



IPv6 でのファーストホップ冗長プロトコルの設定

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

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) FHRP は、障害が発生したルータまたは回線からデータ トラフィックを保護し、冗長ルータ間でパケットのロード シェアリングを実行できるようにします。Hot Standby Router Protocol (HSRP; ホットスタンバイ ルータ プロトコル) は、ゲートウェイで障害が発生した場合にデータ トラフィックを保護します。

機能情報の確認

ご使用のソフトウェア リリースによっては、この章に記載されている機能の中に、一部サポートされていないものがあります。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。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、「IPv6 における First Hop Redundancy Protocol の機能情報」(P.30) を参照してください。

Cisco Feature Navigator を使用すると、プラットフォーム、および Cisco ソフトウェア イメージの各サポート情報を検索できます。Cisco Feature Navigator には、<http://www.cisco.com/go/cfn> からアクセスしてください。Cisco.com のアカウントは必要ありません。

目次

- 「機能情報の確認」(P.1)
- 「IPv6 における First Hop Redundancy Protocol の前提条件」(P.2)
- 「IPv6 における First Hop Redundancy Protocol に関する情報」(P.2)
- 「IPv6 における First Hop Redundancy Protocol の設定方法」(P.8)
- 「IPv6 における First Hop Redundancy Protocol の設定例」(P.24)
- 「その他の関連資料」(P.28)

- 「IPv6 における First Hop Redundancy Protocol の機能情報」 (P.30)
- 「用語集」 (P.32)

IPv6 における First Hop Redundancy Protocol の前提条件

- GLBP を設定する前に、ルータが物理インターフェイス上の複数の MAC アドレスをサポートできることを確認してください。設定される GLBP フォワーダごとに、追加の MAC アドレスが使用されます。
- GLBP が設定されたインターフェイスでは、スタティック リンクローカル アドレッシングを使用しないでください。
- HSRP IPv6 を設定する前に、インターフェイスに対して HSRP バージョン 2 をイネーブルにする必要があります。

IPv6 における First Hop Redundancy Protocol に関する情報

- 「GLBP for IPv6」 (P.2)
- 「HSRP for IPv6」 (P.6)

GLBP for IPv6

- 「GLBP for IPv6 の概要」 (P.2)
- 「GLBP の利点」 (P.3)
- 「GLBP アクティブ仮想ゲートウェイ」 (P.3)
- 「GLBP 仮想 MAC アドレスの割り当て」 (P.4)
- 「GLBP 仮想ゲートウェイの冗長性」 (P.5)
- 「GLBP 仮想フォワーダの冗長性」 (P.5)
- 「GLBP ゲートウェイのプライオリティ」 (P.5)
- 「GLBP ゲートウェイの重み付けとトラッキング」 (P.6)

GLBP for IPv6 の概要

ゲートウェイ ロード バランシング プロトコル機能は、IEEE 802.3 LAN 上の 1 つのデフォルト ゲートウェイが設定された IPv6 ホストに対して自動ルータ バックアップを提供します。LAN 上にある複数のファーストホップ ルータの組み合わせによって、1 つの仮想ファーストホップ IPv6 ルータが提供され、IPv6 パケット転送のロード シェアリングが実行されます。GLBP では、HSRP と同様のユーザ用機能を実行します。HSRP では、仮想 IPv6 アドレスが設定された仮想ルータ グループに複数のルータが参加できます。1 つのメンバがアクティブ ルータとして選択され、グループの仮想 IPv6 アドレスに送信されたパケットを転送します。グループ内の他のルータは、アクティブ ルータで障害が発生するまでは冗長ルータです。これらのスタンバイ ルータには、プロトコルによって使用されていない未使用帯域幅があります。同じルータ セットに対して複数の仮想ルータ グループを設定できますが、ホストは異なるデフォルト ゲートウェイに対して設定する必要があります。その結果、管理上の負担が大きく

なります。GLBP の利点は、1 つの仮想 IPv6 アドレスと複数の仮想 MAC アドレスを使用して、複数のルータ（ゲートウェイ）に対するロード バランシングが可能なことです。転送負荷は、GLBP グループ内のすべてのルータ間に分散されるため、単一のルータだけが処理して残りのルータがアイドルのままになるようなことはありません。各ホストに同じ仮想 IPv6 アドレスが設定され、仮想ルータグループ内のすべてのルータがパケットの転送に関与します。

GLBP の利点

GLBP for IPv6 には、次の利点があります。

ロード シェアリング

LAN クライアントからのトラフィックを複数のルータに公平に分散するように GLBP を設定できます。

複数の仮想ルータ

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

プリエンブション

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

認証

業界標準の Message Digest Algorithm 5（MD5）アルゴリズムを使用して、信頼性、セキュリティ、および GLBP スプリーディング ソフトウェアからの保護を向上させることもできます。GLBP グループ内のルータの認証文字列が他のルータとは異なる場合、そのルータは他のグループ メンバによって無視されます。GLBP グループ メンバ間で簡単なテキスト パスワード認証方式を使用して、設定エラーを検出することもできます。

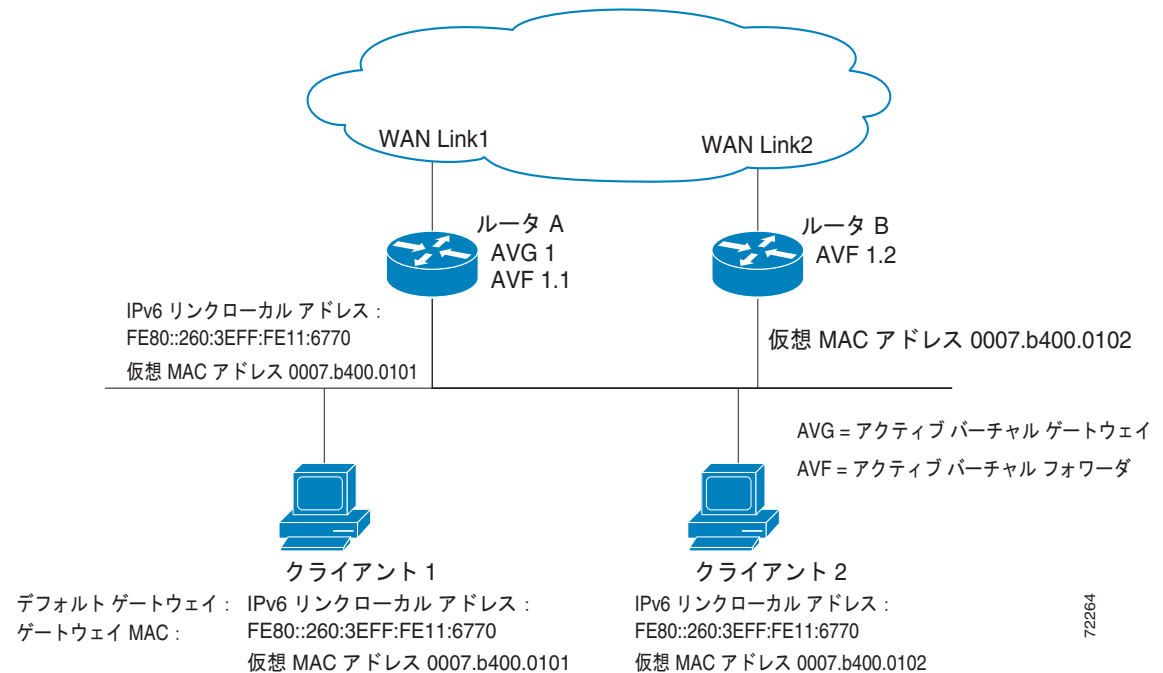
GLBP アクティブ仮想ゲートウェイ

GLBP グループのメンバは、1 つのゲートウェイをそのグループの Active Virtual Gateway（AVG; アクティブ仮想ゲートウェイ）として選択します。他のグループ メンバは、AVG が使用できなくなった場合のバックアップとなります。AVG の機能は、仮想 MAC アドレスを GLBP グループの各メンバに割り当てることです。各ゲートウェイは、AVG によって割り当てられている仮想 MAC アドレスに送信されたパケットを転送する役割を引き継ぎます。これらのゲートウェイは、仮想 MAC アドレスの Active Virtual Forwarder（AVF; アクティブ仮想フォワーダ）と呼ばれます。

