VRRP の設定

Virtual Router Redundancy Protocol（VRRP; 仮想ルータ冗長プロトコル）は、LAN 上の VRRP ルータに対し、1 台または複数台の仮想ルータの役割をダイナミックに割り当てる選択プロトコルです。この場合、マルチアクセス リンク上にある何台かのルータが同じバーチャル IP アドレスを使用できるようにします。VRRP ルータは、LAN に接続されている 1 台以上の他のルータと連動して VRRP プロトコルを実行するように設定されます。VRRP 設定では、1 台のルータが仮想ルータ マスターとして選定され、他のルータは仮想ルータ マスターが機能を停止した場合のバックアップとして動作します。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。この章に記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「VRRP の機能情報」（P.27）を参照してください。

プラットフォーム サポートと 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

VRRP の制約事項

- VRRP は、マルチアクセス、マルチキャスト、またはブロードキャストに対応したイーサネット LAN 上で使用できるように設計されています。VRRP は既存のダイナミック プロトコルの代替にはなりません。
- VRRP は、イーサネット、ファスト イーサネット、Bridge Group Virtual Interface（BVI）、およびギガビット イーサネット インターフェイス、Multiprotocol Label Switching（MPLS; マルチプロトコル ラベル スイッチング）Virtual Private Network（VPN; バーチャル プライベート ネットワーク）、VRF を認識する MPLS VPN、および VLAN 上でサポートされます。
- BVI インターフェイスの初期化に関連して転送遅延が発生するため、VRRP アドバタイズ タイマーの時間は BVI インターフェイスでの転送遅延時間と同じにするか、または長く設定する必要があります。このように設定することで、最近初期化された BVI インターフェイス上にある VRRP ルータが無条件にマスター ロールを引き継ぐことがなくなります。BVI インターフェイスでの転送遅延を設定するには、**bridge forward-time** コマンドを使用します。VRRP アドバタイズメント タイマーを設定するには、**vrrp timers advertise** コマンドを使用します。
- Enhanced Object Tracking（EOT; 拡張オブジェクト トラッキング）はステートフル スイッチオーバー（SSO）を認識しないため、SSO モードで VRRP と併用することはできません。

VRRP について

VRRP を設定する前に、次の概念を理解しておく必要があります。

VRRP の動作

LAN クライアントが特定のリモート宛先に対してファーストホップとなるルータを決定する場合、いくつかの方法があります。クライアントは、ダイナミック プロセスまたはスタティック設定を使用できます。次に、ダイナミックなルータ検出の例を示します。

- プロキシ ARP：クライアントは Address Resolution Protocol（ARP; アドレス解決プロトコル）を使用して到達先の宛先を取得します。ルータは自分の MAC アドレスを使用して ARP 要求に応答します。
- ルーティング プロトコル：クライアントは、（たとえば、Routing Information Protocol（RIP）からの）ダイナミック ルーティング プロトコル アップデートをリスンし、独自にルーティング テーブルを作成します。
- IRDP（ICMP Router Discovery Protocol）クライアント：このクライアントは Internet Control Message Protocol（ICMP; インターネット制御メッセージ プロトコル）ルータ検出クライアントを実行します。

ダイナミック ディスカバリ プロトコルの欠点として、LAN クライアントで多少の設定が必要となることと、処理のオーバーヘッドが生じることが挙げられます。また、ルータが機能を停止した場合、他のルータへの切り替えを行うプロセスに時間がかかることがあります。

