが SSO に設定されている場合にデフォルトでイネーブルになっています。ここでは、SSO に対応するように HSRP を再度イネーブルにする作業を行います（ディセーブルになっている場合）。



(注) SSO が他の接続のトラフィック フローを保持しているときに HSRP トラフィックを冗長デバイスにスイッチする必要がある LAN セグメントがある場合は、**no standby sso** コマンドを使用して SSO HSRP をディセーブルにすることができます。

手順の概要

1. **enable**
2. **configure terminal**
3. **redundancy**
4. **mode sso**
5. **exit**
6. **no standby sso**
7. **standby sso**
8. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	enable 例： Router> enable	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	configure terminal 例： Router# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	redundancy 例： Router(config)# redundancy	冗長コンフィギュレーション モードを開始します。
ステップ 4	mode sso 例： Router(config-red)# mode sso	SSO に対する動作の冗長モードをイネーブルにします。 • このステップを実行すると、HSRP 用に設定されているインターフェイスで HSRP の動作が SSO に対応した状態になり、スタンバイ RP が自動的にリセットされます。
ステップ 5	exit 例： Router(config-red)# exit	冗長コンフィギュレーション モードを終了します。

	コマンドまたはアクション	目的
ステップ 6	<code>no standby sso</code> 例： Router(config)# no standby sso	すべての HSRP グループの HSRP SSO モードをディセーブルにします。
ステップ 7	<code>standby sso</code> 例： Router(config)# standby sso	SSO HSRP 機能をイネーブルにします (ディセーブルになっている場合)。
ステップ 8	<code>end</code> 例： Router(config)# end	現在の設定セッションを終了し、特権 EXEC モードに戻ります。

SSO 対応 HSRP の検証

HSRP の SSO 動作を検証またはデバッグするためには、次の手順をアクティブ RP コンソールで行います。

手順の概要

1. `show standby`
2. `debug standby events ha`

手順の詳細

ステップ 1 `show standby`

`show standby` コマンドを実行すると、スタンバイ RP のステータスが表示されます。次に例を示します。

```
Router# show standby

GigabitEthernet3/25 - Group 1
State is Init (standby RP, peer state is Active)
Virtual IP address is 10.0.0.1
Active virtual MAC address is unknown
Local virtual MAC address is 0000.0c07.ac01 (v1 default)
Hello time 3 sec, hold time 10 sec
Preemption disabled
Active router is unknown
Standby router is unknown
Priority 100 (default 100)
Group name is "hsrp-Gi3/25-1" (default)
```

ステップ 2 `debug standby events ha`

`debug standby events ha` コマンドを実行すると、アクティブ RP とスタンバイ RP が表示されます。次に例を示します。

```
Router# debug standby events ha

!Active RP
```

```
*Sep 1 09:46:19.788 UTC: HSRP: Gi3/25 Grp 1 HA send sync state Listen
*Sep 1 09:46:31.435 UTC: HSRP: Gi3/25 Grp 1 HA send sync state Speak
*Sep 1 09:46:40.940 UTC: HSRP: Gi3/25 Grp 1 HA send sync state Standby
*Sep 1 09:46:41.724 UTC: HSRP: Gi3/25 Grp 1 HA send sync state Active

Standby RP

*Sep 1 09:46:19.143 UTC: STBY: HSRP: Gi3/25 Grp 1 RF sync state Unknown -> Init
*Sep 1 09:46:20.167 UTC: STBY: HSRP: Gi3/25 Grp 1 RF sync state Init -> Listen
*Sep 1 09:46:30.812 UTC: STBY: HSRP: Gi3/25 Grp 1 RF sync state Listen -> Speak
*Sep 1 09:46:41.315 UTC: STBY: HSRP: Gi3/25 Grp 1 RF sync state Speak -> Standby
*Sep 1 09:46:42.103 UTC: STBY: HSRP: Gi3/25 Grp 1 RF sync state Standby -> Active
```

HSRP MIB トラップのイネーブル化

手順の概要

1. **enable**
2. **configure terminal**
3. **snmp-server enable traps hsrp**
4. **snmp-server host *host community-string* hsrp**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	enable 例： Router> enable	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	configure terminal 例： Router# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	snmp-server enable traps hsrp 例： Router(config)# snmp-server enable traps hsrp	SNMP トラップ、SNMP インフォーム、HSRP 通知をルータが送信できるようにします。
ステップ 4	snmp-server host <i>host community-string</i> hsrp 例： Router(config)# snmp-server host myhost.comp.com public hsrp	SNMP 通知動作の受信者と、HSRP 通知がホストに送信されることを指定します。

インターフェイスでの BFD セッションパラメータの設定

ここでは、BFD セッションのベースライン パラメータをインターフェイスで設定して、インターフェイスで BFD を設定する作業を行います。この手順のステップは、BFD ネイバーに BFD セッションを実行する各インターフェイスで行ってください。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface type number**
4. **bfd interval milliseconds min_rx milliseconds multiplier interval-multiplier**
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	enable 例： Router> enable	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	configure terminal 例： Router# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	interface type number 例： Router(config)# interface FastEthernet 6/0	インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	bfd interval milliseconds min_rx milliseconds multiplier interval-multiplier 例： Router(config-if)# bfd interval 50 min_rx 50 multiplier 5	インターフェイスで BFD をイネーブルにします。
ステップ 5	end 例： Router(config-if)# end	インターフェイス コンフィギュレーション モードを終了します。

HSRP BFD ピアリングの設定

ここでは、HSRP BFD ピアリングをイネーブルにする作業を行います。この手順のステップは、HSRP ピアに BFD セッションを実行する各インターフェイスで行ってください。

HSRP はデフォルトで BFD ピアリングをサポートしています。HSRP BFD ピアリングは、手動でディセーブルになっている場合、ルータ レベルで再度イネーブルにして、すべてのインターフェイスの BFD サポートをまとめてイネーブル化したり、インターフェイス レベルでインターフェイスごとに再度イネーブルにしたりすることができます。

前提条件

- 参加中のすべてのルータで HSRP が実行されている。
- Cisco Express Forwarding (CEF; シスコ エクスプレス フォワーディング) がイネーブルになっている。

手順の概要

1. `enable`
2. `configure terminal`
3. `ip cef [distributed]`
4. `interface type number`
5. `ip address ip-address mask`
6. `standby [group-number] ip [ip-address [secondary]]`
7. `standby bfd`
8. `exit`
9. `standby bfd all-interfaces`
10. `exit`
11. `show standby [neighbors]`

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<code>enable</code> 例: Router> enable	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	<code>configure terminal</code> 例: Router# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	<code>ip cef [distributed]</code> 例: Router(config)# ip cef	CEF または分散 CEF をイネーブルにします。

