GLBP の設定

Gateway Load Balancing Protocol（GLBP; ゲートウェイ ロード バランシング プロトコル）は、Hot Standby Router Protocol（HSRP; ホット スタンバイ ルータ プロトコル）や Virtual Router Redundancy Protocol（VRRP; 仮想ルータ冗長プロトコル）のように、機能を停止したルータや回路からデータ トラフィックを保護します。このとき、冗長化されたルータのグループ間でパケットのロード シェアリングを行うことができます。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。この章に記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「GLBP の機能情報」（P.26）を参照してください。

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

この章の構成

GLBP の制約事項

Enhanced Object Tracking（EOT; 拡張オブジェクト トラッキング）はステートフル スイッチオーバー（SSO）を認識しないため、SSO モードで GLBP と併用することはできません。

GLBP の前提条件

GLBP を設定する前に、ルータが物理インターフェイス上で複数の MAC アドレスをサポートできることを確認します。設定している GLBP フォワーダごとに、追加の MAC アドレスが使用されます。

GLBP について

GLBP を設定するには、次の概念を理解しておく必要があります。

GLBP の概要

GLBP は、IEEE 802.3 LAN 上の単一のデフォルト ゲートウェイを使用して設定されている IP ホストの自動ルータ バックアップを提供します。LAN 上の複数のファーストホップ ルータを連結し、IP パケットの転送負荷を共有しながら単一の仮想ファーストホップ IP ルータを提供します。LAN 上にあるその他のルータは、冗長化された GLBP ルータとして動作できます。このルータは、既存のフォワーディング ルータが機能しなくなった場合にアクティブになります。

GLBP は、ユーザに対しては HSRP や VRRP と同様の機能を実行します。HSRP や VRRP では、バーチャル IP アドレスを使用して設定されている仮想ルータ グループに複数のルータを参加させることができます。グループのバーチャル IP アドレスに送信されたパケットを転送するアクティブ ルータとして、1 つのメンバが選択されます。グループ内の他のルータは、アクティブ ルータが機能を停止するまで冗長化されます。これらのスタンバイ ルータには、プロトコルが使用していない、未使用の帯域幅があります。1 つのルータ セットに複数の仮想ルータ グループを設定できますが、そのホストに設定するデフォルト ゲートウェイは異なるようにする必要があります。結果として、追加の管理上の負担がかかります。GLBP には、単一のバーチャル IP アドレスと複数のバーチャル MAC アドレスを使用して、複数のルータ（ゲートウェイ）上でのロード バランシングを提供するというメリットがあります。転送負荷は、GLBP グループ内のすべてのルータ間で共有されます。単一のルータだけで処理して、他のルータがアイドルのままになっているということはありません。各ホストは、同じバーチャル

IP アドレスで設定され、仮想ルータ グループ内のすべてのルータが参加してパケットの転送を行います。GLBP メンバは、Hello メッセージを使用して相互に通信します。このメッセージは 3 秒ごとにマルチキャスト アドレス 224.0.0.102、User Datagram Protocol（UDP; ユーザ データグラム プロトコル）ポート 3222（送信元と宛先）に送信されます。

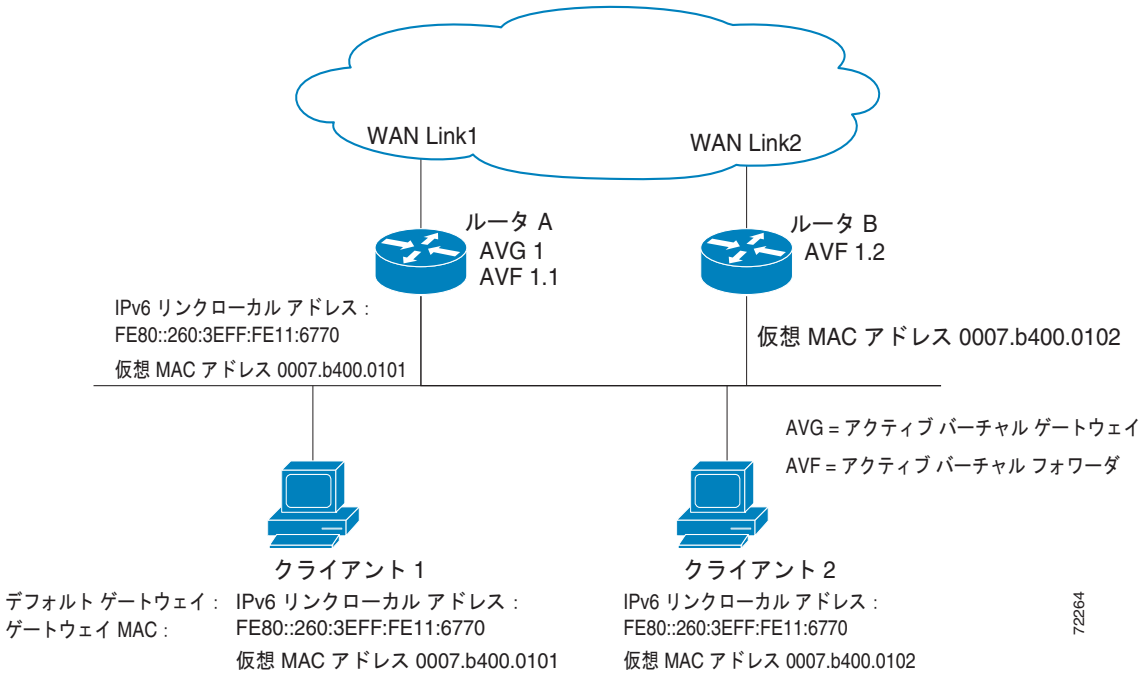
GLBP アクティブ バーチャル ゲートウェイ

GLBP グループのメンバは、そのグループの Active Virtual Gateway（AVG; アクティブ バーチャル ゲートウェイ）となるゲートウェイを 1 つ選択します。他のグループ メンバは、AVG が使用できなくなった場合に AVG のバックアップを提供します。AVG の機能として、バーチャル MAC アドレスを GLBP グループの各メンバに割り当てることが挙げられます。各ゲートウェイは、AVG によって割り当てられたバーチャル MAC アドレスに送信されたパケットの転送を行います。これらのゲートウェイはバーチャル MAC アドレスの「アクティブ バーチャル フォワーダ（AVF）」と呼ばれます。

AVG は、バーチャル IP アドレスの Address Resolution Protocol（ARP; アドレス解決プロトコル）要求への応答も行います。異なるバーチャル MAC アドレスを使用して ARP 要求に応答することで、AVG によるロード シェアリングが実現します。

図 1 では、ルータ A は GLBP グループの AVG で、バーチャル IP アドレス 10.21.8.10 に関する処理を行います。ルータ A はバーチャル 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、バーチャル MAC アドレス 0007.b400.0102 の AVF として指定されています。クライアント 1 のデフォルト ゲートウェイ IP アドレスは 10.21.8.10、ゲートウェイ MAC アドレスは 0007.b400.0101 です。クライアント 2 は、同じデフォルト ゲートウェイ IP アドレスを共有しますが、ゲートウェイ MAC アドレス 0007.b400.0102 を受信します。これは、ルータ B はルータ A とトラフィックの負荷を共有しているためです。