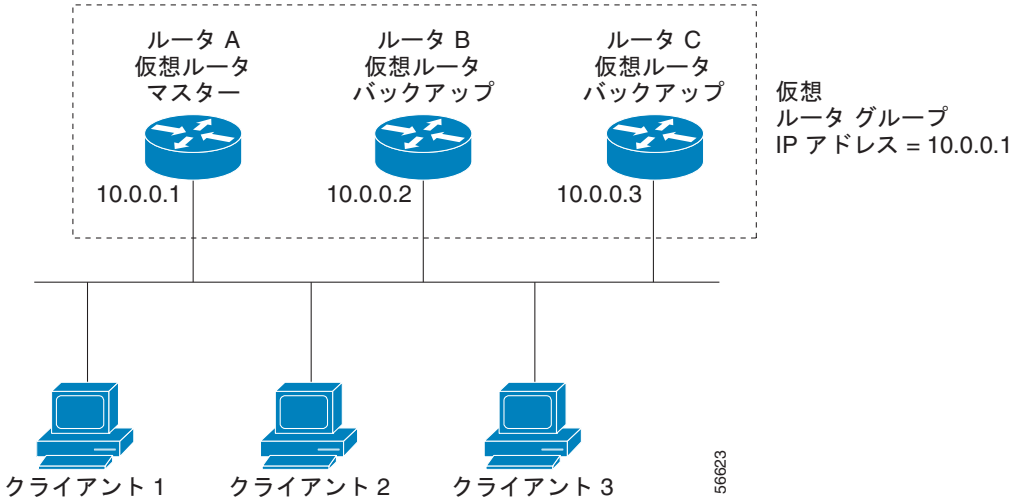
ダイナミック ディスカバリ プロトコルの代替方法として、クライアント上でデフォルト ルータをスタティックに設定する方法があります。このアプローチでは、クライアントの設定と処理は簡略化されますが、単一障害点が生じます。デフォルト ゲートウェイが機能を停止すると、LAN クライアントが通信できるのはローカル IP ネットワーク セグメントだけに制限され、残りのネットワークからは切断されます。

VRRP を使用すると、スタティックな設定の問題は解消されます。VRRP は、ルータのグループを使用して単一の*仮想ルータ*を形成します。これにより、仮想ルータをデフォルト ゲートウェイとして使用するように、LAN クライアントを設定できます。ルータのグループを表す仮想ルータは、「VRRP グループ」とも呼ばれます。

VRRP は、イーサネット、ファスト イーサネット、BVI、およびギガビット イーサネット インターフェイス、MPLS VPN、VRF を認識する MPLS VPN、および VLAN 上でサポートされます。

図 1 に、VRRP が設定された LAN トポロジを示します。この例では、ルータ A、B、および C は仮想ルータで構成される *VRRP ルータ*（VRRP を実行するルータ）です。仮想ルータの IP アドレスは、ルータ A のイーサネット インターフェイスに設定されたアドレス（10.0.0.1）と同じです。

図 1　　VRRP の基本トポロジ

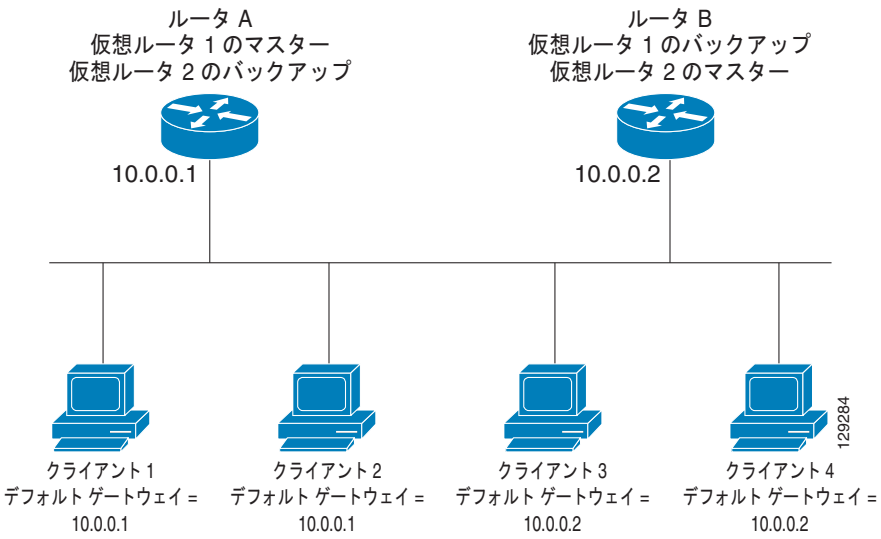


仮想ルータはルータ A の物理イーサネット インターフェイスの IP アドレスを使用するため、ルータ A は*仮想ルータ マスター*のロールを担い、「*IP アドレス所有者*」とも呼ばれます。ルータ A は、仮想ルータ マスターとして、仮想ルータの IP アドレスを管理し、この IP アドレスに送信されたパケットの転送を行います。クライアント 1 ～ 3 はデフォルト ゲートウェイ IP アドレス（10.0.0.1）を使用して設定されます。