	コマンドまたはアクション	目的
ステップ 4	interface <i>type number</i> 例： Router(config)# interface FastEthernet 6/0	インターフェイス コンフィギュレーション モードを開始します。
ステップ 5	ip address <i>ip-address mask</i> 例： Router(config-if)# ip address 10.0.0.11 255.255.255.0	インターフェイスの IP アドレスを設定します。
ステップ 6	standby [<i>group-number</i>] ip [<i>ip-address</i> [secondary]] 例： Router(config-if)# standby 1 ip 10.0.0.11	HSRP をアクティブにします。
ステップ 7	standby bfd 例： Router(config-if)# standby bfd	(任意) インターフェイスで HSRP の BFD サポートをイネーブルにします。
ステップ 8	exit 例： Router(config-if)# exit	インターフェイス コンフィギュレーション モードを終了します。
ステップ 9	standby bfd all-interfaces 例： Router(config)# standby bfd all-interfaces	(任意) すべてのインターフェイスで HSRP の BFD サポートをイネーブルにします。
ステップ 10	exit 例： Router(config)# exit	グローバル コンフィギュレーション モードを終了します。
ステップ 11	show standby [<i>neighbors</i>] 例： Router# show standby neighbors	(任意) HSRP の BFD サポートに関する情報を表示します。

HSRP BFD ピアリングの検証

HSRP BFD ピアリングを検証するには、次のコマンドを必要に応じて実行します。

手順の概要

1. **show standby**
2. **show standby neighbors** [*type number*]
3. **show bfd neighbor** [*details*]

手順の詳細

ステップ 1 **show standby**

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

```
Router# show standby

FastEthernet2/0 - Group 1
  State is Active
    2 state changes, last state change 00:08:06
  Virtual IP address is 10.0.0.11
  Active virtual MAC address is 0000.0c07.ac01
    Local virtual MAC address is 0000.0c07.ac01 (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 2.772 secs
  Preemption enabled
  Active router is local
  Standby router is 10.0.0.2, priority 90 (expires in 8.268 sec)
  BFD enabled !
  Priority 110 (configured 110)
  Group name is "hsrp-Fa2/0-1" (default)
```

ステップ 2 **show standby neighbors** [*type number*]

show standby neighbors コマンドを実行すると、インターフェイスの HSRP ピア ルータに関する情報が表示されます。

```
Router1# show standby neighbors

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

Router2# show standby neighbors

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

ステップ 3 **show bfd neighbors** [*details*]

show bfd neighbors コマンドを実行すると、現在の Bidirectional Forwarding Detection (BFD; 双方向フォワーディング検出) の隣接関係が 1 行ずつ一覧表示されます。**details** キーワードを付けると、各ネイバーの BFD プロトコルのパラメータとタイマーが表示されます。

```

Router# show bfd neighbors details

OurAddr      NeighAddr    LD/RD  RH/RS  Holdown(mult)  State  Int
10.0.0.2     10.0.0.1     5/0    Down   0 (0)          Down   Fa2/0
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 1000000, MinRxInt: 1000000, Multiplier: 3
Received MinRxInt: 0, Received Multiplier: 0
Holdown (hits): 0(0), Hello (hits): 1000(55)
Rx Count: 0, Rx Interval (ms) min/max/avg: 0/0/0 last: 3314120 ms ago
Tx Count: 55, Tx Interval (ms) min/max/avg: 760/1000/872 last: 412 ms ago
Registered protocols: HSRP !
Last packet: Version: 1          - Diagnostic: 0
                  State bit: AdminDown - Demand bit: 0
                  Poll bit: 0          - Final bit: 0
                  Multiplier: 0        - Length: 0
                  My Discr.: 0         - Your Discr.: 0
                  Min tx interval: 0   - Min rx interval: 0
                  Min Echo interval: 0

```

HSRP gratuitous ARP の設定

ここでは、ARP キャッシュのエントリが正しいことを確認し、1 つまたは複数のアクティブ HSRP グループから gratuitous ARP パケットを定期的送信するように HSRP を設定する作業を行います。HSRP は、デフォルトでは HSRP グループのステータスが Active に変化したときに、そのグループから gratuitous ARP パケットを 3 個送信します。最初の 1 個はグループがアクティブになったときに送信しますが、残りの 2 個が送信されるのは 2 秒後と 4 秒後です。

手順の概要

1. **enable**
2. **standby send arp** [*interface-type interface-number* [*group-number*]]
3. **configure terminal**
4. **interface** *type number*
5. **standby arp gratuitous** [*count number*] [*interval seconds*]
6. **end**
7. **show standby arp gratuitous** [*type number*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	enable 例： Router> enable	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	standby send arp [<i>interface-type</i> <i>interface-number</i> [<i>group-number</i>]] 例： Router# standby send arp Ethernet1/1 1	(任意) アクティブ HSRP グループごとに 1 つの gratuitous ARP パケットを送信するように HSRP を設定します。

	コマンドまたはアクション	目的
ステップ 3	configure terminal 例： Router# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 4	interface type number 例： Router(config)# interface Ethernet1/1	インターフェイス タイプを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 5	standby arp gratuitous [count number] [interval seconds] 例： Router(config-if)# standby arp gratuitous count 3 interval 4	アクティブ HSRP グループによって送信される gratuitous ARP パケットの数と送信頻度を設定します。
ステップ 6	end 例： Router(config-if)# end	(任意) 特権 EXEC モードに戻ります。
ステップ 7	show standby arp gratuitous [type number] 例： Router# show standby arp gratuitous ethernet1/1	(任意) HSRP によって送信される gratuitous ARP パケットの数と、設定されている送信間隔を表示します。

例

次のサンプルは、**show standby arp gratuitous** コマンドからの出力です。

```
Router# show standby arp gratuitous ethernet1/1

HSRP Gratuitous ARP
Interface          Interval  Count
Ethernet1/1 4          3
```

HSRP の設定例

- 「例：HSRP のプライオリティとプリエンプション」 (P.56)
- 「例：HSRP オブジェクト トラッキング」 (P.57)
- 「例：HSRP グループ シャットダウン」 (P.57)
- 「例：キー ストリングを使用した HSRP MD5 認証」 (P.58)
- 「例：キー チェーンを使用した HSRP MD5 認証」 (P.58)
- 「例：キー ストリングとキー チェーンを使用した HSRP MD5 認証」 (P.58)
- 「例：HSRP テキスト認証」 (P.59)
- 「例：ロード バランシング用の複数の HSRP」 (P.59)
- 「例：HSRP 複数グループ最適化を使用した CPU およびネットワークのパフォーマンスの向上」 (P.61)
- 「例：ICMP リダイレクト メッセージの HSRP サポート」 (P.61)
- 「例：HSRP 仮想 MAC アドレスと BIA MAC アドレス」 (P.62)
- 「例：HSRP グループへの IP 冗長性クライアントのリンク」 (P.62)
- 「例：HSRP バージョン 2」 (P.63)
- 「例：SSO HSRP」 (P.63)
- 「例：HSRP MIB トラップ」 (P.63)
- 「例：HSRP BFD ピアリング」 (P.64)
- 「例：HSRP Gratuitous ARP」 (P.65)

例：HSRP のプライオリティとプリエンプション

次の例では、ルータ A は、ルータ B よりもプライオリティが高いためにグループ 1 のアクティブ ルータになっているほか、グループ 2 のスタンバイ ルータになっています。ルータ B は、グループ 2 のアクティブ ルータおよびグループ 1 のスタンバイ ルータになるように設定されています。

ルータ A の設定