図 1　　GLBP トポロジ



ルータ A が使用できなくなっても、クライアント 1 が WAN にアクセスできなくなることはありません。これは、ルータ B が、ルータ A のバーチャル MAC アドレスに送信されたパケットの転送を行うためです。また、独自のバーチャル MAC アドレスに送信されたパケットについても処理を実行します。ルータ B は、GLBP グループ全体で AVG のロールを担います。GLBP グループ内のルータが機能を停止しても、GLBP メンバ間の通信は継続されます。

GLBP バーチャル MAC アドレス割り当て

GLBP グループは、グループごとに最大 4 つのバーチャル MAC アドレスを設定できます。グループの各メンバへのバーチャル MAC アドレスの割り当ては、AVG が行います。他のグループ メンバは、Hello メッセージを通じて AVG を検出すると、バーチャル MAC アドレスを要求します。ゲートウェイは、順番に、次の MAC アドレスを割り当てられます。AVG によってバーチャル MAC アドレスが割り当てられたバーチャル フォワーダは、「プライマリ バーチャル フォワーダ」と呼ばれます。
GLBP グループの他のメンバは、Hello メッセージからバーチャル MAC アドレスを学習します。バーチャル MAC アドレスを学習したバーチャル フォワーダは、「セカンダリ バーチャル フォワーダ」と呼ばれます。

GLBP バーチャル ゲートウェイの冗長化

GLBP は、HSRP と同じ方法でバーチャル ゲートウェイの冗長化を行います。1 つのゲートウェイが AVG として選択され、別のゲートウェイがスタンバイ バーチャル ゲートウェイとして選択されます。残りのゲートウェイは、リスン ステートになります。

AVG の機能が停止すると、スタンバイ バーチャル ゲートウェイが該当するバーチャル IP アドレスの処理を担当します。新しいスタンバイ バーチャル ゲートウェイは、リスン ステートにあるゲートウェイの中から選ばれます。

GLBP バーチャル フォワーダの冗長化

バーチャル フォワーダの冗長化は、AVF で使用するバーチャル ゲートウェイの冗長化に類似しています。AVF の機能が停止すると、リスン ステートにあるセカンダリ バーチャル フォワーダの 1 つが、該当するバーチャル MAC アドレスの処理を担当します。

新しい AVF は、別のフォワーダ番号のプライマリ バーチャル フォワーダにもなります。GLBP は、2 つのタイマーを使用して古いフォワーダ番号からホストを移行します。このタイマーは、ゲートウェイがアクティブ バーチャル フォワーダ状態になるとすぐに作動を開始します。GLBP は Hello メッセージを使用して、タイマーの現在の状態を伝えます。

AVG が継続して古いバーチャル フォワーダ MAC アドレスにホストをリダイレクトしている時間が、リダイレクト時間になります。リダイレクト時間が経過すると、AVG は ARP 応答で古いバーチャル フォワーダ MAC アドレスを使用するのを停止しますが、バーチャル フォワーダは、古いバーチャル フォワーダ MAC アドレスに送信されたパケットの転送を引き続き行います。

バーチャル フォワーダが有効である時間は、セカンダリ ホールド時間になります。セカンダリ ホールド時間が経過すると、GLBP グループのすべてのゲートウェイからバーチャル フォワーダが削除されます。期限の切れたバーチャル フォワーダ番号は、AVG によって再割り当てされるようになります。

GLBP ゲートウェイ プライオリティ

各 GLBP ゲートウェイが果たすロールと、AVG の機能が停止したときにどのようなことが発生するかについては、GLBP ゲートウェイ プライオリティによって決まります。

また、GLBP ルータがバックアップ バーチャル ゲートウェイとして機能するかどうかや、現在の AVG の機能が停止したときに AVG になる順序を決定するのもプライオリティです。**glbp priority** コマンドを使用して 1 ～ 255 の値を設定し、各バックアップ バーチャル ゲートウェイのプライオリティを設定できます。

図 1 では、ルータ A（LAN トポロジの AVG）の機能が停止すると、選択プロセスが行われ、処理を引き継ぐバックアップ バーチャル ゲートウェイが決定されます。この例では、グループ内の他のメンバはルータ B だけであるため、このルータが自動的に新しい AVG になります。同じ GLBP グループに別のルータが存在しており、そのルータにより高いプライオリティが設定されている場合は、高いプライオリティが設定されているルータが選択されます。両方のルータのプライオリティが同じである場合は、IP アドレスが大きい方のバックアップ バーチャル ゲートウェイが選択され、アクティブ バーチャル ゲートウェイになります。

デフォルトでは、GLBP バーチャル ゲートウェイのプリエンプティブ スキームはディセーブルになっています。バックアップ バーチャル ゲートウェイが AVG になるのは、現在の AVG が機能を停止した場合だけです。この場合、バーチャル ゲートウェイに割り当てられているプライオリティは関係ありません。GLBP バーチャル ゲートウェイ プリエンプティブ スキームをイネーブルにするには、**glbp preempt** コマンドを使用します。プリエンプションにより、バックアップ バーチャル ゲートウェイに現在の AVG よりも高いプライオリティが割り当てられている場合でも、バックアップ バーチャル ゲートウェイが AVG になることができます。

GLBP ゲートウェイの重み付けと追跡

GLBP は重み付けスキームを使用して、GLBP グループ内の各ルータの転送機能を指定できます。GLBP グループ内のルータに割り当てられている重み付けを使用して、そのルータがパケットを転送するかどうかを指定します。転送する場合は、パケット転送を行う LAN 上のホストの比率を指定します。GLBP グループの重み付けが特定の値を下回った場合は転送をディセーブルにするように、しきい値を設定できます。また、別のしきい値を上回ったときに転送を自動的に再度イネーブルにすることができます。

GLBP グループの重み付けは、ルータ内のインターフェイスのステートを追跡することで、自動的な調整が可能です。追跡対象のインターフェイスがダウンすると、GLBP グループの重み付けは指定された値の分だけ減じられます。別のインターフェイスを追跡して、GLBP の重み付けを減じることができます（減じる分量は変化させることができます）。

デフォルトでは、GLBP バーチャル フォワーダ プリエンプティブ スキームは、30 秒遅延してイネーブルにされます。バックアップ バーチャル フォワーダは、現在の AVF の重み付けが 30 秒間にわたって低い重みしきい値を下回った場合に、AVF になることができます。GLBP フォワーダ プリエンプティブ スキームをディセーブルにするには、**no glbp forwarder preempt** コマンドを使用します。遅延時間を変更するには、**glbp forwarder preempt delay minimum** コマンドを使用します。

GLBP クライアント キャッシュ

GLBP クライアント キャッシュには、GLBP グループをデフォルト ゲートウェイとして使用しているネットワーク ホストに関する情報が含まれています。

GLBP グループの Active Virtual Gateway（AVG）が、ネットワーク ホストから GLBP バーチャル IP アドレスの IPv4 Address Resolution Protocol（ARP; アドレス解決プロトコル）要求または IPv6 Neighbor Discovery（ND; ネイバ ディスカバリ）要求を受け取ると、GLBP クライアント キャッシュに新しいエントリが作成されます。キャッシュ エントリには、ARP 要求または ND 要求を送信したホスト、および AVG が割り当てたフォワーダに関する情報が含まれています。