ルータ B とルータ C は*仮想ルータ バックアップ*として機能します。仮想ルータ マスターが機能を停止すると、高いプライオリティに設定されているルータが仮想ルータ マスターとなり、LAN ホストには継続してサービスが提供されます。ルータ A が回復すると、ルータ A が再び仮想ルータ マスターになります。VRRP ルータが果たすロールと、仮想ルータ マスターが機能を停止したときにどのようなことが起こるかについての詳細は、このドキュメント内の「VRRP ルータ プライオリティとプリエンプション」を参照してください。

図 2 に示す LAN トポロジでは、ルータ A とルータ B がクライアント 1 ～ 4 のトラフィックを共有し、ルータ A とルータ B がいずれかのルータが機能を停止したときに相互に仮想ルータ バックアップとして機能するように VRRP が設定されています。

図 2　　ロード シェアリングと冗長化が設定された VRRP トポロジ



このトポロジでは、2 つの仮想ルータが設定されています（詳細については、このドキュメント内の「複数の仮想ルータのサポート」を参照してください）。仮想ルータ 1 では、ルータ A が IP アドレス 10.0.0.1 の所有者で、仮想ルータ マスターになっています。ルータ B はルータ A に対する仮想ルータ バックアップです。クライアント 1 と クライアント 2 はデフォルト ゲートウェイ IP アドレス（10.0.0.1）を使用して設定されています。

仮想ルータ 2 では、ルータ B が IP アドレス 10.0.0.2 の所有者で、仮想ルータ マスターになっています。ルータ A はルータ B に対する仮想ルータ バックアップです。クライアント 3 と クライアント 4 はデフォルト ゲートウェイ IP アドレス（10.0.0.2）を使用して設定されています。

VRRP の利点

冗長性

VRRP により、複数のルータをデフォルト ゲートウェイ ルータとして設定できるようになり、ネットワークに単一障害点が生じる可能性を低減できます。

ロード シェアリング

LAN クライアントとの間のトラフィックを複数のルータで共有するように VRRP を設定できるため、利用可能なルータ間でより均等にトラフィックの負荷を分散できます。

複数の仮想ルータ

プラットフォームが複数の MAC アドレスをサポートする場合、VRRP はルータの物理インターフェイス上で最大 255 の仮想ルータ（VRRP グループ）をサポートします。複数の仮想ルータをサポートすることで、LAN トポロジ内で冗長化とロード シェアリングを実装できます。

複数の IP アドレス

仮想ルータは、セカンダリ IP アドレスを含め複数の IP アドレスを管理できます。そのため、イーサネット インターフェイスに複数のサブネットを設定した場合、サブネットごとに VRRP を設定できます。

プリエンプション

VRRP の冗長性スキームにより、仮想ルータ バックアップのプリエンプトが可能になり、より高いプライオリティが設定された仮想ルータ バックアップが、機能を停止した仮想ルータ マスターを引き継ぐようにできます。

認証

VRRP の Message Digest 5（MD5; メッセージ ダイジェスト 5）アルゴリズム認証は、VRRP スプーフィング ソフトウェアから保護し、業界標準の MD5 アルゴリズムを使用して、信頼性とセキュリティを高めます。

アドバタイズメント プロトコル

VRRP は専用の Internet Assigned Numbers Authority（IANA）標準マルチキャスト アドレス（224.0.0.18）を使用して VRRP アドバタイズメントを行います。このアドレッシング方式により、マルチキャストにサービスを提供しなければならないルータの数を最小限に抑え、テスト装置がセグメントの VRRP パケットを正確に特定できるようになります。IANA は VRRP に IP プロトコル番号 112 を割り当てました。

VRRP オブジェクト トラッキング

VRRP オブジェクト トラッキングにより、インターフェイスや IP ルート ステートなどの追跡対象オブジェクトのステータスに応じて VRRP プライオリティを変更することで、最適な VRRP ルータがグループの仮想ルータ マスターになります。