```
Router(config)# interface Ethernet0/0
Router(config-if)# ip address 10.1.0.21 255.255.0.0
Router(config-if)# standby 1 priority 110
Router(config-if)# standby 1 preempt
Router(config-if)# standby 1 ip 10.1.0.1
Router(config-if)# standby 2 priority 95
Router(config-if)# standby 2 preempt
Router(config-if)# standby 2 ip 10.1.0.2
```

ルータ B の設定

```
Router(config)# interface Ethernet0/0
Router(config-if)# ip address 10.1.0.22 255.255.0.0
Router(config-if)# standby 1 preempt
Router(config-if)# standby 1 priority 105
Router(config-if)# standby 1 ip 10.1.0.1
Router(config-if)# standby 2 priority 110
Router(config-if)# standby 2 preempt
Router(config-if)# standby 2 ip 10.1.0.2
```

例 : HSRP オブジェクト トラッキング

次の例では、トラッキング プロセスはシリアル インターフェイス 1/0 の IP ルーティング機能を追跡するように設定されています。イーサネット インターフェイス 0/0 の HSRP は、シリアル インターフェイス 1/0 の IP ルーティング ステートに何らかの変更が生じた場合には通知されるように、トラッキング プロセスに登録します。シリアル インターフェイス 1/0 の IP ステートがダウンになると、その HSRP グループのプライオリティが 10 だけ引き下げられます。

両方のシリアル インターフェイスが動作している場合は、ルータ A はルータ B よりもプライオリティが高いので、ルータ A が HSRP アクティブ ルータになります。ただし、ルータ A のシリアル インターフェイス 1/0 の IP ルーティングに障害が発生すると、HSRP グループのプライオリティが引き下げられてルータ B がアクティブ ルータとして処理を引き継ぐため、ホストに対するデフォルトの仮想ゲートウェイ サービスはサブネット 10.1.0.0 で継続されます。

ルータ A の設定

```
Router(config)# track 100 interface serial1/0 ip routing
Router(config-track)# exit
Router(config)# interface Ethernet0/0
Router(config-if)# ip address 10.1.0.21 255.255.0.0
Router(config-if)# standby 1 preempt
Router(config-if)# standby 1 priority 110
Router(config-if)# standby 1 track 100 decrement 10
Router(config-if)# standby 1 ip 10.1.0.1
```

ルータ B の設定

```
Router(config)# track 100 interface serial1/0 ip routing
Router(config-track)# exit
Router(config)# interface Ethernet0/0
Router(config-if)# ip address 10.1.0.22 255.255.0.0
Router(config-if)# standby 1 preempt
Router(config-if)# standby 1 priority 105
Router(config-if)# standby 1 track 100 decrement 10
Router(config-if)# standby 1 ip 10.1.0.1
```

例 : HSRP グループ シャットダウン

次の例では、トラッキング プロセスはシリアル インターフェイス 1/0 の IP ルーティング機能を追跡するように設定されています。イーサネット インターフェイス 0/0 の HSRP は、シリアル インターフェイス 1/0 の IP ルーティング ステートに何らかの変更が生じた場合には通知されるように、トラッキング プロセスに登録します。シリアル インターフェイス 1/0 の IP ステートがダウンになると、HSRP グループはディセーブルになります。

両方のシリアル インターフェイスが動作している場合は、ルータ A はルータ B よりもプライオリティが高いので、ルータ A が HSRP アクティブ ルータになります。ただし、ルータ A のシリアル インターフェイス 1/0 の IP ルーティングに障害が発生すると、HSRP グループがディセーブルになってルータ B がアクティブ ルータとして処理を引き継ぐため、ホストに対するデフォルトの仮想ゲートウェイ サービスはサブネット 10.1.0.0 で継続されます。

ルータ A の設定

```
Router(config)# track 100 interface serial1/0 ip routing
Router(config-track)# exit
Router(config)# interface Ethernet0/0
Router(config-if)# ip address 10.1.0.21 255.255.0.0
Router(config-if)# standby 1 ip 10.1.0.1
Router(config-if)# standby 1 preempt
```

```
Router(config-if)# standby 1 priority 110
Router(config-if)# standby 1 track 100 shutdown
```

ルータ B の設定

```
Router(config)# track 100 interface serial1/0 ip routing
Router(config-track)# exit
Router(config)# interface Ethernet0/0
Router(config-if)# ip address 10.1.0.22 255.255.0.0
Router(config-if)# standby 1 ip 10.1.0.1
Router(config-if)# standby 1 preempt
Router(config-if)# standby 1 priority 105
Router(config-if)# standby 1 track 100 shutdown
```

あるオブジェクトが HSRP グループによってすでにトラッキングされている場合、HSRP グループ シャットダウン機能を使用するようにこのトラッキング設定を変更することはできません。先に、**no standby track** コマンドを使用してトラッキング設定を解除し、**shutdown** キーワードとともに **standby track** コマンドを使用してトラッキング設定を再度設定する必要があります。

次の例は、HSRP グループ シャットダウン機能が追加されるようにトラッキング対象のオブジェクトの設定を変更する方法を示しています。

```
Router(config-if)# no standby 1 track 101 decrement 10
Router(config-if)# standby 1 track 101 shutdown
```

例：キー ストリングを使用した HSRP MD5 認証

次に、キー ストリングを使用して HSRP MD5 認証を設定する例を示します。

```
Router(config)# interface Ethernet0/1
Router(config-if)# standby 1 priority 110
Router(config-if)# standby 1 preempt
Router(config-if)# standby 1 authentication md5 key-string 54321098452103ab timeout 30
Router(config-if)# standby 1 ip 10.21.0.10
```

例：キー チェーンを使用した HSRP MD5 認証

次の例では、特定のキー チェーンに対して現在アクティブになっているキーとキー ID を取得するため、HSRP にはキー チェーン「hsrp1」が必要です。