GLBP クライアント キャッシュには、特定の GLBP グループを使用する各ホストの MAC アドレス、各ネットワーク ホストに割り当てられている GLBP フォワーダの数、GLBP グループの各フォワーダに現在割り当てられているネットワーク ホストの総数が格納されます。また、各ネットワーク ホストによって使用されるプロトコル アドレス、ホストとフォワーダの割り当てが最後に更新されてから経過した時間も格納されます。

GLBP クライアント キャッシュに GLBP グループのネットワーク ホスト（最大 2000）に関する情報を格納することもできます。一般には、最大 1000 のネットワーク ホストが設定されることが想定されています。**glbp client-cache maximum** コマンドを使用すると、各 GLBP グループを使用するネットワーク ホストの数に基づいて、各 GLBP グループごとにキャッシュされるネットワーク ホストの最大数を低く設定することができます。このコマンドにより、GLBP グループごとに、使用されるキャッシュ メモリの分量を制限できます。GLBP クライアント キャッシュが設定されたクライアントの最大数に達しているときに、新しいクライアントを追加すると、最も長い間更新されていないクライアント エントリが破棄されます。このような状況に陥ることは、設定された上限が小さすぎることを示します。

GLBP クライアント キャッシュによって使用されるメモリの分量は、GLBP グループを使用するネットワーク ホスト（クライアント キャッシュがイネーブルになっているもの）の数に左右されます。各ホストには、少なくとも 20 バイトが必要です。GLBP グループごとに、追加で 3200 バイトが必要になります。

GLBP グループで現在 AVG のロールを果たしているルータで **show glbp detail** コマンドを使用すると、GLBP クライアント キャッシュの内容を表示できます。GLBP グループの別のルータで **show glbp detail** コマンドを発行すると、クライアント キャッシュ情報を参照するには、このコマンドを AVG 上で再発行するようにメッセージが表示されます。**show glbp detail** コマンドでは、GLBP クライアント キャッシュの使用状況、およびフォワーダ間でのクライアントの分散に関する統計情報も表示されます。キャッシュ タイムアウトとクライアント制限パラメータが適切に設定されていれば、正確な統計情報を得られます。ネットワーク上のエンド ホストの数が制限値を超えておらず、エンド ホストの最大 ARP キャッシュ タイムアウトが GLBP クライアント キャッシュ タイムアウトを超えていない場合は、値は適切であると言えます。

各 GLBP グループの GLBP クライアント キャッシュは、**glbp client-cache** コマンドを使用して個別にイネーブルまたはディセーブルに設定できます。デフォルトでは、GLBP クライアント キャッシュはディセーブルになっています。GLBP クライアント キャッシュをイネーブルに設定できるグループの数に制限はありません。

GLBP キャッシュ エントリは、**glbp client-cache maximum** コマンドに **timeout** キーワード オプションを指定して、指定時間が経過した後にタイムアウトするように設定できます。

ISSU と GLBP

GLBP は In Service Software Upgrade（ISSU; インサービス ソフトウェア アップグレード）をサポートします。In Service Software Upgrade（ISSU）を使用すると、アクティブおよびスタンバイの Route Processor（RP; ルート プロセッサ）またはラインカード上で異なるバージョンの Cisco IOS ソフトウェアが実行されている場合でも、ハイアベイラビリティ（HA）システムをステートフル スイッチオーバー（SSO）モードで実行できるようになります。

ISSU は、サポートされる Cisco IOS リリースから別のリリースへアップグレードまたはダウングレードする機能を提供します。この場合、パケット転送は継続して行われ、セッションは維持されるため、予定されるシステムの停止時間を短くすることができます。アップグレードまたはダウングレードする機能は、アクティブ RP およびスタンバイ RP 上で異なるバージョンのソフトウェアを実行することで

実現します。これにより、RP 間でステート情報を維持する時間が短くなります。この機能により、システムをアップグレード対象（またはダウングレード対象）のソフトウェアを実行するセカンダリ RP に切り替えることができ、セッションを切断することなく、またパケットの損失も最小限に抑えながら、継続してパケットを転送できます。この機能は、デフォルトでイネーブルにされています。

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

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

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

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

GLBP SSO

GLBP SSO 機能が導入されたため、GLBP はステートフル スイッチオーバー（SSO）を認識するようになりました。GLBP は、ルータがセカンダリ RP にフェールオーバーしたことを検出し、グループの現在の状態を継続することができます。

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

GLBP が SSO を認識する前に、RP が冗長化されたルータに GLBP を展開した場合、アクティブ RP とスタンバイ RP 間のロールがスイッチオーバーされると、ルータの GLBP グループ メンバとしてのアクティビティは破棄され、ルータはリロードされた場合と同様にグループに再び参加することになります。GLBP SSO 機能により、スイッチオーバーが行われても、GLBP は継続してグループ メンバとしてのアクティビティを継続できます。冗長化された RP 間の GLBP ステート情報は維持されるため、スタンバイ RP はスイッチオーバーの実行中も実行後も GLBP 内で引き続きルータのアクティビティを実行できます。

この機能は、デフォルトでイネーブルにされています。この機能をディセーブルにするには、グローバル コンフィギュレーション モードで **no glbp sso** コマンドを使用します。

詳細については、『*Stateful Switchover*』を参照してください。

GLBP の利点

ロード シェアリング

LAN クライアントからのトラフィックを複数のルータで共有するように GLBP を設定できるため、利用可能なルータ間でより公平にトラフィックの負荷を共有できます。

複数の仮想ルータ

GLBP は、ルータの物理インターフェイスごとに、最大 1024 台の仮想ルータ（GLBP グループ）をサポートします。また、グループごとに最大 4 つのバーチャル フォワーダをサポートします。

プリエンプション

GLBP の冗長性スキームにより、アクティブ バーチャル ゲートウェイのプリエンプトが可能になり、より高いプライオリティが設定されたバックアップ バーチャル ゲートウェイを利用できるようになります。フォワーダ プリエンプションも同様に動作しますが、フォワーダ プリエンプションではプライオリティではなく重み付けを使用する点が異なります。また、フォワーダ プリエンプションはデフォルトでイネーブルになっています。

認証

信頼性やセキュリティを向上させて GLBP スプーフィング ソフトウェアからの保護を強化するため、業界標準の Message Digest 5（MD5; メッセージ ダイジェスト 5）アルゴリズムを使用することもできます。GLBP グループ内で、他のルータとは異なる認証文字列を使用するルータは、他のグループ メンバに無視されます。別の方法として、GLBP グループ メンバ間で簡易テキスト パスワード認証スキームを使用して、設定エラーを検出することもできます。

GLBP の設定方法

ここでは、次の各手順について説明します。

- 「GLBP のイネーブル化と確認」（P.8）（必須）
- 「GLBP のカスタマイズ」（P.10）（任意）
- 「GLBP 認証の設定」（P.13）（任意）
- 「GLBP 重み値とオブジェクト トラッキングの設定」（P.18）（任意）
- 「GLBP のトラブルシューティング」（P.20）（任意）

GLBP のイネーブル化と確認

インターフェイス上で GLBP をイネーブルにし、設定と操作を確認するには、次の手順を実行します。GLBP は設定しやすいように設計されています。GLBP グループ内の各ゲートウェイは、同じグループ番号を使用して設定する必要があります。また、GLBP グループ内の少なくとも 1 つのゲートウェイは、そのグループで使うバーチャル IP アドレスを使用して設定しなければなりません。その他、必要となるすべてのパラメータは学習することができます。