IPv6 ネイバー探索プロセスでは、IPv6 メッセージおよび請求ノード マルチキャスト アドレスで Internet Control Message Protocol（ICMP; インターネット制御メッセージプロトコル）を使用して、同じネットワーク（ローカルリンク）上のネイバーのリンクレイヤアドレスを判断し、ネイバーに到達可能かどうかを確認し、ネイバー ルータを追跡します。IPv6 ネイバー探索プロセスでは、ICMPv6 メッセージおよび請求ノード マルチキャスト アドレスを使用して、同じネットワーク（ローカルリンク）上のネイバーのリンクレイヤアドレスを判断し、ネイバーに到達可能かどうかを確認し、ネイバー ルータを追跡します。AVG は、仮想 IPv6 アドレスに対する ICMPv6 ネイバー探索要求に回答します。ロード シェアリングは、AVG が異なる仮想 MAC アドレスで ICMPv6 ネイバー探索要求に回答することによって行われます。

図 1 では、ルータ A が GLBP グループの AVG であり、IPv6 リンクローカルアドレス FE80::260:3EFF:FE11:6770 を担当します。ルータ A は、仮想 MAC アドレス 0007.b400.0101 の AVF でもあります。ルータ B は同じ GLBP グループのメンバであり、仮想 MAC アドレス 0007.b400.0102 の AVF として指定されています。クライアント 1 には、デフォルトゲートウェイ IPv6 アドレス FE80::260:3EFF:FE11:6770 とゲートウェイ MAC アドレス 0007.b400.0101 が設定されています。クライアント 2 は、同じデフォルトゲートウェイ IP アドレスを共有しますが、ルータ B がルータ A とトラフィック負荷を分担するため、ゲートウェイ MAC アドレス 0007.b400.0102 が与えられます。

図 1 GLBP トポロジ



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

GLBP 仮想 MAC アドレスの割り当て

GLBP グループごとに最大 4 つの仮想 MAC アドレスを設定できます。AVG は、仮想 MAC アドレスをグループの各メンバに割り当てます。他のグループメンバは、hello メッセージを通じて AVG を検出したあとで仮想 MAC アドレスを要求します。ゲートウェイには、シーケンスにおける次の MAC アドレスが割り当てられます。AVG によって仮想 MAC アドレスが割り当てられた仮想フォワーダは、プライマリ仮想フォワーダと呼ばれます。GLBP グループの他のメンバは、hello メッセージから仮想 MAC アドレスを学習します。仮想 MAC アドレスを学習した仮想フォワーダは、セカンダリ仮想フォワーダと呼ばれます。

GLBP 仮想ゲートウェイの冗長性

GLBP では、HSRP と同じ方法で仮想ゲートウェイの冗長性が実現されます。1 つのゲートウェイが AVG として選択され、もう 1 つのゲートウェイがスタンバイ仮想ゲートウェイとして選択されます。残りのゲートウェイはリッスン状態になります。

AVG で障害が発生すると、スタンバイ仮想ゲートウェイが仮想 IPv6 アドレスの役割を引き継ぎます。その後、リッスン状態のゲートウェイから新しいスタンバイ仮想ゲートウェイが選択されます。

GLBP 仮想フォワーダの冗長性

GLBP 仮想フォワーダの冗長性は、AVF による仮想ゲートウェイの冗長性と似ています。AVF で障害が発生すると、リッスン状態のセカンダリ仮想フォワーダの 1 つが仮想 MAC アドレスの役割を引き継ぎます。

新しい AVF は、別のフォワーダ番号のプライマリ仮想フォワーダでもあります。GLBP は、ゲートウェイがアクティブ仮想フォワーダ状態になるとすぐに始動する 2 つのタイマーを使用して、古いフォワーダ番号からホストを移行します。GLBP は hello メッセージを使用してタイマーの現在の状態を通信します。

リダイレクト時間は、AVG がホストを古い仮想フォワーダ MAC アドレスにリダイレクトし続ける時間です。リダイレクト時間が経過すると、仮想フォワーダが、古い仮想フォワーダ MAC アドレスに送信されたパケットを転送し続けても、AVG は、ICMPv6 ND 応答で古い仮想フォワーダ MAC アドレスの使用を停止します。

セカンダリ保留時間は、仮想フォワーダが有効である時間です。セカンダリ保留時間が経過すると、仮想フォワーダは GLBP グループ内のすべてのゲートウェイから削除されます。期限切れになった仮想フォワーダ番号は、AVG による再割り当てが可能になります。

GLBP ゲートウェイのプライオリティ

GLBP ゲートウェイのプライオリティによって、各 GLBP ゲートウェイの役割と AVG で障害が発生した場合の結果が決まります。

また、GLBP ルータがバックアップ仮想ゲートウェイとして機能するかどうか、および現在の AVG で障害が発生した場合に AVG になる順番も決まります。各バックアップ仮想ゲートウェイのプライオリティには、**glbp priority** コマンドを使用して 1 ~ 255 の値を設定できます。

図 1 では、LAN トポロジ内の AVG であるルータ A で障害が発生すると、選択プロセスが実行され、処理を引き継ぐバックアップ仮想ゲートウェイが決定されます。この例では、ルータ B がグループ内の唯一の他のメンバであるため、ルータ B が自動的に新しい AVG になります。同じ GLBP グループ内にプライオリティの高い別のルータが存在していた場合は、そのプライオリティの高いルータが選択されます。両方のルータでプライオリティが同じ場合は、高い方の IPv6 アドレスを持つバックアップ仮想ゲートウェイがアクティブ仮想ゲートウェイとして選択されます。

デフォルトでは、GLBP 仮想ゲートウェイのプリエンプティブ方式はディセーブルになっています。バックアップ仮想ゲートウェイが AVG になるのは、仮想ゲートウェイに割り当てられているプライオリティにかかわらず、現在の AVG で障害が発生した場合だけです。**glbp preempt** コマンドを使用すると、GLBP 仮想ゲートウェイのプリエンプティブ方式をイネーブルにすることができます。プリエンプションを使用すると、バックアップ仮想ゲートウェイに現在の AVG よりも高いプライオリティが割り当てられている場合に、そのバックアップ仮想ゲートウェイを AVG にすることができます。

GLBP ゲートウェイの重み付けとトラッキング

GLBP では、重み付けによって GLBP グループ内の各ルータの転送容量を決定します。GLBP グループ内のルータに割り当てられた重み付けを使用して、そのルータがパケットを転送するかどうか、転送する場合はパケットを転送する LAN 内のホストの比率を決定できます。しきい値を設定すると、重み付けが特定の値を下回ったときに転送をディセーブルにすることができます。重み付けがもう一方のしきい値を上回ると、転送は自動的に再びイネーブルになります。