```
Router(config)# key chain hsrp1
Router(config-keychain)# key 1
Router(config-keychain-key)# key-string 54321098452103ab
Router(config-keychain-key)# exit
Router(config)# interface Ethernet0/1
Router(config-if)# standby 1 priority 110
Router(config-if)# standby 1 preempt
Router(config-if)# standby 1 authentication md5 key-chain hsrp1
Router(config-if)# standby 1 ip 10.21.0.10
```

例：キー ストリングとキー チェーンを使用した HSRP MD5 認証

キー ストリング認証のキー ID は常にゼロです。キー チェーンのキー ID がゼロに設定されている場合、次のように設定できます。

ルータ 1

```
Router(config)# key chain hsrp1
```

```
Router(config-keychain)# key 0
Router(config-keychain-key)# key-string 54321098452103ab
Router(config-keychain-key)# exit
Router(config)# interface Ethernet0/1

Router(config-if)# standby 1 authentication md5 key-chain hsrp1
Router(config-if)# standby 1 ip 10.21.0.10
```

ルータ 2

```
Router(config)# interface Ethernet0/1
Router(config-if)# standby 1 authentication md5 key-string 54321098452103ab
Router(config-if)# standby 1 ip 10.21.0.10
```

例：HSRP テキスト認証

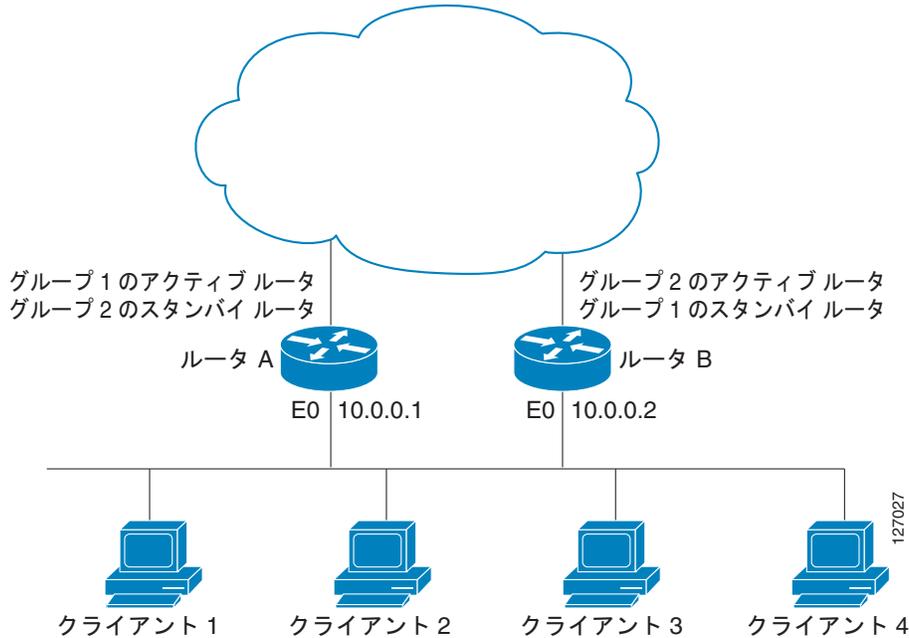
次の例は、テキスト文字列を使用して HSRP テキスト認証を設定する方法を示しています。

```
Router(config)# interface Ethernet0/1
Router(config-if)# standby 1 priority 110
Router(config-if)# standby 1 preempt
Router(config-if)# standby 1 authentication text company2
Router(config-if)# standby 1 ip 10.21.0.10
```

例：ロード バランシング用の複数の HSRP

ロードシェアリングを設定するときは、HSRP または複数の HSRP グループを使用できます。図 4 では、クライアントの半数はルータ A 用に設定され、残りの半数はルータ B 用に設定されています。ルータ A とルータ B の設定が組み合わせられて、2 つのホットスタンバイグループが確立されています。グループ 1 では、ルータ A に最も高いプライオリティが割り当てられているため、ルータ A がデフォルトのアクティブルータであり、ルータ B がスタンバイルータです。グループ 2 では、ルータ B に最も高いプライオリティが割り当てられているため、ルータ B がデフォルトのアクティブルータであり、ルータ A がスタンバイルータです。通常の動作中は、2 つのルータに IP トラフィックの負荷が共有されます。どちらかのルータが使用不能になると、もう一方のルータがアクティブになり、使用不能になったルータの packets 転送機能を引き継ぎます。ルータが停止し、後で復帰した場合に、プリエンプションを実行してロードシェアリング状態に戻すために、インターフェイス コンフィギュレーション コマンド **standby preempt** が必要です。

図 4 HSRP ロード シェアリングの例



次の例は、プライオリティが 110 で、グループ 1 のアクティブ ルータとして設定されているルータ A と、プライオリティが 110 で、グループ 2 のアクティブ ルータとして設定されているルータ B を示しています。デフォルトのプライオリティ レベルは 100 です。グループ 1 で使用されている仮想 IP アドレスは 10.0.0.3 で、グループ 2 で使用されている仮想 IP アドレスは 10.0.0.4 です。

ルータ A の設定

```
Router(config)# hostname RouterA
RouterA(config)# interface ethernet 0
RouterA(config-if)# ip address 10.0.0.1 255.255.255.0
RouterA(config-if)# standby 1 ip 10.0.0.3
RouterA(config-if)# standby 1 priority 110
RouterA(config-if)# standby 1 preempt
RouterA(config-if)# standby 2 preempt
RouterA(config-if)# standby 2 ip 10.0.0.4
```

ルータ B の設定

```
Router(config)# hostname RouterB
RouterB(config)# interface ethernet 0
RouterB(config-if)# ip address 10.0.0.2 255.255.255.0
RouterB(config-if)# standby 1 ip 10.0.0.3
RouterB(config-if)# standby 1 preempt
RouterB(config-if)# standby 2 priority 110
RouterB(config-if)# standby 2 preempt
RouterB(config-if)# standby 2 ip 10.0.0.4
```

例：HSRP 複数グループ最適化を使用した CPU およびネットワークのパフォーマンスの向上

次の例は、HSRP クライアントおよびマスター グループを設定する方法を示しています。