前提条件

インターフェイスで VLAN を使用している場合、GLBP のグループ番号は VLAN ごとに異なる番号を使用する必要があります。

手順の概要

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

7. **show glbp** [*interface-type interface-number*] [*group*] [*state*] [**brief**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* 例： `Router(config)# interface fastethernet 0/0`	インターフェイス タイプおよび番号を指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ip address** *ip-address mask* [**secondary**] 例： `Router(config-if)# ip address 10.21.8.32 255.255.255.0`	インターフェイスのプライマリ IP アドレスまたはセカンダリ IP アドレスを指定します。
ステップ 5	**glbp** *group* **ip** [*ip-address* [**secondary**]] 例： `Router(config-if)# glbp 10 ip 10.21.8.10`	インターフェイス上で GLBP をイネーブルにし、バーチャル ゲートウェイのプライマリ IP アドレスを指定します。 • プライマリ IP アドレスを指定すると、もう一度 **glbp** *group* **ip** コマンドを **secondary** キーワードとともに使用して、このグループでサポートする追加の IP アドレスを指定できます。
ステップ 6	**exit** 例： `Router(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了し、ルータをグローバル コンフィギュレーション モードに戻します。
ステップ 7	**show glbp** [*interface-type interface-number*] [*group*] [*state*] [**brief**] 例： `Router(config)# show glbp 10`	（任意）ルータの GLBP グループに関する情報を表示します。 • オプションの **brief** キーワードを使用すると、各バーチャル ゲートウェイまたはバーチャル フォワーダに関する情報が 1 行で表示されます。 • 「例」で、このタスクのコマンド出力を参照してください。

例

次に、ルータ上にある GLBP グループ 10 のステータス出力例を示します。

```
Router# show glbp 10

FastEthernet0/0 - Group 10
  State is Active
    2 state changes, last state change 23:50:33
  Virtual IP address is 10.21.8.10
  Hello time 5 sec, hold time 18 sec
```

```
  Next hello sent in 4.300 secs
Redirect time 1800 sec, forwarder time-out 28800 sec
Authentication text, string "authword"
Preemption enabled, min delay 60 sec
Active is local
Standby is unknown
Priority 254 (configured)
Weighting 105 (configured 110), thresholds: lower 95, upper 105
  Track object 2 state Down decrement 5
Load balancing: host-dependent
There is 1 forwarder (1 active)
Forwarder 1
  State is Active
    1 state change, last state change 23:50:15
  MAC address is 0007.b400.0101 (default)
  Owner ID is 0005.0050.6c08
  Redirection enabled
  Preemption enabled, min delay 60 sec
  Active is local, weighting 105
```

GLBP のカスタマイズ

GLBP 設定をカスタマイズするには、次の手順を実行します。

GLBP の動作のカスタマイズはオプションです。GLBP グループをイネーブルにするとすぐに、そのグループは動作を開始することに注意してください。GLBP をカスタマイズする前に GLBP グループをイネーブルにすると、ルータがグループの制御を引き継ぎ、機能のカスタマイズを完了する前に AVG になることがあります。このため、GLBP をカスタマイズする場合には、カスタマイズを行ってから GLBP をイネーブルにすることを推奨します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip address** *ip-address mask* [**secondary**]
5. **glbp** *group* **timers** [**msec**] *hellotime* [**msec**] *holdtime*
6. **glbp** *group* **timers redirect** *redirect timeout*
7. **glbp** *group* **load-balancing** [**host-dependent** | **round-robin** | **weighted**]
8. **glbp** *group* **priority** *level*
9. **glbp** *group* **preempt** [**delay minimum** *seconds*]
10. **glbp** *group* **client-cache maximum** *number* [**timeout** *minutes*]
11. **glbp** *group* **name** *redundancy-name*
12. **exit**
13. **no glbp sso**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* **例：** `Router(config)# interface fastethernet 0/0`	インターフェイス タイプおよび番号を指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ip address** *ip-address mask* [**secondary**] **例：** `Router(config-if)# ip address 10.21.8.32 255.255.255.0`	インターフェイスのプライマリ IP アドレスまたはセカンダリ IP アドレスを指定します。
ステップ 5	**glbp** *group* **timers** [**msec**] *hellotime* [**msec**] *holdtime* **例：** `Router(config-if)# glbp 10 timers 5 18`	GLBP グループで AVG が連続して送信する hello パケットの間隔を設定します。 • *holdtime* 引数を使用して、hello パケット内のバーチャル ゲートウェイおよびバーチャル フォワーダ情報が有効と見なされるまでのインターバル（秒）を指定します。 • オプションの **msec** キーワードを指定すると、引数の単位は（デフォルトの秒ではなく）ミリ秒を表すことになります。
ステップ 6	**glbp** *group* **timers redirect** *redirect timeout* **例：** `Router(config-if)# glbp 10 timers redirect 1800 28800`	AVG が継続してクライアントを AVF にリダイレクトする期間を設定します。デフォルト値は 600 秒（10 分）です。 • *timeout* 引数は、セカンダリ バーチャル フォワーダが無効になるまでのインターバル（秒）を指定します。デフォルトは 14,400 秒（4 時間）です。 **（注）** *redirect* 引数のゼロ（0）値は、指定できる値の範囲から除外することはできません。Cisco IOS ソフトウェアの事前設定でゼロ（0）値を使用しているため、アップグレードに悪影響を及ぼすことになります。ただし、ゼロ（0）値に設定することは推奨しません。この値を使用すると、リダイレクト タイマーが期限切れになりません。リダイレクト タイマーが期限切れにならないと、ルータが機能を停止したときに、バックアップにリダイレクトされず、機能を停止したルータに割り当てられている新しいホストが継続して動作します。

	コマンドまたはアクション	目的
ステップ 7	**glbp** *group* **load-balancing** [**host-dependent** | **round-robin** | **weighted**] 例： `Router(config-if)# glbp 10 load-balancing host-dependent`	GLBP AVG で採用するロード バランシングの方法を指定します。
ステップ 8	**glbp** *group* **priority** *level* 例： `Router(config-if)# glbp 10 priority 254`	GLBP グループ内のゲートウェイのプライオリティ レベルを設定します。 • デフォルト値は 100 です。
ステップ 9	**glbp** *group* **preempt** [**delay minimum** *seconds*] 例： `Router(config-if)# glbp 10 preempt delay minimum 60`	現在の AVG よりも高いプライオリティが設定されている場合、GLBP グループの AVG として引き継ぐルータを指定します。 • このコマンドは、デフォルトでディセーブルになっています。 • オプションの **delay** キーワードと **minimum** キーワード、および *seconds* 引数を使用して、AVG のプリエンプションが発生するまでの最小遅延時間（秒）を指定します。
ステップ 10	**glbp** *group* **client-cache maximum** *number* [**timeout** *minutes*] 例： `Router(config-if)# glbp 10 client-cache maximum 1200 timeout 245`	（任意）GLBP クライアント キャッシュをイネーブルにします。 • このコマンドは、デフォルトでディセーブルになっています。 • *number* 引数を使用して、キャッシュがこの GLBP グループのためにホールドするクライアントの最大数を指定します。範囲は 8 ～ 2000 です。 • オプションの **timeout** *minutes* キーワードと引数のペアを使用して、クライアント情報が最後に更新されてから、クライアント エントリが GLBP クライアント キャッシュに保管される最大時間を設定します。範囲は、1 ～ 1440 分（1 日）です。 **（注）** IPv4 ネットワークでは、最大限に予測されるエンドホストの Address Resolution Protocol（ARP; アドレス解決プロトコル）キャッシュ タイムアウト値よりもやや長い GLBP クライアント キャッシュ タイムアウト値を設定することを推奨します。
ステップ 11	**glbp** *group* **name** *redundancy-name* 例： `Router(config-if)# glbp 10 name abcompany`	GLBP グループに名前を割り当てることで、IP 冗長性をイネーブルにします。 • GLBP が冗長化されたクライアントは、同じ GLBP グループ名を使用して設定する必要があります。このようにすることで、冗長化されたクライアントと GLBP グループを接続できます。