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

デフォルトでは、GLBP 仮想フォワーダのプリエンプティブ方式はイネーブルになっており、遅延は 30 秒です。現在の AVF の重み付けが下限しきい値を下回り、その状態で 30 秒経過すると、バックアップ仮想フォワーダが AVF になります。GLBP フォワーダのプリエンプティブ方式をディセーブルにするには **no glbp forwarder preempt** コマンドを使用し、遅延を変更するには **glbp forwarder preempt delay minimum** コマンドを使用します。

HSRP for IPv6

- 「[HSRP for IPv6 の概要](#)」 (P.6)
- 「[HSRP IPv6 仮想 MAC アドレスの範囲](#)」 (P.7)
- 「[HSRP IPv6 UDP ポート番号](#)」 (P.7)
- 「[HSRP グローバル IPv6 アドレス](#)」 (P.7)

HSRP for IPv6 の概要

HSRP は、ファーストホップ IP ルータの透過的なフェールオーバーを可能にする FHRP です。デフォルト ゲートウェイの IP アドレスが設定されたイーサネット上の IP ホストにファーストホップのルーティング冗長性を確保することによって、高いネットワーク アベイラビリティを提供します。ルータのグループで HSRP を使用して、アクティブ ルータとスタンバイ ルータを選択します。ルータ インターフェイスのグループ内では、アクティブ ルータはパケットをルーティングするルータです。スタンバイ ルータは、アクティブ ルータで障害が発生した場合、またはプリセットされた条件が満たされた場合に処理を引き継ぐルータです。

IPv6 ホストは、IPv6 ネイバー探索の RA メッセージを通じて使用可能な IPv6 ルータを学習します。これらのメッセージは定期的にマルチキャストされるか、またはホストによって請求されることもあります。HSRP は、IPv6 ホストに仮想ファースト ホップだけを提供するように設計されています。

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

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

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

HSRP IPv6 仮想 MAC アドレスの範囲

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

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

HSRP IPv6 UDP ポート番号

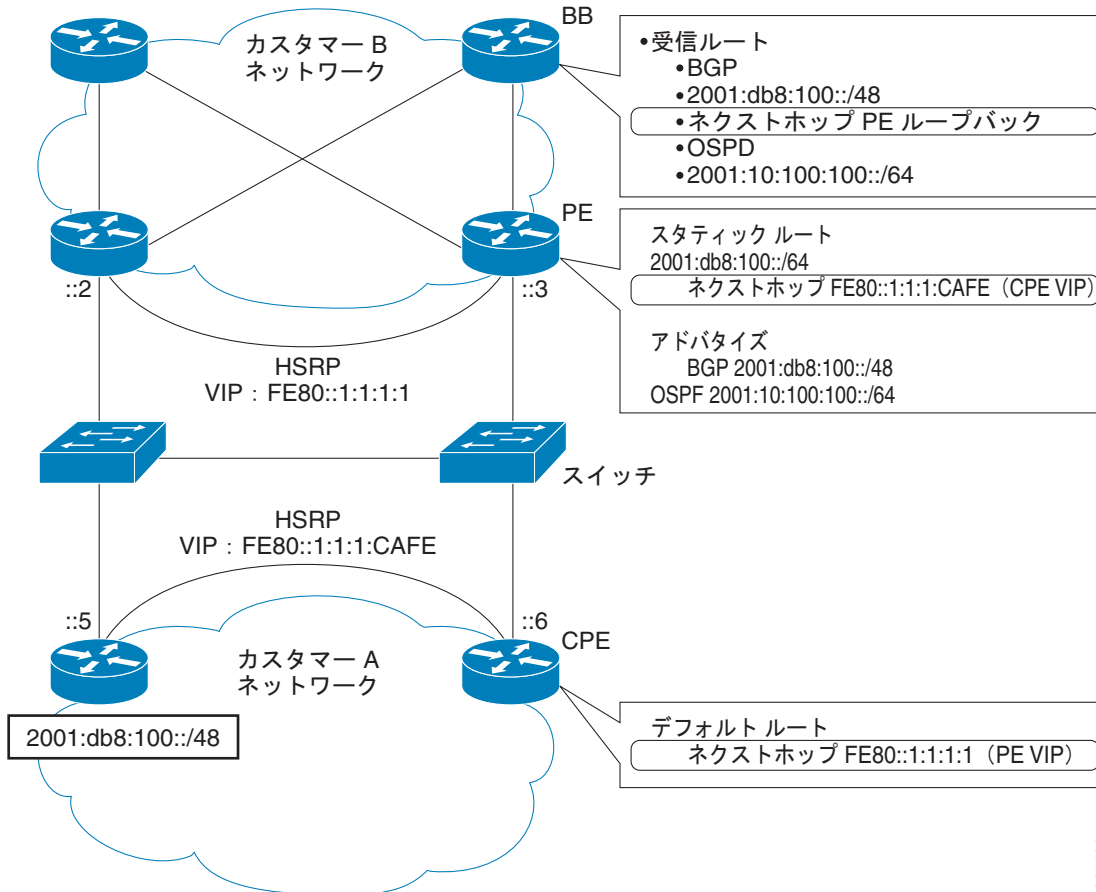
HSRP IPv6 には、ポート番号 2029 が割り当てられています。

HSRP グローバル IPv6 アドレス

HSRP グローバル IPv6 アドレス機能では、ユーザが複数の非リンク ローカル アドレスを仮想アドレスとして設定できます。また、既存のプライマリ リンクローカル アドレスに加えて、複数のグローバル IPv6 仮想アドレスを保管し、管理できます。IPv6 アドレスを使用する場合、そのアドレスに IPv6 プレフィクス長を含める必要があります。リンクローカル アドレスを使用する場合は、プレフィクスを与えてはいけません。

図 2 に、HSRP IPv6 グローバル仮想インターフェイスを使用した展開シナリオを示します。

図 2 Gan HSRP IPv6 グローバル仮想インターフェイスの使用シナリオ



207491

図 2 の場合、Provider Equipment (PE) ルータは、バックボーン ルータから Customer Premises Equipment (CPE; 宅内装置) に到達するためのルートを挿入する必要があります。2 台の CPE が存在するため、HSRP を使用すると便利です。スタティック ルートは、リンクローカル ネクスト ホップ (FE80::1:1:1:CAFE) で設定されます。リンクローカル アドレスはレイヤ 2 ローカル LAN 空間内のスコープしか持たないため、このアドレスがバックボーンに挿入されても、リンクローカル ネクストホップのままではこのルートは役に立ちません。この問題に対処するには、バックボーン ルータがパケットを PE ルータにルーティングできるように、仮想アドレスへのスタティック ルートのネクストホップを非リンクローカル アドレスに設定する必要があります。ネクストホップのアドレス解決時、アクティブ HSRP グループ メンバが、非リンクローカル アドレスへ送信された Neighbor Solicitation (NS; ネイバー請求) メッセージに応答します。

IPv6 における First Hop Redundancy Protocol の設定方法

- 「GLBP の設定とカスタマイズ」 (P.9)
- 「IPv6 用 HSRP グループの動作のイネーブル化」 (P.21)

GLBP の設定とカスタマイズ

GLBP 動作のカスタマイズは任意です。GLBP グループをイネーブルにすると、そのグループはすぐに動作します。GLBP グループをイネーブルにしてから GLBP をカスタマイズすると、機能のカスタマイズを完了する前にルータがグループの制御を引き継ぎ、AVG になる可能性があります。したがって、GLBP をカスタマイズする場合は、GLBP をイネーブルにする前に行うことを推奨します。