複数の仮想ルータのサポート

ルータの物理インターフェイスには、最大 255 の仮想ルータを設定できます。ルータ インターフェイスがサポートできる実際の仮想ルータの数は、次の要因によって決定されます。

- ルータの処理機能
- ルータのメモリ機能
- 複数の MAC アドレスのルータ インターフェイス サポート

1 つのルータ インターフェイス上に複数の仮想ルータが設定されているトポロジでは、インターフェイスは 1 つの仮想ルータにはマスターとして動作し、1 つまたは複数の仮想ルータにはバックアップとして動作することができます。

VRRP ルータ プライオリティとプリエンプション

VRRP 冗長性スキームの重要な一面に、ルータ プライオリティがあります。プライオリティにより、各 VRRP ルータが果たすロールと、仮想ルータ マスターが機能を停止したときにどのようなことが起こるかが決定されます。

ある VRRP ルータが仮想ルータの IP アドレスと物理インターフェイスの IP アドレスを所有している場合、このルータが仮想ルータ マスターとして機能します。

VRRP ルータが仮想ルータ バックアップとして機能するかどうかや、仮想ルータ マスターが機能を停止した場合に仮想ルータ マスターを引き継ぐ順序も、プライオリティによって決定されます。**vrrp priority** コマンドを使用して 1 ～ 254 の値を設定し、各仮想ルータ バックアップのプライオリティを設定できます。

たとえば、ルータ A（LAN トポロジの仮想ルータ マスター）が機能を停止した場合、選択プロセスが行われ、仮想ルータ バックアップ B と C のどちらが引き継ぐかが決定されます。ルータ B とルータ C がそれぞれ プライオリティ 101 と 100 に設定されている場合、プライオリティの高いルータ B が仮想ルータ マスターになります。ルータ B とルータ C が両方ともプライオリティ 100 に設定されている場合、IP アドレスが高い方の仮想ルータ バックアップが選択されて仮想ルータ マスターになります。

デフォルトでは、プリエンプティブ スキームはイネーブルになっています。この場合、仮想ルータ マスターになるように選択されている仮想ルータ バックアップの中で、より高いプライオリティが設定されている仮想ルータ バックアップが仮想ルータ マスターになります。このプリエンプティブ スキームをディセーブルにするには、**no vrrp preempt** コマンドを使用します。プリエンプションがディセーブルになっている場合は、元の仮想ルータ マスターが回復して再びマスターになるまで、仮想ルータ マスターになるように選択されている仮想ルータ バックアップがマスターのロールを果たします。

VRRP アドバタイズメント

仮想ルータ マスターは、同じグループ内の他の VRRP ルータに VRRP アドバタイズメントを送信します。アドバタイズメントでは、仮想ルータ マスターのプライオリティとステートを伝えます。VRRP アドバタイズメントは IP パケットにカプセル化され、VRRP グループに割り当てられた IP バージョン 4 マルチキャスト アドレスに送信されます。アドバタイズメントは、デフォルトで 1 秒に 1 回送信されますが、この間隔は設定可能です。

VRRP オブジェクト トラッキング

オブジェクト トラッキングは、インターフェイス ライン プロトコルのステートなど、追跡対象オブジェクトの作成、モニタ、削除を管理する独立したプロセスです。Hot Standby Router Protocol（HSRP; ホット スタンバイ ルータ プロトコル）、Gateway Load Balancing Protocol（GLBP; ゲートウェイ ロード バランシング プロトコル）、そして VRRP のようなクライアントは、追跡対象オブジェクトを登録し、オブジェクトのステートが変更されたときにアクションを実行できます。

各追跡対象オブジェクトには、トラッキング CLI（コマンドライン インターフェイス）で指定される一意の番号があります。VRRP などのクライアント プロセスは、この番号を使用して特定のオブジェクトを追跡します。

トラッキング プロセスは、追跡対象オブジェクトを定期的にポーリングし、値に変化がないかどうかを確認します。追跡対象オブジェクトに変化があれば登録されているクライアント プロセスに通知します。ただちに通知する場合と、指定された時間遅延後に通知する場合があります。オブジェクトの値は、アップまたはダウンとして報告されます。