	コマンドまたはアクション	目的
ステップ 12	**exit** 例： `Router(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了し、ルータをグローバル コンフィギュレーション モードに戻します。
ステップ 13	**no glbp sso** 例： `Router(config)# no glbp sso`	（任意）SSO の GLBP サポートをディセーブルにします。

GLBP 認証の設定

ここでは、GLBP 認証の設定方法について説明します。実行する作業は、認証方法（テキスト認証、簡易 MD5 キー ストリング、MD5 キー チェーン）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.13）
- 「キー チェーンを使用した GLBP MD5 認証の設定」（P.15）
- 「GLBP テキスト認証の設定」（P.17）

GLBP MD5 認証のしくみ

MD5 認証は、代替となるプレーン テキスト認証スキームよりも高いセキュリティを実現します。MD5 認証を使用すると、各 GLBP グループ メンバが秘密鍵を使用して、発信パケットの一部である鍵付き MD5 ハッシュを生成できます。着信パケットの鍵付きハッシュが生成されると、生成されたハッシュと着信パケット内のハッシュが一致しない場合、パケットは無視されます。

MD5 ハッシュの鍵は、キー ストリングを使用して設定に直接指定することもできますし、キー チェーンを通して間接的に提供することもできます。

ルータは、GLBP グループと認証の設定が異なるルータから着信した GLBP パケットは無視します。GLBP には、次の 3 つの認証スキームがあります。

- 認証なし
- プレーン テキスト認証
- MD5 認証

GLBP パケットは、次の場合はいずれも拒否されます。

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

GLBP MD5 認証の利点

- スプーフィング ソフトウェアから保護します。
- 業界標準の MD5 アルゴリズムを使用して、信頼性とセキュリティを高めます。

キー ストリングを使用した GLBP MD5 認証の設定

キー ストリングを使用して GLBP MD5 認証を設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip address** *ip-address mask* [**secondary**]
5. **glbp** *group-number* **authentication md5 key-string** [**0** | **7**] *key*
6. **glbp** *group-number* **ip** [*ip-address* [**secondary**]]
7. 通信を行う各ルータ上でステップ 1 ～ 6 を繰り返します。
8. **end**
9. **show glbp**

手順の詳細

	コマンド	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* 例： `Router(config)# interface Ethernet0/1`	インターフェイス タイプを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ip address** *ip-address mask* [**secondary**] 例： `Router(config-if)# ip address 10.0.0.1 255.255.255.0`	インターフェイスのプライマリ IP アドレスまたはセカンダリ IP アドレスを指定します。
ステップ 5	**glbp** *group-number* **authentication md5 key-string** [**0** | **7**] *key* 例： `Router(config-if)# glbp 1 authentication md5 key-string d00b4r987654321a`	GLBP MD5 認証の認証キーを設定します。 • コマンドの文字数とキー ストリングの文字数を加えた値が 255 文字を超えることはできません。 • *key* 引数にはプレフィクスを指定しません。**0** を指定すると、キーは暗号化されていないことを示します。 • **7** を指定すると、キーは暗号化されていることを示します。**service password-encryption** グローバル コンフィギュレーション コマンドがイネーブルになっていると、key-string 認証キーは自動的に暗号化されます。
ステップ 6	**glbp** *group-number* **ip** [*ip-address* [**secondary**]] 例： `Router(config-if)# glbp 1 ip 10.0.0.10`	インターフェイス上で GLBP をイネーブルにし、バーチャル ゲートウェイのプライマリ IP アドレスを指定します。

	コマンド	目的
ステップ 7	通信を行う各ルータ上でステップ 1 ～ 6 を繰り返します。	—
ステップ 8	**end** **例：** `Router(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 9	**show glbp** **例：** `Router# show glbp`	（任意）GLBP 情報を表示します。 • このコマンドを使用して、設定を確認します。キー ストリングと認証タイプは、設定されている場合に表示されます。

キー チェーンを使用した GLBP MD5 認証の設定

キー チェーンを使用して GLBP MD5 認証を設定するには、次の手順を実行します。キー チェーンを使用すると、キー チェーンの設定に基づき、場合に応じて異なるキー ストリングを使用できます。GLBP は適切なキー チェーンを照会し、特定のキー チェーンに対して現在アクティブになっているキーとキー ID を取得します。

手順の概要

1. **enable**
2. **configure terminal**
3. **key chain** *name-of-chain*
4. **key** *key-id*
5. **key-string** *string*
6. **exit**
7. exit
8. **interface** *type number*
9. **ip address** *ip-address mask* [**secondary**]
10. **glbp** *group-number* **authentication md5 key-chain** *name-of-chain*
11. **glbp** *group-number* **ip** [*ip-address* [**secondary**]]
12. 通信を行う各ルータ上でステップ 1 ～ 10 を繰り返します。
13. **end**
14. **show glbp**
15. **show key chain**

手順の詳細

	コマンド	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードなど、高位の権限レベルをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**key chain** *name-of-chain* **例：** `Router(config)# key chain glbp2`	ルーティング プロトコルの認証をイネーブルにし、認証キーのグループを識別します。
ステップ 4	**key** *key-id* **例：** `Router(config-keychain)# key 100`	キー チェーンの認証キーを識別します。 • *key-id* は、数値で指定する必要があります。
ステップ 5	**key-string** *string* **例：** `Router(config-keychain-key)# key-string xmen382`	キーの認証文字列を指定します。 • *string* には、1 ～ 80 文字の大文字と小文字の英数字を指定できます。ただし、最初の文字を数値にすることはできません。
ステップ 6	**exit** **例：** `Router(config-keychain-key)# exit`	キーチェーン コンフィギュレーション モードに戻ります。
ステップ 7	**exit** **例：** `Router(config-keychain)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 8	**interface** *type number* **例：** `Router(config)# interface Ethernet0/1`	インターフェイス タイプを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 9	**ip address** *ip-address mask* [**secondary**] **例：** `Router(config-if)# ip address 10.21.0.1 255.255.255.0`	インターフェイスのプライマリ IP アドレスまたはセカンダリ IP アドレスを指定します。
ステップ 10	**glbp** *group-number* **authentication md5 key-chain** *name-of-chain* **例：** `Router(config-if)# glbp 1 authentication md5 key-chain glbp2`	GLBP MD5 認証の認証 MD5 キー チェーンを設定します。 • キー チェーン名は、ステップ 3 で指定した名前と一致する必要があります。
ステップ 11	**glbp** *group-number* **ip** [*ip-address* [**secondary**]] **例：** `Router(config-if)# glbp 1 ip 10.21.0.12`	インターフェイス上で GLBP をイネーブルにし、バーチャル ゲートウェイのプライマリ IP アドレスを指定します。