ここでは、次の任意の手順について説明します。

- 「GLBP のカスタマイズ」(P.9)
- 「GLBP 認証の設定」(P.11)
- 「GLBP の重み付けの値とオブジェクト トラッキング」(P.17)
- 「GLBP のイネーブル化と確認」(P.18)
- 「GLBP のトラブルシューティング」(P.20)

GLBP のカスタマイズ

手順の概要

1. **enable**
2. **configure terminal**
3. **interface type number**
4. **ipv6 address** {*ipv6-global-address* | *prefix-name ipv6-prefix/prefix-length* | **autoconfig** [*default-route*]}
5. **glbp group timers** [*msec*] *hellotime* [*msec*] *holdtime*
6. **glbp group timers redirect** *redirect timeout*
7. **glbp group load-balancing** [*host-dependent* | **round-robin** | **weighted**]
8. **glbp group priority** *level*
9. **glbp group preempt** [**delay minimum** *seconds*]
10. **glbp group name** *redundancy-name*
11. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ1	enable 例： Router> enable	特権 EXEC モードをイネーブルにします。 • 必要に応じて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。

IPv6 における First Hop Redundancy Protocol の設定方法

	コマンドまたはアクション	目的
ステップ3	<pre>interface type number</pre> <p>例： Router(config)# interface fastethernet 0/0</p>	インターフェイスのタイプおよび番号を指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ4	<pre>ipv6 address {ipv6-address/prefix-length prefix-name ipv6-prefix/prefix-length autoconfig [default-route]}</pre> <p>例： Router(config-if)# ipv6 address 2001:DB8:0:7272::72/64</p>	IPv6 の一般的なプレフィクスに基づいて IPv6 アドレスを設定し、インターフェイスにおける IPv6 処理をイネーブ ルにします。
ステップ5	<pre>glbp group timers [msec] hellotime [msec] holdtime</pre> <p>例： Router(config-if)# glbp 10 timers 5 18</p>	<p>GLBP グループ内の AVG によって連続的に送信される hello パケットの間隔を設定します。</p> <ul style="list-style-type: none"> • <i>holdtime</i> 引数には、hello パケット内の仮想ゲートウェイと仮想フォワーダの情報が無効と見なされるまでの時間を秒数で指定します。 • オプションの msec キーワードは、そのあとに続く引数がデフォルトの秒単位ではなくミリ秒単位であることを指定します。
ステップ6	<pre>glbp group timers redirect redirect timeout</pre> <p>例： Router(config-if)# glbp 10 timers redirect 600 7200</p>	<p>AVG がクライアントを AVF にリダイレクトし続ける時間を設定します。</p> <ul style="list-style-type: none"> • <i>timeout</i> 引数には、セカンダリ仮想フォワーダが無効になるまでの時間を秒数で指定します。
ステップ7	<pre>glbp group load-balancing [host-dependent round-robin weighted]</pre> <p>例： Router(config-if)# glbp 10 load-balancing host-dependent</p>	GLBP AVG で使用するロード バランシングの方式を指定 します。
ステップ8	<pre>glbp group priority level</pre> <p>例： Router(config-if)# glbp 10 priority 254</p>	<p>GLBP グループ内のゲートウェイのプライオリティ レベルを設定します。</p> <ul style="list-style-type: none"> • デフォルト値は 100 です。
ステップ9	<pre>glbp group preempt [delay minimum seconds]</pre> <p>例： Router(config-if)# glbp 10 preempt delay minimum 60</p>	<p>ルータのプライオリティが現在の AVG よりも高い場合に、GLBP グループの AVG として処理を引き継ぐようにルータを設定します。</p> <ul style="list-style-type: none"> • このコマンドは、デフォルトでディセーブルになっています。 • オプションの delay キーワードと minimum キーワードおよび <i>seconds</i> 引数を使用して、AVG のプリエンプションが実行されるまでの最小遅延時間を秒数で指定 します。

	コマンドまたはアクション	目的
ステップ 10	<pre>glbp group name redundancy-name</pre> <p>例： Router(config-if)# glbp 10 name abcompany</p>	<p>GLBP グループに名前を割り当てることによって、IPv6 冗長性をイネーブルにします。</p> <ul style="list-style-type: none"> 冗長クライアントと GLBP グループを接続できるように、GLBP 冗長クライアントに同じ GLBP グループ名を設定する必要があります。
ステップ 11	<pre>exit</pre> <p>例： Router(config-if)# exit</p>	<p>インターフェイス コンフィギュレーション モードを終了し、ルータをグローバル コンフィギュレーション モードに戻します。</p>

GLBP 認証の設定

ここでは、GLBP 認証の設定作業について説明します。実行する作業は、認証に使用するのがテキスト認証であるか、単純な MD5 キー文字列であるか、または MD5 キー チェーンであるかによって異なります。

- 「[キー ストリングを使用した GLBP MD5 認証の設定](#)」(P.11)
- 「[キー チェーンを使用した GLBP MD5 認証の設定](#)」(P.13)
- 「[GLBP テキスト認証の設定](#)」(P.15)

GLBP MD5 認証を使用すると、別のプレーン テキスト認証方式よりもセキュリティを強化できます。MD5 認証では、各 GLBP グループ メンバが秘密キーを使用して、発信パケットに含まれるキー付き MD5 ハッシュを生成できます。着信パケットのキー付きハッシュが生成され、着信パケット内のハッシュが生成されたハッシュに一致しない場合、そのパケットは無視されます。

MD5 ハッシュのキーは、キー ストリングを使用して設定で直接指定するか、またはキー チェーンを使用して間接的に指定できます。

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

- 認証なし
- プレーン テキスト認証
- MD5 認証

GLBP パケットは、次のいずれかの場合に拒否されます。

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

キー ストリングを使用した GLBP MD5 認証の設定

GLBP MD5 認証を設定すると、ルータをスプーフィング ソフトウェアから保護し、業界標準の MD5 アルゴリズムによって信頼性とセキュリティを向上できます。

手順の概要

- enable
- configure terminal
- interface *type number*

IPv6 における First Hop Redundancy Protocol の設定方法

4. **ipv6 address** {*ipv6-address/prefix-length* | *prefix-name ipv6-prefix/prefix-length* | **autoconfig** [*default-route*]}
5. **glbp group-number authentication md5 key-string** [0 | 7] *key*
6. **glbp group ipv6** [*ipv6-address* | **autoconfig**]
7. 通信する各ルータに対してステップ 1 ~ 6 を繰り返します。
8. **end**
9. **show glbp**

手順の詳細

	コマンド	目的
ステップ1	enable 例： Router> enable	特権 EXEC モードをイネーブルにします。 <ul style="list-style-type: none">必要に応じてパスワードを入力します。
ステップ2	configure terminal 例： Router# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ3	interface type number 例： Router(config)# interface Ethernet 0/1	インターフェイス タイプを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ4	ipv6 address { <i>ipv6-address/prefix-length</i> <i>prefix-name ipv6-prefix/prefix-length</i> autoconfig [<i>default-route</i>]}	IPv6 の一般的なプレフィクスに基づいて IPv6 アドレスを設定し、インターフェイスにおける IPv6 処理をイネーブルにします。
ステップ5	glbp group-number authentication md5 key-string [0 7] <i>key</i> 例： Router(config-if)# glbp 1 authentication md5 key-string d00b4r987654321a	GLBP MD5 認証の認証キーを設定します。 <ul style="list-style-type: none">コマンドとキー スtringの文字数が 255 文字を超えないようにします。<i>key</i> 引数の前にキーワードを指定しないか、または 0 を指定した場合、キーは暗号化されません。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場合、key-string 認証キーは自動的に暗号化されます。
ステップ6	glbp group ipv6 [<i>ipv6-address</i> autoconfig] 例： Router(config-if)# glbp 1 ipv6 FE80::260:3EFF:FE11:6770	IPv6 の GLBP をイネーブルにします。
ステップ7	通信する各ルータに対してステップ 1 ~ 6 を繰り返します。	—