```
Router(config)# interface Ethernet1/0
Router(config-if)# no shutdown
Router(config-if)# standby mac-refresh 30
! Client Hello message interval
!
Router(config)# interface Ethernet1/0.2
Router(config-if)# no shutdown
Router(config-if)# encapsulation dot1Q 2
Router(config-if)# ip vrf forwarding VRF2
Router(config-if)# ip address 10.0.0.100 255.255.0.0
Router(config-if)# standby 1 ip 10.0.0.254
Router(config-if)# standby 1 priority 110
Router(config-if)# standby 1 preempt
Router(config-if)# standby 1 name HSRP1
!Server group
!
Router(config)# interface Ethernet1/0.3
Router(config-if)# no shutdown
Router(config-if)# encapsulation dot1Q 3
Router(config-if)# ip vrf forwarding VRF3
Router(config-if)# ip address 10.0.0.100 255.255.0.0
Router(config-if)# standby 2 ip 10.0.0.254
Router(config-if)# standby 2 follow HSRP1
! Client group
!
Router(config)# interface Ethernet1/0.4
Router(config-if)# no shutdown
Router(config-if)# encapsulation dot1Q 4
Router(config-if)# ip vrf forwarding VRF4
Router(config-if)# ip address 10.0.0.100 255.255.0.0
Router(config-if)# standby 2 ip 10.0.0.254
Router(config-if)# standby 2 follow HSRP1
! Client group
```

例：ICMP リダイレクト メッセージの HSRP サポート

次の設定例は、ICMP リダイレクト メッセージのフィルタリングが可能な 2 つの HSRP グループです。

ルータ A の設定：グループ 1 に対してはアクティブでグループ 2 に対してはスタンバイ

```
RouterA(config)# interface Ethernet1
RouterA(config-if)# ip address 10.0.0.10 255.0.0.0
RouterA(config-if)# standby redirect
RouterA(config-if)# standby 1 priority 120
RouterA(config-if)# standby 1 preempt delay minimum 20
RouterA(config-if)# standby 1 ip 10.0.0.1
RouterA(config-if)# standby 2 priority 105
RouterA(config-if)# standby 2 preempt delay minimum 20
RouterA(config-if)# standby 2 ip 10.0.0.2
```

ルータ B の設定：グループ 1 に対してはスタンバイでグループ 2 に対してはアクティブ

```
RouterB(config)# interface Ethernet1
RouterB(config-if)# ip address 10.0.0.11 255.0.0.0
RouterB(config-if)# standby redirect
```

```

RouterB(config-if)# standby 1 priority 105
RouterB(config-if)# standby 1 preempt delay minimum 20
RouterB(config-if)# standby 1 ip 10.0.0.1
RouterB(config-if)# standby 2 priority 120
RouterB(config-if)# standby 2 preempt delay minimum 20
RouterB(config-if)# standby 2 ip 10.0.0.2

```

例：HSRP 仮想 MAC アドレスと BIA MAC アドレス

APPN ネットワークでは、エンドノードは隣接するネットワーク ノードの MAC アドレスを使用して設定されていることがほとんどです。次の例では、エンドノードが 4000.1000.1060 を使用するように設定されている場合、HSRP グループ 1 は同じ MAC アドレスを使用するように設定されます。

```

Router(config)# interface Ethernet0/2
Router(config-if)# ip address 10.0.0.1
Router(config-if)# standby 1 mac-address 4000.1000.1060
Router(config-if)# standby 1 ip 10.0.0.11

```

次の例では、トークンリング インターフェイス 3/0 のバーンドインアドレスは、仮想 IP アドレスにマッピングされる仮想 MAC アドレスになります。

```

Router(config)# interface token3/0
Router(config-if)# standby use-bia

```



(注)

standby use-bia コマンドと **standby mac-address** コマンドを同じ設定で使用することはできません。

例：HSRP グループへの IP 冗長性クライアントのリンク

次の例は、HSRP のスタティック NAT 設定サポートを示しています。NAT クライアントアプリケーションは、**standby name** コマンドで指定される名前の相互関係によって HSRP にリンクされます。また、2 台のルータが HSRP アクティブ ルータと HSRP スタンバイ ルータとして動作しているほか、インターフェイス内の NAT は HSRP が使用可能になっており、「group1」という名前のグループに属するように設定されています。

アクティブ ルータの設定

```

Router(config)# interface BVI10
Router(config-if)# ip address 192.168.5.54 255.255.255.255.0
Router(config-if)# no ip redirects
Router(config-if)# ip nat inside
Router(config-if)# standby 10 ip 192.168.5.30
Router(config-if)# standby 10 priority 110
Router(config-if)# standby 10 preempt
Router(config-if)# standby 10 name group1
Router(config-if)# standby 10 track Ethernet2/1
!
!
Router(config)# ip default-gateway 10.0.18.126
Router(config)# ip nat inside source static 192.168.5.33 10.10.10.5 redundancy group1
Router(config)# ip classless
Router(config)# ip route 10.10.10.0 255.255.255.0 Ethernet2/1
Router(config)# ip route 172.22.33.0 255.255.255.0 Ethernet2/1
Router(config)# no ip http server

```

スタンバイ ルータの設定

```

Router(config)# interface BVI10
Router(config-if)# ip address 192.168.5.56 255.255.255.255.0

```

```
Router(config-if)# no ip redirects
Router(config-if)# ip nat inside
Router(config-if)# standby 10 priority 95
Router(config-if)# standby 10 preempt
Router(config-if)# standby 10 name group1
Router(config-if)# standby 10 ip 192.168.5.30
Router(config-if)# standby 10 track Ethernet3/1
Router(config-if)# exit
Router(config)# ip default-gateway 10.0.18.126
Router(config)# ip nat inside source static 192.168.5.33 3.3.3.5 redundancy group1
Router(config)# ip classless
Router(config)# ip route 10.0.32.231 255.255.255 Ethernet3/1
Router(config)# ip route 10.10.10.0 255.255.255.0 Ethernet3/1
Router(config)# no ip http server
```

例 : HSRP バージョン 2

次の例は、グループ番号が 350 のインターフェイスで HSRP バージョン 2 を設定する方法を示しています。

```
Router(config)# interface vlan350
Router(config-if)# standby version 2
Router(config-if)# standby 350 priority 110
Router(config-if)# standby 350 preempt
Router(config-if)# standby 350 timers 5 15
Router(config-if)# standby 350 ip 172.20.100.10
```

例 : SSO HSRP

次の例は、冗長モードを SSO に設定する方法を示しています。このモードがイネーブルになっていると、HSRP は自動的に SSO に対応します。

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

no standby sso コマンドを使用して SSO HSRP をディセーブルにしている場合は、**standby sso** コマンドをグローバル コンフィギュレーション モードで使用して SSO HSRP を再度イネーブルにすることができます。

例 : HSRP MIB トラップ

次の例は、HSRP を 2 台のルータで設定し、HSRP MIB トラップのサポート機能をイネーブルにする方法を示しています。多くの環境と同様に、1 台のルータがアクティブ ルータとして優先されます。あるルータにアクティブ ルータとしての優先度を設定するには、他のルータよりも高いプライオリティ レベルでそのルータを設定し、プリエンプションをイネーブルにします。次の例では、アクティブ ルータはプライマリ ルータと呼ばれ、2 番目のルータはバックアップ ルータと呼ばれます。

ルータ A