VRRP オブジェクト トラッキングにより、VRRP はトラッキング プロセスで追跡可能なすべてのオブジェクトにアクセスします。トラッキング プロセスでは、インターフェイス ライン プロトコルのステート、IP ルートのステート、ルートの到達可能性など、オブジェクトを個別に追跡する機能が提供されます。

VRRP はトラッキング プロセスに対するインターフェイスを提供します。VRRP グループごとに、VRRP ルータのプライオリティに影響を及ぼす可能性のある複数のオブジェクトを追跡できます。追跡対象のオブジェクト番号を指定すると、そのオブジェクトに何らかの変更が生じた場合に VRRP によって通知されます。VRRP は、追跡対象オブジェクトのステートに基づいて、仮想ルータのプライオリティを増加（または減少）させます。

ISSU と VRRP

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

ISSU を使用すると、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できます。この場合、パケット転送は継続して行われ、セッションは維持されるため、予定されるシステムの停止時間を短くすることができます。アップグレードまたはダウングレードする機能は、アクティブ RP およびスタンバイ RP 上で異なるバージョンのソフトウェアを実行することで実現します。これにより、RP 間でステート情報を維持する時間が短くなります。この機能により、システムをアップグレード対象（またはダウングレード対象）のソフトウェアを実行するセカンダリ RP に切り替えることができ、セッションを切断することなく、またパケットの損失も最小限に抑えながら、継続してパケットを転送できます。この機能は、デフォルトでイネーブルにされています。

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

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

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

http://www.cisco.com/en/US/partner/products/hw/routers/ps368/products_configuration_guide_chapter09186a00807f1c85.html

SSO と VRRP

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

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

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

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

詳細については、次の URL に掲載されている『*Stateful Switchover*』を参照してください。

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

VRRP の設定方法

ここでは、次の各手順について説明します。

- 「VRRP のカスタマイズ」（P.8）（任意）
- 「VRRP のイネーブル化」（P.10）（必須）
- 「インターフェイスでの VRRP のディセーブル化」（P.11）（任意）
- 「VRRP オブジェクト トラッキングの設定」（P.12）（任意）
- 「VRRP 認証の設定」（P.14）（任意）
- 「SNMP VRRP 通知を送信するようにルータをイネーブル化」（P.20）（任意）

VRRP のカスタマイズ

VRRP をカスタマイズするには、次の手順を実行します。

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

オブジェクト トラッキングが VRRP ルータのプライオリティに及ぼす影響

オブジェクト トラッキングが設定されている場合に、追跡対象のオブジェクトがダウンすると、デバイスのプライオリティはダイナミックに変化します。トラッキング プロセスは、追跡対象オブジェクトを定期的にポーリングし、値に変化がないかどうかを確認します。追跡対象オブジェクトに変化があれば VRRP に通知します。ただちに通知する場合と、指定された時間遅延後に通知する場合があります。オブジェクトの値は、アップまたはダウンとして報告されます。インターフェイスのライン プロトコル ステートと IP ルートの到達可能性が追跡されるオブジェクトの例を示します。対象のオブジェクトがダウンすると、VRRP プライオリティは減じられます。その場合、**vrrp preempt** コマンドが設定されていると、より高いプライオリティが設定された VRRP ルータが仮想ルータ マスターになります。オブジェクト トラッキングの詳細については、「VRRP オブジェクト トラッキング」を参照してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip address** *ip-address mask*
5. **vrrp** *group* **description** *text*
6. **vrrp** *group* **priority** *level*
7. **vrrp** *group* **preempt** [**delay minimum** *seconds*]
8. **vrrp** *group* **timers advertise** [**msec**] *interval*
9. **vrrp** *group* **timers learn**
10. **no vrrp sso**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* 例： `Router(config)# interface ethernet 0`	インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ip address** *ip-address mask* 例： `Router(config-if)# ip address 172.16.6.5 255.255.255.0`	インターフェイスの IP アドレスを設定します。
ステップ 5	**vrrp** *group* **description** *text* 例： `Router(config-if)# vrrp 10 description working-group`	VRRP グループに説明テキストを割り当てます。
ステップ 6	**vrrp** *group* **priority** *level* 例： `Router(config-if)# vrrp 10 priority 110`	VRRP グループ内のルータのプライオリティ レベルを設定します。 • デフォルトのプライオリティは 100 です。
ステップ 7	**vrrp** *group* **preempt** [**delay minimum** *seconds*] 例： `Router(config-if)# vrrp 10 preempt delay minimum 380`	現在の仮想ルータ マスターよりも高いプライオリティが設定されている場合、VRRP グループの仮想ルータ マスターとして引き継ぐルータを指定します。 • デフォルトの遅延時間は 0 秒です。 • このコマンドの設定にかかわらず、IP アドレスの所有者であるルータがプリエンプトします。
ステップ 8	**vrrp** *group* **timers advertise** [**msec**] *interval* 例： `Router(config-if)# vrrp 10 timers advertise 110`	VRRP グループの仮想ルータ マスターが行う、連続したアドバタイズ インターバルを設定します。 • 間隔の単位は、**msec** キーワードが指定された場合を除き、「秒」です。デフォルトの *interval* 値は 1 秒です。 **（注）** VRRP グループ内のすべてのルータが同じタイマー値を使用する必要があります。同じタイマー値が設定されていないと、VRRP グループ内のルータが相互通信せず、正しく設定されていないルータのステートがマスターに変わります。