	コマンド	目的
ステップ 8	end 例： Router(config-if)# end	特権 EXEC モードに戻ります。
ステップ 9	show glbp 例： Router# show glbp	(任意) GLBP の情報を表示します。 • このコマンドを使用して、設定を確認します。設定されている場合はキー ストリングと認証タイプが表示されます。

キー チェーンを使用した GLBP MD5 認証の設定

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

手順の概要

1. **enable**
2. **configure terminal**
3. **key chain *name-of-chain***
4. **key *key-id***
5. **key-string *string***
6. **exit**
7. **exit**
8. **interface *type number***
9. **ipv6 address {*ipv6-address/prefix-length* | *prefix-name ipv6-prefix/prefix-length* | **autoconfig** [*default-route*]}**
10. **glbp *group-number* authentication md5 key-chain *name-of-chain***
11. **glbp group ipv6 [*ipv6-address* | **autoconfig**]**
12. 通信する各ルータに対してステップ 1 ~ 11 を繰り返します。
13. **end**
14. **show glbp**
15. **show key chain**

IPv6 における First Hop Redundancy Protocol の設定方法

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。 • 必要に応じてパスワードを入力します。
ステップ2	configure terminal 例： Router# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ3	key chain name-of-chain 例： Router(config)# key chain glbp2	ルーティング プロトコルの認証をイネーブルにし、認証キーのグループを識別します。
ステップ4	key key-id 例： Router(config-keychain)# key 100	キー チェーンの認証キーを識別します。 • <i>key-id</i> は数字である必要があります。
ステップ5	key-string string 例： Router(config-keychain-key)# key-string string1	キーの認証文字列を指定します。 • <i>string</i> は、1 ~ 80 文字の大文字または小文字の英数字である必要があります。最初の文字には数字を使用できません。
ステップ6	exit 例： Router(config-keychain-key)# exit	キーチェーン コンフィギュレーション モードに戻ります。
ステップ7	exit 例： Router(config-keychain)# exit	グローバル コンフィギュレーション モードに戻ります。
ステップ8	interface type number 例： Router(config)# interface Ethernet 0/1	インターフェイス タイプを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ9	ipv6 address {ipv6-address/prefix-length prefix-name ipv6-prefix/prefix-length autoconfig [default-route]} 例： Router(config-if)# ipv6 address 2001:DB8:0:7272::72/64	IPv6 の一般的なプレフィクスに基づいて IPv6 アドレスを設定し、インターフェイスにおける IPv6 処理をイネーブルにします。
ステップ10	glbp group-number authentication md5 key-chain name-of-chain 例： Router(config-if)# glbp 1 authentication md5 key-chain glbp2	GLBP MD5 認証の認証 MD5 キー チェーンを設定します。 • キー チェーン名は、ステップ 3 で指定した名前に一致する必要があります。

	コマンド	目的
ステップ 11	<code>glbp group ipv6 [ipv6-address autoconfig]</code> 例： Router(config-if)# glbp 1 ipv6 FE80::E0:F727:E400:A	IPv6 の GLBP をイネーブルにします。
ステップ 12	通信する各ルータに対してステップ 1 ~ 11 を繰り返します。	—
ステップ 13	<code>end</code> 例： Router(config-if)# end	特権 EXEC モードに戻ります。
ステップ 14	<code>show glbp</code> 例： Router# show glbp	(任意) GLBP の情報を表示します。 • このコマンドを使用して、設定を確認します。 設定されている場合はキーチェーンと認証タイプが表示されます。
ステップ 15	<code>show key chain</code> 例： Router# show key chain	(任意) 認証キー情報を表示します。

GLBP テキスト認証の設定

この認証方式では、最小限のセキュリティが確保されます。セキュリティが必須の場合は、MD5 認証を使用してください。

手順の概要

1. `enable`
2. `configure terminal`
3. `interface type number`
4. `ipv6 address {ipv6-address/prefix-length | prefix-name ipv6-prefix/prefix-length | autoconfig [default-route]}`
5. `glbp group-number authentication text string`
6. `glbp group ipv6 [ipv6-address | autoconfig]`
7. 通信する各ルータに対してステップ 1 ~ 6 を繰り返します。
8. `end`
9. `show glbp`

IPv6 における First Hop Redundancy Protocol の設定方法

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。 • 必要に応じてパスワードを入力します。
ステップ2	configure terminal 例： Router# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ3	interface type number 例： Router(config)# interface Ethernet 0/1	インターフェイス タイプを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ4	ipv6 address {ipv6-address/prefix-length prefix-name ipv6-prefix/prefix-length autoconfig [default-route]} 例： Router(config-if)# ipv6 address 2001:DB8:0:7272::72/64	IPv6 の一般的なプレフィクスに基づいて IPv6 アドレスを設定し、インターフェイスにおける IPv6 処理をイネーブルにします。
ステップ5	glbp group-number authentication text string 例： Router(config-if)# glbp 10 authentication text stringxyz	グループ内の他のルータから受信した GLBP パケットを認証します。 • 認証を設定する場合は、GLBP グループ内のすべてのルータで同じ認証文字列を使用する必要があります。
ステップ6	glbp group ipv6 [ipv6-address autoconfig] 例： Router(config-if)# glbp 1 ipv6 FE80::60:3E47:AC8:8	IPv6 の GLBP をイネーブルにします。
ステップ7	通信する各ルータに対してステップ 1 ~ 6 を繰り返します。	—
ステップ8	end 例： Router(config-if)# end	特権 EXEC モードに戻ります。
ステップ9	show glbp 例： Router# show glbp	(任意) GLBP の情報を表示します。 • このコマンドを使用して、設定を確認します。

GLBP の重み付けの値とオブジェクト トラッキング

GLBP の重み付けは、ルータを仮想フォワーダとして動作できるようにするかどうかを決定するために使用します。重み付けの初期値を設定したり、オプションのしきい値を指定したりできます。インターフェイスの状態を追跡し、インターフェイスがダウンした場合に重み付けの値を減らすための減少値を設定できます。GLBP ルータの重み付けが指定した値を下回ると、ルータはアクティブ仮想フォワーダではなくなります。重み付けが指定した値を上回ると、ルータはアクティブ仮想フォワーダとしての役割を再開できます。

手順の概要

1. `enable`
2. `configure terminal`
3. `track object-number interface type number {line-protocol | ip routing}`
4. `interface type number`
5. `glbp group weighting maximum [lower lower] [upper upper]`
6. `glbp group weighting track object-number [decrement value]`
7. `glbp group forwarder preempt [delay minimum seconds]`
8. `end`
9. `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	<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"> • 必要に応じて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>track object-number interface type number {line-protocol ip routing}</code> 例： Router(config)# track 2 interface POS 6/0 ip routing	GLBP ゲートウェイの重み付けに影響する状態変化を追跡するインターフェイスを設定し、トラッキング コンフィギュレーション モードを開始します。 <ul style="list-style-type: none"> • このコマンドでは、インターフェイス、および glbp weighting track コマンドで使用する、そのインターフェイスに対応するオブジェクト番号を設定します。 • line-protocol キーワードを指定すると、インターフェイスがアップ状態かどうかを追跡されます。ip routing キーワードを指定すると、インターフェイスで IPv6 ルーティングがイネーブルになっているかどうか、および IPv6 アドレスが設定されているかどうかをチェックされます。