```
RouterA(config)# interface Ethernet1
RouterA(config-if)# ip address 10.1.1.1 255.255.0.0
RouterA(config-if)# standby priority 200
RouterA(config-if)# standby preempt
RouterA(config-if)# standby ip 10.1.1.3
RouterA(config-if)# exit
RouterA(config)# snmp-server enable traps hsrp
RouterA(config)#snmp-server host yourhost.cisco.com public hsrp
```

ルータ B

```

RouterB(config)# interface Ethernet1
RouterB(config-if)# ip address 10.1.1.2 255.255.0.0
RouterB(config-if)# standby priority 101
RouterB(config-if)# standby ip 10.1.1.3
RouterB(config-if)# exit
RouterB(config)# snmp-server enable traps hsrp
RouterB(config)# snmp-server host myhost.cisco.com public hsrp

```

例 : HSRP BFD ピアリング

HSRP は、HSRP グループ メンバーのヘルス モニタリング システムの一部として BFD をサポートしています。BFD がないと、HSRP はマルチプロセス システムの 1 つのプロセスとして動作するため、ミリ秒の hello タイマーやホールド タイマーを使用して大量のグループに対応できるように適切なタイミングでスケジュールされることが保証されません。BFD は疑似プリエンティブ プロセスとして動作するため、必要なときに実行されることが保証されます。複数の HSRP グループに早期フェールオーバー通知を実行できるのは、2 台のルータ間の 1 つの BFD セッションだけです。

次の例では、**standby bfd** コマンドと **standby bfd all-interfaces** コマンドは表示されません。**bfd interval** コマンドを使用して、BFD がルータまたはインターフェイスで設定されているときは、HSRP の BFD サポートはデフォルトでイネーブルになっています。**standby bfd** コマンドと **standby bfd all-interfaces** コマンドが必要なのは、ルータまたはインターフェイスで BFD が手動でディセーブルになっている場合だけです。

ルータ A

```

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

```

ルータ B

```

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

```

例 : HSRP Gratuitous ARP

次の例は、ARP キャッシュのエントリが正しいことを確認し、インターフェイスの HSRP グループがアクティブ ステートに変化したときに 4 秒間隔で gratuitous ARP パケットを 3 個送信するように HSRP を設定する方法を示しています。

```
Router> enable
Router# standby send arp Ethernet1/1 1
Router# configure terminal
Router(config)# interface Ethernet1/1
Router(config-if)# standby arp gratuitous count 3 interval 4
Router(config-if)# end
Router# show standby arp gratuitous ethernet1/1
```