	コマンド	目的
ステップ 12	通信を行う各ルータ上でステップ 1 ～ 10 を繰り返します。	—
ステップ 13	**end** **例：** `Router(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 14	**show glbp** **例：** `Router# show glbp`	（任意）GLBP 情報を表示します。 • このコマンドを使用して、設定を確認します。キー チェーンと認証タイプは、設定されている場合に表示されます。
ステップ 15	**show key chain** **例：** `Router# show key chain`	（任意）認証キー情報を表示します。

GLBP テキスト認証の設定

GLBP テキスト認証を設定するには、次の手順を実行します。この認証方法では、最小限のセキュリティが提供されます。高いセキュリティが必要な場合は、MD5 認証を使用してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip address** *ip-address mask* [**secondary**]
5. **glbp** *group-number* **authentication text** *string*
6. **glbp** *group-number* **ip** [*ip-address* [**secondary**]]
7. 通信を行う各ルータ上でステップ 1 ～ 6 を繰り返します。
8. **end**
9. **show glbp**

手順の詳細

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

	コマンド	目的
ステップ 3	**interface** *type number* 例： `Router(config)# interface Ethernet0/1`	インターフェイス タイプを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ip address** *ip-address mask* [**secondary**] 例： `Router(config-if)# ip address 10.0.0.1 255.255.255.0`	インターフェイスのプライマリ IP アドレスまたはセカンダリ IP アドレスを指定します。
ステップ 5	**glbp** *group-number* **authentication text** *string* 例： `Router(config-if)# glbp 10 authentication text stringxyz`	グループ内の他のルータから受信した GLBP パケットを認証します。 • 認証を設定する場合、GLBP グループ内のすべてのルータで同じ認証文字列を使用する必要があります。
ステップ 6	**glbp** *group-number* **ip** [*ip-address* [**secondary**]] 例： `Router(config-if)# glbp 1 ip 10.0.0.10`	インターフェイス上で GLBP をイネーブルにし、バーチャル ゲートウェイのプライマリ IP アドレスを指定します。
ステップ 7	通信を行う各ルータ上でステップ 1 ～ 6 を繰り返します。	—
ステップ 8	**end** 例： `Router(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 9	**show glbp** 例： `Router# show glbp`	（任意）GLBP 情報を表示します。 • このコマンドを使用して、設定を確認します。

GLBP 重み値とオブジェクト トラッキングの設定

GLBP 重み値とオブジェクト トラッキングを設定するには、次の手順を実行します。

GLBP 重み付けにより、GLBP グループがバーチャル フォワーダとして動作できるかどうかが決定されます。初期の重み値は設定可能で、オプションでしきい値を指定できます。インターフェイス ステートの追跡が可能で、インターフェイスがダウンした場合に重み値を減らすように設定できます。GLBP グループの重み付けが指定の値を下回ると、グループがアクティブ バーチャル フォワーダになることはありません。重み付けが指定の値を上回ると、グループは再びアクティブ バーチャル フォワーダとしてのロールを実行できるようになります。

手順の概要

1. **enable**
2. **configure terminal**
3. **track** *object-number* **interface** *type number* {**line-protocol** | **ip routing**}
4. **exit**
5. **interface** *type number*
6. **glbp** *group* **weighting** *maximum* [**lower** *lower*] [**upper** *upper*]
7. **glbp** *group* **weighting track** *object-number* [**decrement** *value*]

8. **glbp** *group* **forwarder preempt** [**delay minimum** *seconds*]
9. **end**
10. **show track** [*object-number* | **brief**] [**interface** [**brief**] | **ip route** [**brief**] | **resolution** | **timers**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**track** *object-number* **interface** *type number* {**line-protocol** | **ip routing**} 例： `Router(config)# track 2 interface POS 6/0 ip routing`	インターフェイスを追跡し、インターフェイスのステートに変更が生じると GLBP ゲートウェイの重み付けを変更して、トラッキング コンフィギュレーション モードを開始するように設定します。 • このコマンドを使って、**glbp weighting track** コマンドで使用されるインターフェイスおよび対応するオブジェクト番号を設定します。 • **line-protocol** キーワードは、インターフェイスがアップしているかどうかを追跡します。**ip routing** キーワードは、インターフェイス上で IP ルーティングがイネーブルになっており、IP アドレスが設定されていることを確認します。
ステップ 4	**exit** 例： `Router(config-track)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 5	**interface** *type number* 例： `Router(config)# interface fastethernet 0/0`	インターフェイス コンフィギュレーション モードを開始します。
ステップ 6	**glbp** *group* **weighting** *maximum* [**lower** *lower*] [**upper** *upper*] 例： `Router(config-if)# glbp 10 weighting 110 lower 95 upper 105`	GLBP ゲートウェイの初期の重み値、上限しきい値、および下限しきい値を指定します。
ステップ 7	**glbp** *group* **weighting track** *object-number* [**decrement** *value*] 例： `Router(config-if)# glbp 10 weighting track 2 decrement 5`	GLBP ゲートウェイの重み付けに影響を与える、追跡対象のオブジェクトを指定します。 • *value* 引数により、追跡対象オブジェクトが機能を停止した場合に、GLBP ゲートウェイの重み付けで減じる値を指定します。

	コマンドまたはアクション	目的
ステップ 8	**glbp** *group* **forwarder preempt** [**delay minimum** *seconds*] 例： `Router(config-if)# glbp 10 forwarder preempt delay minimum 60`	GLBP グループの現在の AVF の値が重みしきい値よりも低くなった場合に、GLBP グループの AVF としてのロールを引き継ぐルータを設定します。 • このコマンドはデフォルトでイネーブルに設定され、30 秒遅延するようになっています。 • オプションの **delay** キーワードと **minimum** キーワード、および *seconds* 引数を使用して、AVF のプリエンプションが発生するまでの最小遅延時間（秒）を指定します。
ステップ 9	**end** 例： `Router(config-if)# exit`	特権 EXEC モードに戻ります。
ステップ 10	**show track** [*object-number* | **brief**] [**interface** [**brief**]| **ip route** [**brief**] | **resolution** | **timers**] 例： `Router# show track 2`	トラッキング情報を表示します。

GLBP のトラブルシューティング

GLBP には、GLBP の動作に関連するさまざまなイベントについての診断内容をコンソールに表示できるように、5 つの特権 EXEC モード コマンドが導入されています。**debug condition glbp**、**debug glbp errors**、**debug glbp events**、**debug glbp packets**、および **debug glbp terse** コマンドを使用すると、大量の情報が出力され、ルータのパフォーマンスが著しく低下するため、このコマンドはトラブルシューティングを行うときにのみ使用するようにしてください。**debug glbp** コマンドを使用したときの影響を最小限に抑えるには、次の手順を実行します。