IPv6 における First Hop Redundancy Protocol の設定方法

	コマンドまたはアクション	目的
ステップ4	<code>interface type number</code> 例： Router(config)# interface fastethernet 0/0	インターフェイス コンフィギュレーション モードを開始します。
ステップ5	<code>glbp group weighting maximum [lower lower] [upper upper]</code> 例： Router(config-if)# glbp 10 weighting 110 lower 95 upper 105	GLBP ゲートウェイの重み付けの初期値、上限しきい値、および下限しきい値を指定します。
ステップ6	<code>glbp group weighting track object-number [decrement value]</code> 例： Router(config-if)# glbp 10 weighting track 2 decrement 5	GLBP ゲートウェイの重み付けに影響する、追跡対象のオブジェクトを指定します。 <ul style="list-style-type: none"> <code>value</code> 引数には、追跡対象のオブジェクトで障害が発生した場合に GLBP ゲートウェイの重み付けを減らす量を指定します。
ステップ7	<code>glbp group forwarder preempt [delay minimum seconds]</code> 例： Router(config-if)# glbp 10 forwarder preempt delay minimum 60	GLBP グループの現在の AVF で重み付けがしきい値を下回った場合に、ルータが GLBP グループの AVF の役割を引き継ぐように設定します。 <ul style="list-style-type: none"> このコマンドは、デフォルトでイネーブルになっており、遅延は 30 秒です。 オプションの <code>delay</code> キーワードと <code>minimum</code> キーワードおよび <code>seconds</code> 引数を使用して、AVF のプリエンプションが実行されるまでの最小遅延時間を秒数で指定します。
ステップ8	<code>end</code> 例： Router(config-if)# exit	特権 EXEC モードに戻ります。
ステップ9	<code>show track [object-number brief] [interface [brief] ip route [brief] resolution timers]</code> 例： Router# show track 2	トラッキング情報を表示します。

GLBP のイネーブル化と確認

GLBP は、簡単に設定できる設計になっています。GLBP グループ内の各ゲートウェイには同じグループ番号を設定し、GLBP グループ内の少なくとも 1 つのゲートウェイにグループで使用する仮想 IPv6 アドレスを設定する必要があります。その他のすべての必須パラメータは学習できます。

前提条件

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

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ipv6 address** {*ipv6-address/prefix-length* | *prefix-name ipv6-prefix/prefix-length* | **autoconfig** [*default-route*]}
5. **glbp group ipv6** [*ipv6-address* | **autoconfig**]
6. **exit**
7. **show glbp** [*interface-type interface-number*] [*group*] [*state*] [**brief**]

手順の詳細

	コマンドまたはアクション	目的
ステップ1	enable 例： Router> enable	特権 EXEC モードをイネーブルにします。 • 必要に応じて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 fastethernet 0/0	インターフェイスのタイプおよび番号を指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ4	ipv6 address { <i>ipv6-address/prefix-length</i> <i>prefix-name ipv6-prefix/prefix-length</i> autoconfig [<i>default-route</i>]} 例： Router(config-if)# ipv6 address 2001:DB8:0:7262::62/64	IPv6 の一般的なプレフィクスに基づいて IPv6 アドレスを設定し、インターフェイスにおける IPv6 処理をイネーブルにします。
ステップ5	glbp group ipv6 [<i>ipv6-address</i> autoconfig] 例： Router(config-if)# glbp 1 ipv6 FE80::60:3E47:AC8:8	IPv6 の GLBP をイネーブルにします。

IPv6 における First Hop Redundancy Protocol の設定方法

	コマンドまたはアクション	目的
ステップ6	<code>exit</code> 例： Router(config-if)# exit	インターフェイス コンフィギュレーション モードを終了し、ルータをグローバル コンフィギュレーション モードに戻します。
ステップ7	<code>show glbp [interface-type interface-number] [group] [state] [brief]</code> 例： Router(config)# show glbp 10	(任意) ルータ上の GLBP グループに関する情報を表示します。 • オプションの brief キーワードを使用すると、各仮想ゲートウェイまたは仮想フォワーダに関する情報が 1 行表示されます。

GLBP のトラブルシューティング

前提条件

この作業では、コンソールに直接接続された GLBP を実行しているルータが必要です。

手順の概要

1. **enable**
2. **configure terminal**
3. **no logging console**
4. Telnet を使用してルータ ポートにアクセスし、ステップ 1 と 2 を繰り返します。
5. **end**
6. **terminal monitor**
7. **debug condition glbp interface-type interface-number group [forwarder]**
8. **terminal no monitor**

手順の詳細

	コマンドまたはアクション	目的
ステップ1	<code>enable</code> 例： Router> enable	特権 EXEC モードをイネーブルにします。 • 必要に応じて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>no logging console</code> 例： Router(config)# no logging console	コンソール端末へのすべてのロギングをディセーブルにします。 • コンソールへのロギングを再度イネーブルにするには、グローバル コンフィギュレーション モードで logging console コマンドを使用します。

	コマンドまたはアクション	目的
ステップ4	Telnet を使用してルータ ポートにアクセスし、ステップ 1 と 2 を繰り返します。	再帰 Telnet セッションでグローバル コンフィギュレーション モードを開始します。これにより、出力をコンソールポートからリダイレクトできます。
ステップ5	<code>end</code> 例： Router(config)# end	終了して、特権 EXEC モードに戻ります。
ステップ6	<code>terminal monitor</code> 例： Router# terminal monitor	仮想端末でのロギング出力をイネーブルにします。
ステップ7	<code>debug condition glbp interface-type interface-number group [forwarder]</code> 例： Router# debug condition glbp fastethernet 0/0 10 1	GLBP 状態に関するデバッグ メッセージを表示します。 <ul style="list-style-type: none"> 特定の <code>debug condition glbp</code> または <code>debug glbp</code> コマンドだけを入力して、出力を特定のサブコンポーネントに分離し、プロセッサの負荷を最小限に抑えます。適切な引数とキーワードを使用して、指定したサブコンポーネント上に詳細なデバッグ情報を生成します。 終了したら、特定の <code>no debug condition glbp</code> または <code>no debug glbp</code> コマンドを入力します。
ステップ8	<code>terminal no monitor</code> 例： Router# terminal no monitor	仮想端末でのロギングをディセーブルにします。

IPv6 用 HSRP グループの動作のイネーブル化

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

- 「[HSRP バージョン 2 のイネーブル化](#)」(P.21)
- 「[IPv6 用 HSRP グループの動作のイネーブル化と確認](#)」(P.22)

HSRP バージョン 2 のイネーブル化

手順の概要

1. `enable`
2. `configure terminal`
3. `interface type number`
4. `standby version {1 | 2}`

手順の詳細

	コマンドまたはアクション	目的
ステップ1	<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">必要に応じて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 0/0	インターフェイスのタイプと番号を指定し、ルータをインターフェイス コンフィギュレーション モードにします。
ステップ4	<code>standby version {1 2}</code> 例： Router(config-if)# standby version 2	HSRP のバージョンを変更します。 <ul style="list-style-type: none">デフォルトはバージョン 1 です。

IPv6 用 HSRP グループの動作のイネーブル化と確認

この作業では、`standby ipv6` コマンドを入力すると、変更された EUI-64 形式のインターフェイス ID が生成されます。このインターフェイス ID は、関連する HSRP 仮想 MAC アドレスに基づいて作成されます。