	コマンドまたはアクション	目的
ステップ 9	**vrrp** *group* **timers learn** 例： `Router(config-if)# vrrp 10 timers learn`	ルータが VRRP グループの仮想ルータ バックアップとして動作している場合、仮想ルータ マスターのアドバタイズ インターバルを学習するようにルータを設定します。
ステップ 10	**no vrrp sso** 例： `Router(config)# no vrrp sso`	（任意）SSO の VRRP サポートをディセーブルにします。SSO の VRRP サポートはデフォルトでイネーブルになっています。

VRRP のイネーブル化

VRRP をイネーブルにするには、次の手順を実行します。

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* 例： `Router(config)# interface ethernet 0`	インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ip address** *ip-address mask* 例： `Router(config-if)# ip address 172.16.6.5 255.255.255.0`	インターフェイスの IP アドレスを設定します。

	コマンドまたはアクション	目的
ステップ 5	**vrrp** *group* **ip** *ip-address* [**secondary**] **例：** `Router(config-if)# vrrp 10 ip 172.16.6.1`	インターフェイスの VRRP をイネーブルにします。 • プライマリ IP アドレスを指定した後、**secondary** キーワードを指定して **vrrp ip** コマンドをもう一度使用すれば、このグループでサポートする追加の IP アドレスを指定できます。 **（注）** VRRP グループ内のすべてのルータには、同じプライマリ アドレスと、仮想ルータで一致するセカンダリ アドレスのリストを設定する必要があります。プライマリ アドレスまたはセカンダリ アドレスに異なるアドレスを設定すると、VRRP グループ内のルータが相互通信せず、正しく設定されていないルータのステートがマスターに変わります。
ステップ 6	**end** **例：** `Router(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 7	`Router#` **show vrrp** [**brief** | *group*] **例：** `Router# show vrrp 10`	（任意）ルータのいずれかまたはすべての VRRP グループについて、簡易なまたは詳細なステータスを表示します。
ステップ 8	`Router#` **show vrrp interface** *type number* [**brief**] **例：** `Router# show vrrp interface ethernet 0`	（任意）指定インターフェイスの VRRP グループおよびそのステータスを表示します。

インターフェイスでの VRRP のディセーブル化

インターフェイスで VRRP をディセーブルにすると、プロトコルをディセーブルにできますが、設定は維持されます。この機能は、VRRP MIB、RFC 2787「*Definitions of Managed Objects for the Virtual Router Redundancy Protocol*」の導入とともに追加されました。

Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）管理ツールを使用して、インターフェイスでの VRRP をイネーブルまたはディセーブルに設定できます。SNMP 管理機能により、**vrrp shutdown** コマンドが導入され、SNMP を使用して設定されたステートが VRRP の CLI を通して表示されるようになりました。

show running-config コマンドを入力すると、VRRP グループが設定されているかどうか、およびイネーブルとディセーブルのどちらに設定されているかをすぐに確認できます。これは、MIB 内でイネーブルされるのと同じ機能です。