この手順により、コンソール ポートが文字単位のプロセッサ割り込みを行わなくなるため、**debug condition glbp** コマンドまたは **debug glbp** コマンドを使用することでルータにかかる負荷が最小限に抑えられます。コンソールに直接接続できない場合は、ターミナル サーバ経由でこの手順を実行できます。ただし、Telnet 接続を切断しなければならない場合は、デバッグ出力の生成でプロセッサに負荷がかかりルータが応答できないことに起因して、再接続できないことがあります。

前提条件

この手順を実行するには、GLBP を実行しているルータがコンソールに直接接続されている必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **no logging console**
4. Telnet を使用してルータ ポートにアクセスし、ステップ 1 および 2 を繰り返します。
5. **end**
6. **terminal monitor**

7. **debug condition glbp** *interface-type interface-number group* [*forwarder*]
8. **terminal no monitor**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**no logging console** 例： `Router(config)# no logging console`	コンソール ターミナルへのロギングをすべてディセーブルにします。 • コンソールへのロギングを再びイネーブルにするには、グローバル コンフィギュレーション モードで **logging console** コマンドを使用します。
ステップ 4	Telnet を使用してルータ ポートにアクセスし、ステップ 1 および 2 を繰り返します。	再帰的 Telnet セッションでグローバル コンフィギュレーション モードを開始します。これにより、出力をコンソール ポートからリダイレクトできるようになります。
ステップ 5	**end** 例： `Router(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**terminal monitor** 例： `Router# terminal monitor`	仮想端末でのロギング出力をイネーブルにします。
ステップ 7	**debug condition glbp** *interface-type interface-number group* [*forwarder*] 例： `Router# debug condition glbp fastethernet 0/0 10 1`	GLBP 状態についてのデバッグ メッセージを表示します。 • 特定の **debug condition glbp** コマンドまたは **debug glbp** コマンドのみを入力し、特定のサブコンポーネントに対する出力を分離してプロセッサにかかる負荷を最小限に抑えるようにします。適切な引数とキーワードを使用し、特定のサブコンポーネントについての詳細なデバッグ情報を生成します。 • 完了したら、特定の **no debug condition glbp** コマンドまたは **no debug glbp** コマンドを入力します。
ステップ 8	**terminal no monitor** 例： `Router# terminal no monitor`	仮想端末でのロギング出力をディセーブルにします。

GLBP の設定例

ここでは、次の設定例について説明します。

- 「GLBP 設定のカスタマイズ：例」（P.22）

GLBP 設定のカスタマイズ：例

次に、図 1 に示すルータ A を設定する例を示します。

```
interface fastethernet 0/0
 ip address 10.21.8.32 255.255.255.0
 glbp 10 timers 5 18
 glbp 10 timers redirect 1800 28800
 glbp 10 load-balancing host-dependent
 glbp 10 priority 254
 glbp 10 preempt delay minimum 60
 glbp 10 client-cache maximum 1200 timeout 245
```

キー ストリングを使用した GLBP MD5 認証の設定：例

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

```
!
interface Ethernet0/1
 ip address 10.0.0.1 255.255.255.0
 glbp 2 authentication md5 key-string ThisStringIsTheSecretKey
 glbp 2 ip 10.0.0.10
```

キー チェーンを使用した GLBP MD5 認証の設定：例

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

```
key chain AuthenticateGLBP
 key 1
  key-string ThisIsASecretKey

interface Ethernet0/1
 ip address 10.0.0.1 255.255.255.0
 glbp 2 authentication md5 key-chain AuthenticateGLBP
 glbp 2 ip 10.0.0.10
```

GLBP テキスト認証の設定：例

次に、テキスト ストリングを使用して GLBP テキスト認証を設定する例を示します。

```
interface fastethernet 0/0
 ip address 10.21.8.32 255.255.255.0
 glbp 10 authentication text stringxyz
 glbp 10 ip 10.21.8.10
```

GLBP 重み付けの設定：例

次の例では、図 1 のルータ A は POS インターフェイス 5/0 および 6/0 の IP ルーティング ステートを追跡するように設定されています。初期の GLBP 重み付けについては、上限しきい値と下限しきい値が設定され、重み付けは 10 ずつ減じるように設定されています。POS インターフェイス 5/0 および 6/0 がダウンすると、ルータの重み値が減じられます。

```
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
```

GLBP 設定のイネーブル化：例

次の例では、図 1 のルータ A は GLBP をイネーブルにするように設定されています。GLBP グループ 10 には、バーチャル IP アドレス 10.21.8.10 が指定されています。

```
interface fastethernet 0/0
 ip address 10.21.8.32 255.255.255.0
 glbp 10 ip 10.21.8.10
```

その他の参考資料

GLBP に関連する参考資料については、次の各項を参照してください。

関連資料

内容	参照先
GLBP コマンド：コマンド構文、コマンド モード、コマンド履歴、デフォルト設定、使用に関する注意事項および例	『*Cisco IOS IP Application Services Command Reference*』
In Service Software Upgrade（ISSU; インサービス ソフトウェア アップグレード）の設定	「Cisco IOS In Service Software Upgrade Process」モジュール
キー チェーンおよびキー管理用コマンド：コマンド構文の詳細、コマンド モード、コマンド履歴、デフォルト設定、使用に関する注意事項および例	『*Cisco IOS IP Routing : RIP Command Reference*』
オブジェクト トラッキング	「Configuring Enhanced Object Tracking」モジュール
ステートフル スイッチオーバー	「Stateful Switchover」モジュール
VRRP	「Configuring VRRP」モジュール
HSRP	「Configuring HSRP」モジュール

規格

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

MIB

MIB	MIB リンク
この機能がサポートする新しい MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco IOS リリース、および機能セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
この機能がサポートする新規 RFC または改訂 RFC はありません。また、この機能による既存 RFC のサポートに変更はありません。	—

シスコのテクニカル サポート

説明	リンク
Cisco Support Web サイトには、豊富なオンライン リソースが提供されており、それらに含まれる資料やツールを利用して、トラブルシューティングやシスコ製品およびテクノロジーに関する技術上の問題の解決に役立てることができます。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 • テクニカル サポートを受ける • ソフトウェアをダウンロードする • セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける • ツールおよびリソースへアクセスする • Product Alert の受信登録 • Field Notice の受信登録 • Bug Toolkit を使用した既知の問題の検索 • Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する • トレーニング リソースへアクセスする • TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する Japan テクニカル サポート Web サイトでは、Technical Support Web サイト（http://www.cisco.com/techsupport）の、利用頻度の高いドキュメントを日本語で提供しています。Japan テクニカル サポート Web サイトには、次の URL からアクセスしてください。 http://www.cisco.com/jp/go/tac	http://www.cisco.com/techsupport

GLBP の機能情報

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

ご使用の Cisco IOS ソフトウェア リリースによっては、コマンドの中に一部使用できないものがあります。特定のコマンドのサポートの導入時期に関する詳細については、コマンド リファレンス マニュアルを参照してください。

ここに記載のないテクノロジーの機能の詳細については、「Cisco IOS IP Application Services Features Roadmap」または「FHRP Features Roadmap」を参照してください。