```
HSRP Gratuitous ARP
Interface Interval Count
Ethernet1/1 4 3
```

その他の参考資料

関連資料

内容	参照先
Cisco IOS コマンド	『 Cisco IOS Master Commands List, All Releases 』
BFD	「 Bidirectional Forwarding Detection 」モジュール
GLBP	「 Configuring GLBP 」モジュール
HSRP コマンド : complete コマンド構文、コマンドモード、コマンド履歴、デフォルト設定、使用に関する注意事項および例	『 Cisco IOS IP Application Services Command Reference 』
HSRP と IPsec	「 IPsec VPN High Availability Enhancements 」モジュールの「 Hot Standby Routing Protocol and IPsec 」
HSRP と IPv6	「 Configuring First Hop Redundancy Protocols in IPv6 」モジュール
ISSU	<ul style="list-style-type: none"> 『Cisco IOS In Service Software Upgrade Process』 『Catalyst 4500 Series Switch Cisco IOS Software Configuration Guide』（リリース 12.2(31)SGA）の「Configuring the Cisco IOS In Service Software Upgrade Process」モジュール
オブジェクトトラッキング	「 Configuring Enhanced Object Tracking 」モジュール
HSRP のトラブルシューティング	<ul style="list-style-type: none"> 『Understanding and Troubleshooting HSRP Problems in Catalyst Switch Networks』 『Hot Standby Router Protocol: Frequently Asked Questions』
VRRP	「 Configuring VRRP 」モジュール

規格

規格	タイトル
この機能がサポートする新しい規格または変更された規格はありません。また、この機能による既存規格のサポートに変更はありません。	—

MIB

MIB	MIB リンク
CISCO-HSRP-MIB CISCO-HSRP-EXT-MIB	選択されたプラットフォーム、シスコ ソフトウェア リリース、およびフィーチャセットの MIB を検索してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
RFC 792	「 <i>Internet Control Message Protocol</i> 」
RFC 1828	「 <i>IP Authentication Using Keyed MD5</i> 」
RFC 2281	「 <i>Cisco Hot Standby Router Protocol</i> 」

シスコのテクニカル サポート

説明	リンク
<p>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。</p> <p>以下を含むさまざまな作業にこの Web サイトが役立ちます。</p> <ul style="list-style-type: none"> ・テクニカル サポートを受ける ・ソフトウェアをダウンロードする ・セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける ・ツールおよびリソースへアクセスする <ul style="list-style-type: none"> - Product Alert の受信登録 - Field Notice の受信登録 - Bug Toolkit を使用した既知の問題の検索 ・Networking Professionals (NetPro) コミュニティで、技術関連のディスカッションに参加する ・トレーニング リソースへアクセスする ・TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する <p>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。</p>	http://www.cisco.com/cisco/web/support/index.html

HSRP の機能情報

表 1 に、この章に記載されている機能および具体的な設定情報へのリンクを示します。

プラットフォーム サポートとソフトウェア イメージ サポートに関する情報を入手するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator を使用すると、特定のソフトウェア リリース、フィーチャセット、またはプラットフォームをサポートするソフトウェア イメージを確認できます。Cisco Feature Navigator には、<http://www.cisco.com/go/cfn> からアクセスします。Cisco.com のアカウントは必要ありません。

表 1 HSRP の機能情報

機能名	リリース	機能情報
FHRP - HSRP BFD ピアリング	12.4(11)T	<p>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。</p> <p>この機能に関する詳細については、次の各項を参照してください。</p> <ul style="list-style-type: none"> 「HSRP の BFD ピアリング」(P.18) 「インターフェイスでの BFD セッション パラメータの設定」(P.50) 「HSRP BFD ピアリングの設定」(P.51) 「HSRP BFD ピアリングの検証」(P.53) 「例：HSRP BFD ピアリング」(P.64) <p>この機能によって導入または修正されたコマンドは、debug standby events neighbor、show standby、show standby neighbors、standby bfd、standby bfd all-interfaces です。</p>

表 1 HSRP の機能情報 (続き)

機能名	リリース	機能情報
FHRP - HSRP グループ シャットダウン	12.4(9)T 12.2(33)SRC 12.2(33)SXI 15.0(1)S	<p>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。</p> <p>この機能に関する詳細については、次の各項を参照してください。</p> <ul style="list-style-type: none"> 「HSRP グループ シャットダウン」 (P.15) 「HSRP のオブジェクト トラッキングの設定」 (P.26) 「例 : HSRP グループ シャットダウン」 (P.57) <p>standby track および show standby の各コマンドがこの機能によって修正されました。</p>
FHRP - HSRP - MIB	12.0(3)T 12.0(12)S	<p>FHRP - HSRP - MIB 機能により、CISCO - HRSP - MIB がサポートされています。</p>
FHRP - HSRP 複数グループ最適化	12.4(6)T 12.2(33)SRB 12.2(33)SXI 15.0(1)S	<p>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。</p> <p>この機能に関する詳細については、次の各項を参照してください。</p> <ul style="list-style-type: none"> 「HSRP 複数グループ最適化」 (P.16) 「HSRP 複数グループ最適化による CPU およびネットワークのパフォーマンスの向上」 (P.39) 「例 : HSRP 複数グループ最適化を使用した CPU およびネットワークのパフォーマンスの向上」 (P.61) <p>standby follow および show standby の各コマンドがこの機能によって導入または修正されました。</p>
FHRP - HSRP の IPv6 サポート	12.4(4)T 12.2(33)SRB 12.2(33)SXI	<p>IPv6 のサポートが追加されました。</p> <p>詳細については、『<i>Cisco IOS IPv6 Configuration Guide</i>』の「Configuring First Hop Redundancy Protocols in IPv6」モジュールを参照してください。</p>
HSRP : グローバル IPv6 アドレス	12.2(33)SXI4	<p>グローバル IPv6 の HSRP サポートが追加されました。</p> <p>詳細については、『<i>Cisco IOS IPv6 Configuration Guide</i>』の「Configuring First Hop Redundancy Protocols in IPv6」モジュールを参照してください。</p>

表 1 HSRP の機能情報 (続き)

機能名	リリース	機能情報
HSRP gratuitous ARP	12.2(33)SXI	<p>HSRP gratuitous ARP 機能により、HSRP は ARP キャッシュ内のエントリが正しいことを確認し、1 つまたは複数のアクティブ HSRP グループから gratuitous ARP パケットを定期的送信するように設定されます。</p> <p>この機能に関する詳細については、次の各項を参照してください。</p> <ul style="list-style-type: none"> 「HSRP gratuitous ARP」 (P.11) 「HSRP gratuitous ARP の設定」 (P.54) 「例 : HSRP Gratuitous ARP」 (P.65) <p>show standby arp gratuitous、standby arp gratuitous、standby send arp の各コマンドがこの機能によって導入されました。</p> <p>show standby および debug standby events の各コマンドがこの機能によって修正されました。</p>
HSRP - ISSU	Cisco IOS XE 3.1.0SG 12.2(31)SGA 12.2(33)SRB1 15.0(1)S	<p>HSRP - In-Service Software Upgrade (ISSU; インサービスマソフトウェアアップグレード) 機能により、HSRP で ISSU がサポートされています。</p> <p>In-Service Software Upgrade (ISSU; インサービスマソフトウェアアップグレード) プロセスにより、パケット転送を続行しながら、Cisco IOS ソフトウェアをアップデートまたは修正することができます。ほとんどのネットワークでは、予定されているソフトウェアアップグレードがダウンタイムの大きな原因になっています。ISSU を使用すると、パケット転送を続行しながら Cisco IOS ソフトウェアを修正できるので、ネットワークの可用性が向上し、予定されているソフトウェアアップグレードによるダウンタイムを短縮することができます。このマニュアルでは、ISSU の概念が説明されているほか、ISSU をシステムで実行するのに必要な手順が説明されています。</p> <p>この機能については、次の項に説明があります。</p> <ul style="list-style-type: none"> 「HSRP - ISSU」 (P.17) <p>この機能の詳細については、『<i>Cisco IOS In Service Software Upgrade Process</i>』を参照してください。</p> <p>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。</p>