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

リンク上のノードは、RA メッセージに含まれるプレフィクス (64 ビット) にそのインターフェイス ID (64 ビット) を付加して、自動的にサイトローカル アドレスとグローバル IPv6 アドレスを設定できます。ノードによって設定された 128 ビットの IPv6 アドレスは、重複アドレス検出の対象となり、リンク上での一意性が確保されます。RA メッセージでアドバタイズされたプレフィクスがグローバルに一意である場合、ノードによって設定された IPv6 アドレスもグローバルに一意になります。ICMPv6 パケット ヘッダーのタイプ フィールドの値が 133 であるルータ送信要求メッセージは、システム始動時にホストによって送信されるため、ホストは次のスケジュールされた RA メッセージを待機することなくすぐに自動設定できます。

手順の概要

1. `enable`
2. `configure terminal`
3. `ipv6 unicast-routing`
4. `interface type number`
5. `standby [group-number] ipv6 {ipv6-global-address | ipv6-address/prefix-length | ipv6-prefix/prefix-length | link-local-address | autoconfig}`
6. `standby [group-number] preempt [delay {minimum seconds | reload seconds | sync seconds}]`

7. `standby [group-number] priority priority`
8. `exit`
9. `show standby [type number [group]] [all | brief]`
10. `show ipv6 interface [brief] [interface-type interface-number] [prefix]`

手順の詳細

	コマンドまたはアクション	目的
ステップ1	<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"> 必要に応じて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>ipv6 unicast-routing</code> 例： Router(config)# ipv6 unicast-routing	IPv6 ユニキャスト データグラムの転送をイネーブルにします。 <ul style="list-style-type: none"> HSRP for IPv6 を機能させるには、ipv6 unicast-routing コマンドをイネーブルにする必要があります。
ステップ4	<code>interface type number</code> 例： Router(config)# interface ethernet 0/0	インターフェイスのタイプと番号を指定し、ルータをインターフェイス コンフィギュレーション モードにします。
ステップ5	<code>standby [group-number] ipv6 {ipv6-global-address ipv6-address/prefix-length ipv6-prefix/prefix-length link-local-address autoconfig}</code> 例： Router(config-if)# standby 1 ipv6 autoconfig	IPv6 の HSRP をアクティブにします。 IPv6 アドレスを使用する場合、そのアドレスに IPv6 プレフィクス長を含める必要があります。リンクローカルアドレスを使用する場合は、プレフィクスを与えてはいけません。
ステップ6	<code>standby [group-number] preempt [delay {minimum seconds reload seconds sync seconds}]</code> 例： Router(config-if)# standby 1 preempt	HSRP プリエンプションとプリエンブション遅延を設定します。
ステップ7	<code>standby [group-number] priority priority</code> 例： Router(config-if)# standby 1 priority 110	HSRP プライオリティを設定します。
ステップ8	<code>exit</code> 例： Router(config-if)# exit	ルータを特権 EXEC モードに戻します。

■ IPv6 における First Hop Redundancy Protocol の設定例

	コマンドまたはアクション	目的
ステップ9	show standby [<i>type number</i> [<i>group</i>]] [all brief] 例 : Router# show standby	HSRP 情報を表示します。
ステップ10	show ipv6 interface [brief] [<i>interface-type interface-number</i>] [prefix] 例 : Router# show ipv6 interface ethernet 0/0	IPv6 用に設定されたインターフェイスが使用可能かどうかのステータスを表示します。

IPv6 における First Hop Redundancy Protocol の設定例

- 「例：GLBP 設定のカスタマイズ」(P.24)
- 「例：キー ストリングを使用した GLBP MD5 認証」(P.24)
- 「例：キー チェーンを使用した GLBP MD5 認証」(P.25)
- 「例：GLBP テキスト認証」(P.25)
- 「例：GLBP の重み付け」(P.25)
- 「例：GLBP 設定のイネーブル化」(P.25)
- 「例：IPv6 用 HSRP グループの動作のイネーブル化と確認」(P.26)

例：GLBP 設定のカスタマイズ

次の例では、図 1 で示したルータ A に複数の GLBP コマンドが設定されています。

```
interface fastethernet 0/0
ipv6 address 2001:DB8:0001:0001:/64
glbp 10 timers 5 18
glbp 10 timers redirect 600 7200
glbp 10 load-balancing host-dependent
glbp 10 priority 254
glbp 10 preempt delay minimum 60
```

例：キー ストリングを使用した GLBP MD5 認証

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

```
!
interface Ethernet 0/1
ipv6 address 2001:DB8:0001:0001:/64
glbp 2 authentication md5 key-string ThisStringIsTheSecretKey
glbp 2 ipv6 FE80::260:3EFF:FE11:6770
```


例：キーチェーンを使用した GLBP MD5 認証

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

```
key chain AuthenticateGLBP
  key 1
    key-string ThisIsASecretKey
interface Ethernet 0/1
  ipv6 address 2001:DB8:0001:0001:/64
  glbp 2 authentication md5 key-chain AuthenticateGLBP
  glbp 2 ipv6 FE80::E0:F727:E400:A
```

例：GLBP テキスト認証

次に、テキスト文字列を使用した GLBP テキスト認証を設定する例を示します。

```
interface fastethernet 0/0
  ipv6 address 2001:DB8:0001:0001:/64
  glbp 10 authentication text stringxyz
  glbp 10 ipv6 FE80::60:3E47:AC8:8
```

例：GLBP の重み付け

次に、図 1 で示したルータ A を POS インターフェイス 5/0 と 6/0 の IP ルーティング状態を追跡するように設定し、GLBP の重み付けの初期値、上限しきい値、下限しきい値、および重み付けの減少値 10 を設定する例を示します。POS インターフェイス 5/0 と 6/0 がダウンすると、ルータの重み付けの値が小さくなります。

```
track 1 interface POS 5/0 ip routing
track 2 interface POS 6/0 ip routing
interface fastethernet 0/0
  glbp 10 weighting 110 lower 95 upper 105
  glbp 10 weighting track 1 decrement 10
  glbp 10 weighting track 2 decrement 10
  glbp 10 forwarder preempt delay minimum 60
```

例：GLBP 設定のイネーブル化

次の例では、ルータは GLBP をイネーブルにするよう設定され、GLBP グループ 10 に仮想 IPv6 アドレス 2001:DB8:0002:0002:/64 が指定されます。

```
interface fastethernet 0/0
  ipv6 address 2001:DB8:0001:0001:/64
  glbp 10 ipv6 FE80::60:3E47:AC8:8
```

次に、GLBP グループ 15 に対して GLBP for IPv6 をイネーブルにする例を示します。

```
interface fastethernet 0/0
  ipv6 address 2001:DB8:0001:0001:/64
  glbp 10 ipv6
```

例：IPv6 用 HSRP グループの動作のイネーブル化と確認

ここでは、次の例を示します。

- 「例：HSRP グループの設定と確認」(P.26)
- 「例：HSRP グローバル IPv6 アドレスの設定」(P.27)