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

表 1　GLBP の機能情報

機能名	リリース	機能設定情報
Gateway Load Balancing Protocol	12.2(14)S 12.2(15)T	GLBP は、冗長化されたルータ グループ間でパケットのロード シェアリングを行う一方、機能を停止したルータや回路（HSRP や VRRP など）からのデータ トラフィックを保護します。 このコンフィギュレーション モジュールのすべての項では、この機能についての情報を提供します。 この機能により、次のコマンドが導入または変更されました。**glbp forwarder preempt**、**glbp ip**、**glbp load-balancing**、**glbp name**、**glbp preempt**、**glbp priority**、**glbp sso**、**glbp timers**、**glbp timers redirect**、**glbp weighting**、**glbp weighting track**、**show glbp**。

表 1　GLBP の機能情報 （続き）

機能名	リリース	機能設定情報
GLBP クライアント キャッシュ	12.4(15)T 12.2(33)SXI	GLBP クライアント キャッシュには、GLBP グループをデフォルト ゲートウェイとして使用しているネットワーク ホストに関する情報が含まれています。 GLBP クライアント キャッシュには、特定の GLBP グループを使用する各ホストの MAC アドレス、各ネットワーク ホストに割り当てられている GLBP フォワーダの数、GLBP グループの各フォワーダに現在割り当てられているネットワーク ホストの総数が格納されます。また、各ネットワーク ホストによって使用されるプロトコル アドレス、ホストとフォワーダの割り当てが最後に更新されてから経過した時間も格納されます。 この機能に関する詳細については、次の各項を参照してください。 • 「GLBP クライアント キャッシュ」（P.5） • 「GLBP のカスタマイズ」（P.10） **glbp client-cache maximum** および **show glbp** の各コマンドがこの機能により導入または変更されました。
GLBP MD5 認証	12.2(18)S 12.3(2)T 12.2(33)SXH	MD5 認証は、代替となるプレーン テキスト認証スキームよりも高いセキュリティを実現します。MD5 認証を使用すると、各 GLBP グループ メンバが秘密鍵を使用して、発信パケットの一部である鍵付き MD5 ハッシュを生成できます。着信パケットの鍵付きハッシュが生成されると、生成されたハッシュと着信パケット内のハッシュが一致しない場合、パケットは無視されます。 この機能に関する詳細については、次の項を参照してください。 • 「GLBP 認証の設定」（P.13） **glbp authentication** および **show glbp** の各コマンドがこの機能により変更されました。

表 1　GLBP の機能情報 （続き）

機能名	リリース	機能設定情報
ISSU と GLBP	12.2(31)SB2 12.2(33)SRB1	GLBP は In Service Software Upgrade（ISSU; インサービス ソフトウェア アップグレード）をサポートします。ISSU を使用すると、アクティブおよびスタンバイの Route Processor（RP; ルート プロセッサ）またはライン カード上で異なるバージョンの Cisco IOS ソフトウェアが実行されている場合でも、ハイアベイラビリティ（HA）システムをステートフル スイッチオーバー（SSO）モードで実行できるようになります。 この機能は、ソフトウェア アップグレード中に予定されたシステム停止中も同じレベルの HA 機能を提供します。不測のシステム停止が発生した場合も、SSO を使用できます。つまり、システムをセカンダリ RP に切り替えることができ、セッションを切断することなく、またパケットの損失も最小限に抑えながら、継続してパケットを転送できます。 この機能は、デフォルトでイネーブルにされています。 この機能に関する詳細については、次の各項を参照してください。 • 「ISSU と GLBP」（P.6） この機能により、新規追加または変更されたコマンドはありません。
SSO：GLBP	12.2(31)SB2 12.2(33)SRB 12.2(33)SXH	GLBP が SSO を認識するようになりました。GLBP は、ルータがセカンダリ RP にフェールオーバーしたことを検出し、GLBP グループの現在の状態を継続することができます。 2 番目の RP がインストールされ、プライマリ RP が機能を停止した場合にはその処理を引き継ぐように設定されても、SSO を認識する前であるときは GLBP はこれを認識できません。プライマリが機能を停止すると、GLBP デバイスは GLBP グループに参加しなくなります。また、そのロールに応じて、グループ内の他のルータにアクティブ ルータとしてのロールが引き継がれます。このように機能が強化され、GLBP がセカンダリ RP に対するフェールオーバーを検出できるようになったため、GLBP グループに何ら変化は生じません。セカンダリ RP が機能を停止した場合、プライマリ RP が以前として利用できない状態であると、GLBP グループはこの状態を検出して新たなアクティブ GLBP ルータを再度選定します。 この機能は、デフォルトでイネーブルにされています。 この機能に関する詳細については、次の各項を参照してください。 • 「GLBP SSO」（P.7） • 「GLBP のカスタマイズ」（P.10） **debug glbp events**、**glbp sso**、**show glbp** の各コマンドがこの機能により導入または変更されました。

用語集

AVF：Active Virtual Forwarder（アクティブ バーチャル フォワーダ）。GLBP グループ内の 1 つのバーチャル フォワーダが、指定のバーチャル MAC アドレスのアクティブ バーチャル フォワーダとして選定されます。選定されたフォワーダは、指定の MAC アドレスに対するパケットの転送を処理します。1 つの GLBP グループに複数のアクティブ バーチャル フォワーダを存在させることができます。

AVG：Active Virtual Gateway（アクティブ バーチャル ゲートウェイ）。GLBP グループ内の 1 つのバーチャル ゲートウェイが、アクティブ バーチャル ゲートウェイとして選定されます。選定されたゲートウェイは、プロトコル動作を処理します。

GLBP グループ：Gateway Load Balancing Protocol グループ。接続されたイーサネット インターフェイス上で同じ GLBP グループ番号を持つ、1 つまたは複数の GLBP ゲートウェイ。

GLBP ゲートウェイ：Gateway Load Balancing Protocol ゲートウェイ。GLBP を実行するルータまたはゲートウェイ。各 GLBP ゲートウェイは、1 つまたは複数の GLBP グループに参加できます。

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

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

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

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

RPR+：RPR の拡張。スタンバイ RP が完全に初期化されます。

SSO：Stateful Switchover（ステートフル スイッチオーバー）。アクティブ装置とスタンバイ装置間のステート情報を保持するためのアプリケーションおよび機能をイネーブルにします。

vIP：バーチャル IP アドレス。IPv4 アドレス。設定された各 GLBP グループには、必ず 1 つのバーチャル IP アドレスがあります。バーチャル IP アドレスは、少なくとも 1 つの GLBP グループ メンバに設定する必要があります。他の GLBP グループ メンバは、Hello メッセージを通してバーチャル IP アドレスを学習します。

アクティブ RP：Route Processor（RP; ルート プロセッサ）はシステムの制御、ネットワーク サービスの提供、ルーティング プロトコルの実行、システム管理インターフェイスの有効化を実行します。

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

スタンバイ RP：完全に初期化され、アクティブ RP から制御を引き受ける準備が整った RP。手動または機能停止によってスイッチオーバーが発生します。

チェックポインティング：クライアント固有のステート データを保存または同期する処理。このデータは、冗長性のあるスイッチオーバーを実現するため、リモートのピア クライアントに転送されます。また、プロセスを再開始するため、ローカル ルータに転送されます。有効なチェックポインティング セッションが確立すると、チェックポイントされたステート データは順番に破損のない状態でリモートのピア クライアントに配信されることが保証されます。