表 1 HSRP の機能情報 (続き)

機能名	リリース	機能情報
HSRP MD5 認証	Cisco IOS XE 3.1.0SG 12.3(2)T 12.2(25)S 12.2(33)SRA 12.2(33)SXH 15.0(1)S	<p>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。</p> <p>この機能に関する詳細については、次の各項を参照してください。</p> <ul style="list-style-type: none"> • 「HSRP MD5 認証」 (P.9) • 「キー スtringを使用した HSRP MD5 認証の設定」 (P.28) • 「キー チェーンを使用した HSRP MD5 認証の設定」 (P.30) • 「HSRP MD5 認証のトラブルシューティング」 (P.32) • 「例：キー スtringを使用した HSRP MD5 認証」 (P.58) • 「例：キー チェーンを使用した HSRP MD5 認証」 (P.58) • 「例：キー スtringとキー チェーンを使用した HSRP MD5 認証」 (P.58) <p>show standby および standby authentication の各コマンドがこの機能によって導入または修正されました。</p>
HSRP の ICMP リダイレクト サポート	12.1(3)T 15.0(1)S	<p>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。</p> <p>この機能に関する詳細については、次の各項を参照してください。</p> <ul style="list-style-type: none"> • 「HSRP の ICMP リダイレクト サポート」 (P.12) • 「HSRP の ICMP リダイレクト サポートのイネーブル化」 (P.41) • 「例：ICMP リダイレクト メッセージの HSRP サポート」 (P.61) <p>この機能によって導入または修正されたコマンドは、debug standby event、debug standby events icmp、show standby、standby redirects です。</p>

表 1 HSRP の機能情報 (続き)

機能名	リリース	機能情報
HSRP の MPLS VPN サポート	12.0(23)S、 12.0(17)ST、 12.2(28)SB、 12.2(17b)SXA 、12.2(8)T 15.0(1)S	<p>HSRP の Multiprotocol Label Switching (MPLS; マルチプロトコル ラベル スイッチング) Virtual Private Network (VPN; バーチャル プライベート ネットワーク) インターフェイス サポートが役に立つのは、次のいずれかの状態で 2 つの Provider Edge (PE; プロバイダー エッジ) ルータ間でイーサネット LAN が接続されている場合です。</p> <p>この機能については、次の項に説明があります。</p> <ul style="list-style-type: none"> 「HSRP の MPLS VPN サポート」 (P.16) <p>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。</p>
HSRP バージョン 2	Cisco IOS XE 3.1.0SG 12.3(4)T 12.2(25)S 15.0(1)S	<p>HSRP バージョン 2 機能は、今後の機能拡張に備え、HSRP バージョン 1 よりも機能を拡張するために導入されました。HSRP バージョン 2 のパケット形式は、バージョン 1 とは異なります。</p> <p>この機能に関する詳細については、次の各項を参照してください。</p> <ul style="list-style-type: none"> 「HSRP バージョン 2 の設計」 (P.4) 「HSRP バージョン 2 への変更」 (P.45) 「例 : HSRP バージョン 2」 (P.63) <p>show standby、standby ip、standby version の各コマンドがこの機能によって導入または修正されました。</p>
SSO - HSRP	Cisco IOS XE 3.1.0SG 12.2(25)S 12.2(33)SRA 12.2(33)SXH 15.0(1)S	<p>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。</p> <p>この機能に関する詳細については、次の各項を参照してください。</p> <ul style="list-style-type: none"> 「SSO HSRP」 (P.17) 「デュアルルートプロセッサの SSO とシスコ ノンストップ フォワーディング」 (P.17) 「HSRP と SSO の協調動作」 (P.18) 「SSO 対応 HSRP のイネーブル化」 (P.47) 「SSO 対応 HSRP の検証」 (P.48) 「例 : SSO HSRP」 (P.63) <p>debug standby events および standby sso の各コマンドがこの機能によって導入または修正されました。</p>

用語集

ARP : Address Resolution Protocol (ARP; アドレス解決プロトコル)。ARP は IP ルーティングに必要な機能です。ARP は、ホストのハードウェア アドレスをホストの既知の IP アドレスから検出します。このハードウェア アドレスは **Media Access Control (MAC; メディア アクセス制御)** アドレスとも呼ばれます。ARP が保持するキャッシュ (テーブル) では、MAC アドレスが IP アドレスにマッピングされています。ARP は IP が動作しているすべての Cisco IOS システムの一部です。

BFD : Bidirectional Forwarding Detection (双方向フォワーディング検出)。これは、カプセル化、トポロジ、ルーティング プロトコルの転送パスの障害を高速に検出するように設定された検出プロトコルです。また、転送パス障害を高速で検出するだけでなく、一貫した障害検出方式をネットワーク管理者が使用できるようにします。

HSRP : Hot Standby Router Protocol (ホットスタンバイ ルータ プロトコル)。これによって、ネットワークの可用性が高まるほか、透過的にネットワーク トポロジを変更できます。HSRP は、HSRP アドレスに送信されるすべてのパケットを処理するメイン ルータのあるルータ グループを作成します。メイン ルータは、グループの他のルータによってモニタされます。メイン ルータに障害が発生すると、これらのスタンバイ HSRP ルータのいずれかが、メイン ルータとしての地位と HSRP グループ アドレスを継承します。

ISSU : In Service Software Upgrade (インサービス ソフトウェア アップグレード)。パケット転送の実行中に Cisco IOS ソフトウェアの更新や変更を可能にするプロセス。ほとんどのネットワークでは、予定されているソフトウェア アップグレードがダウンタイムの大きな原因になっています。ISSU を使用すると、パケット転送を続行しながら Cisco IOS ソフトウェアを修正できるので、ネットワークの可用性が向上し、予定されているソフトウェア アップグレードによるダウンタイムを短縮することができます。

NSF : Nonstop Forwarding (ノンストップ フォワーディング)。機能停止状態からの回復処理を行っているルータに対してトラフィックの転送を継続するルータの機能。また、障害からの回復中であるルータは、自身に送信されたトラフィックをピアによって正しく転送することができます。

RF : Redundancy Facility (冗長ファシリティ)。ステートがアクティブおよびスタンバイであるクライアントに進捗およびイベントを通知するのに使用される、構造化された機能インターフェイスです。

RP : Route Processor (ルート プロセッサ)。シャーシの中央制御装置の総称です。一般に、プラットフォーム固有の用語が使用されます (Cisco 7500 では RSP、Cisco 10000 では PRE、Cisco 7600 では SUP+MSFC など)。

RPR : Route Processor Redundancy (ルート プロセッサ冗長性)。RPR は、High System Availability (HSA) 機能に代替方法を提供します。HSA を使用すると、システムはアクティブ RP が機能を停止したときにスタンバイ RP をリセットして使用できます。RPR を活用すると、アクティブ RP に致命的なエラーが発生したときにアクティブ RP とスタンバイ RP の間で迅速なスイッチオーバーが行われるため、不測のダウンタイムを減らすことができます。

RPR+ : RPR の拡張。スタンバイ RP が完全に初期化されます。

SSO : Stateful Switchover (ステートフル スイッチオーバー)。SSO とは、アプリケーションや機能が、定義されているステートをアクティブ RP とスタンバイ RP との間で維持できる Cisco IOS ソフトウェアの実装を指しています。スイッチオーバーが発生しても、転送処理とセッションが維持されます。NSF と SSO を組み合わせると、RP に障害が発生してもネットワークに影響がおよぶことはありません。

アクティブ RP : アクティブ RP は、システムの制御やネットワーク サービスの提供を行うほか、ルーティング プロトコルを実行したり、システム管理インターフェイスを表示したりします。

アクティブ ルータ : 仮想ルータにパケットを現在転送している HSRP グループのプライマリ ルータ。

クライアント グループ : サブインターフェイスに作成され、グループ名でマスター グループにリンクされる HSRP グループ。

スイッチオーバー：システム制御とルーティング プロトコルの実行がアクティブ RP からスタンバイ RP に移行するイベント。スイッチオーバーは、手動操作によって、またはハードウェア/ソフトウェアの機能停止によって発生します。スイッチオーバーには、個々のユニットのシステム制御とパケット転送を組み合わせるシステムでのパケット転送機能の移行が含まれることがあります。

スタンバイ RP：バックアップ RP。

スタンバイ グループ：HSRP に参加しているルータのうち、共同で仮想ルータをエミュレートする一連のルータ。

スタンバイ ルータ：HSRP グループのバックアップ ルータ。

仮想 IP アドレス：HSRP グループに設定されるデフォルト ゲートウェイの IP アドレス。

仮想 MAC アドレス：イーサネットおよび FDDI で、HSRP が設定されるときに自動的に生成される MAC アドレス。使用される標準の仮想 MAC アドレスは、0000.0C07.ACxy です。この xy は 16 進数のグループ番号です。機能アドレスはトークン リングに使用されます。HSRP バージョン 2 では、仮想 MAC アドレスが異なります。

マスター グループ：アクティブ ルータとスタンバイ ルータを選出するために物理インターフェイスに必要な HSRP グループ。

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

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

© 2005–2010 Cisco Systems, Inc.
All rights reserved.

Copyright © 2005–2011, シスコシステムズ合同会社.
All rights reserved.