例：HSRP グループの設定と確認

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

ルータ 1 設定

```
interface FastEthernet0/0.100
description DATA VLAN for PCs
encapsulation dot1Q 100
ipv6 address 2001:DB8:CAFE:2100::BAD1:1010/64
standby version 2
standby 101 priority 120
standby 101 preempt delay minimum 30
standby 101 authentication ese
standby 101 track Serial0/1/0.17 90
standby 201 ipv6 autoconfig
standby 201 priority 120
standby 201 preempt delay minimum 30
standby 201 authentication ese
standby 201 track Serial0/1/0.17 90

Router1# show standby

FastEthernet0/0.100 - Group 101 (version 2)
State is Active
2 state changes, last state change 5w5d
Active virtual MAC address is 0000.0c9f.f065
Local virtual MAC address is 0000.0c9f.f065 (v2 default)
Hello time 3 sec, hold time 10 sec
Next hello sent in 2.296 secs
Authentication text "ese"
Preemption enabled, delay min 30 secs
Active router is local
Priority 120 (configured 120)
Track interface Serial0/1/0.17 state Up decrement 90
IP redundancy name is "hsrp-Fa0/0.100-101" (default)
FastEthernet0/0.100 - Group 201 (version 2)
State is Active
2 state changes, last state change 5w5d
Virtual IP address is FE80::5:73FF:FEA0:C9
Active virtual MAC address is 0005.73a0.00c9
Local virtual MAC address is 0005.73a0.00c9 (v2 IPv6 default)
Hello time 3 sec, hold time 10 sec
Next hello sent in 2.428 secs
Authentication text "ese"
Preemption enabled, delay min 30 secs
Active router is local
Standby router is FE80::20F:8FFF:FE37:3B70, priority 100 (expires in 7.856 sec)
Priority 120 (configured 120)
Track interface Serial0/1/0.17 state Up decrement 90
IP redundancy name is "hsrp-Fa0/0.100-201" (default)
```

ルータ 2 設定

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

```
Router2# show standby
```

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

例 : HSRP グローバル IPv6 アドレスの設定

次に、明示的に設定された 1 つのリンクローカル アドレスと 3 つの HSRP グローバル IPv6 アドレスの例を示します。

```
interface Ethernet0/0
no ip address
ipv6 address 2001::DB8:1/64
standby version 2
standby 1 ipv6 FE80::1:CAFÉ
standby 1 ipv6 2001::DB8:2/64
standby 1 ipv6 2001:DB8::3/64
standby 1 ipv6 2001:DB8::4/64
end
```

その他の関連資料

関連資料

関連項目	参照先
IPv6 リンクローカル アドレスとステートレス自動設定	『Cisco IOS IPv6 Configuration Guide』の「 Implementing IPv6 Addressing and Basic Connectivity 」
IPv6 コマンド: コマンド構文、コマンドモード、コマンド履歴、デフォルト、使用上のガイドライン、および例	『Cisco IOS IPv6 Command Reference』
IPv4 における HSRP の設定	『Cisco IOS IP Application Services Configuration Guide』の「 Configuring HSRP 」

規格

規格	タイトル
この機能によってサポートされ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
なし	選択したプラットフォーム、Cisco ソフトウェア リリース、および機能セットの MIB の場所を検索し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 2281	『Cisco Hot Standby Router Protocol (HSRP)』

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>	<p>http://www.cisco.com/cisco/web/support/index.html</p>

IPv6 における First Hop Redundancy Protocol 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。

プラットフォームのサポートおよびソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator により、どのソフトウェア イメージが特定のソフトウェア リリース、機能セット、またはプラットフォームをサポートするか調べることができます。Cisco Feature Navigator には、<http://www.cisco.com/go/cfn> からアクセスします。Cisco.com のアカウントは必要ありません。



(注)

表 1 には、一連のソフトウェア リリースのうち、特定の機能が初めて導入されたソフトウェア リリースだけが記載されています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 1 IPv6 における First Hop Redundancy Protocol の機能情報

機能名	リリース	機能設定情報
FHRP : IPv6 用 GLBP のサポート	12.2(58)SE 12.2(33)SXI 12.4(6)T	<p>GLBP は、障害が発生したルータまたは回線からデータトラフィックを保護し、冗長ルータ間でパケットのロードシェアリングを実行できるようにします。</p> <p>この機能に関する詳細については、次の項を参照してください。</p> <ul style="list-style-type: none"> • 「GLBP for IPv6」 (P.2) • 「GLBP の設定とカスタマイズ」 (P.9) • 「GLBP のトラブルシューティング」 (P.20) • 「例 : GLBP 設定のカスタマイズ」 (P.24) • 「例 : GLBP の重み付け」 (P.25) • 「例 : GLBP 設定のイネーブル化」 (P.25) <p>glbp forwarder preempt、glbp ipv6、glbp load-balancing、glbp preempt、glbp priority、glbp name、glbp timers、glbp timers redirect、glbp weighting、glbp weighting track、track interface の各コマンドがこの機能のために導入または修正されました。</p>
GLBP MD5 認証	12.2(18)S 12.3(2)T	<p>MD5 認証を使用すると、別のプレーンテキスト認証方式よりもセキュリティを強化できます。MD5 認証では、各 GLBP グループ メンバが秘密キーを使用して、発信パケットに含まれるキー付き MD5 ハッシュを生成できます。着信パケットのキー付きハッシュが生成され、発信パケット内のハッシュが生成されたハッシュに一致しない場合、そのパケットは無視されます。</p> <p>この機能に関する詳細については、次の項を参照してください。</p> <ul style="list-style-type: none"> • 「GLBP 認証の設定」 (P.11) • 「例 : キー ストリングを使用した GLBP MD5 認証」 (P.24) • 「例 : キー チェーンを使用した GLBP MD5 認証」 (P.25) • 「例 : GLBP テキスト認証」 (P.25) <p>glbp authentication、key、key chain、key-string (認証)、show glbp、show key chain の各コマンドがこの機能のために導入または修正されました。</p>

表 1 IPv6 における (続き) First Hop Redundancy Protocol の機能情報 (続き)

機能名	リリース	機能設定情報
IPv6 サービス : HSRP for IPv6	12.4(4)T 12.2(33)SRB 12.2(33)SXI	<p>HSRP は、ファーストホップ IPv6 ルータの透過的なフェールオーバーを可能にする FHRP です。</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 for IPv6」(P.6) 「IPv6 用 HSRP グループの動作のイネーブル化」(P.21) 「例 : IPv6 用 HSRP グループの動作のイネーブル化と確認」(P.26) <p>show standby、standby ipv6、standby preempt、standby priority 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 : グローバル IPv6 アドレス	12.2(33)SXI4	<p>HSRP グローバル IPv6 アドレス機能では、ユーザが複数の非リンク ローカル アドレスを仮想アドレスとして設定できます。</p> <p>この機能に関する詳細については、次の各項を参照してください。</p> <ul style="list-style-type: none"> 「HSRP グローバル IPv6 アドレス」(P.7) 「IPv6 用 HSRP グループの動作のイネーブル化と確認」(P.22) 「例 : HSRP グローバル IPv6 アドレスの設定」(P.27) <p>standby ipv6 コマンドが、この機能によって修正されました。</p>

用語集

- **CPE** : Customer Premises Equipment (CPE; 宅内装置)
- **FHRP** : First Hop Redundancy Protocol (FHRP)
- **GLBP** : 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)
- **HSRP** : Hot Standby Routing Protocol (HSRP)
- **NA** : Neighbor Advertisement (NA; ネイバー アドバタイズメント)
- **ND** : Neighbor Discovery (ND; ネイバー探索)
- **NS** : Neighbor Solicitation (NS; ネイバー請求)
- **PE** : Provider Equipment (PE)
- **RA** : Router Advertisement (RA; ルータ アドバタイズメント)
- **RS** : Router Solicitation (RS; ルータ請求)

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、および図は、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。

© 2006–2011 Cisco Systems, Inc.
All rights reserved.

Copyright © 2006–2011, シスコシステムズ合同会社.
All rights reserved.