このコマンドを **no** 形式で使用すると、MIB 内で実行される同じ動作がイネーブルになります。SNMP インターフェイスを使用して **vrrp shutdown** コマンドを指定した場合、Cisco IOS CLI を使って **no vrrp shutdown** コマンドを入力すると、VRRP グループが再びイネーブルになります。

手順の概要

1. **enable**
2. **configure terminal**

3. **interface** *type number*
4. **ip address** *ip-address mask*
5. **vrrp** *group* **shutdown**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* 例： `Router(config)# interface ethernet 0`	インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ip address** *ip-address mask* 例： `Router(config-if)# ip address 172.16.6.5 255.255.255.0`	インターフェイスの IP アドレスを設定します。
ステップ 5	**vrrp** *group* **shutdown** 例： `Router(config-if)# vrrp 10 shutdown`	インターフェイスの VRRP をイネーブルにします。 • コマンドがルータに表示されるようになります。 **（注）** 設定を維持した状態で、1 つの VRRP グループをディセーブルにし、別の VRRP グループをイネーブルにできます。

VRRP オブジェクト トラッキングの設定

VRRP 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。

制約事項

VRRP グループが IP アドレス所有者である場合、そのプライオリティは 255 に固定され、オブジェクト トラッキングで減じることはできません。

手順の概要

1. **enable**
2. **configure terminal**
3. **track** *object-number* **interface** *type number* {**line-protocol** | **ip routing**}
4. **interface** *type number*
5. **vrrp** *group* **ip** *ip-address*

6. **vrrp** *group* **priority** *level*
7. **vrrp** *group* **track** *object-number* [**decrement** *priority*]
8. **end**
9. **show track** [*object-number*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**track** *object-number* **interface** *type number* {**line-protocol** | **ip routing**} 例： `Router(config)# track 2 interface serial 6 line-protocol`	インターフェイスを追跡し、インターフェイスのステートに変更が生じると VRRP グループのプライオリティに影響するように設定します。 • このコマンドを使って、**vrrp track** コマンドで使用されるインターフェイスおよび対応するオブジェクト番号を設定します。 • **line-protocol** キーワードを指定すると、インターフェイスがアップしているかどうかを追跡します。**ip routing** キーワードを指定すると、インターフェイス上で IP ルーティングがイネーブルになっていて、アクティブになっていることも確認します。 • **track IP route** コマンドを使用して、IP ルートまたはメトリック タイプのオブジェクトの到達可能性を追跡することもできます。
ステップ 4	**interface** *type number* 例： `Router(config)# interface Ethernet 2`	インターフェイス コンフィギュレーション モードを開始します。
ステップ 5	**vrrp** *group* **ip** *ip-address* 例： `Router(config-if)# vrrp 1 ip 10.0.1.20`	インターフェイス上で VRRP をイネーブルにし、仮想ルータのプライマリ IP アドレスを指定します。
ステップ 6	**vrrp** *group* **priority** *level* 例： `Router(config-if)# vrrp 1 priority 120`	VRRP グループ内のルータのプライオリティ レベルを設定します。
ステップ 7	**vrrp** *group* **track** *object-number* [**decrement** *priority*] 例： `Router(config-if)# vrrp 1 track 2 decrement 15`	オブジェクトを追跡するように VRRP を設定します。

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

VRRP 認証の設定

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

ここでは、VRRP 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 VRRP MD5 認証の設定」（P.15）
- 「キー チェーンを使用した VRRP MD5 認証の設定」（P.16）
- 「VRRP MD5 認証設定の確認」（P.18）
- 「VRRP テキスト認証の設定」（P.19）

VRRP 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 VRRP 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、その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、キー チェーンを通して間接的に指定することもできます。

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

- 認証なし
- プレーン テキスト認証
- MD5 認証

VRRP パケットは、次の場合はいずれも拒否されます。

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

制約事項

RFC 2338 方式を実装したベンダーとの相互運用性は、有効ではありません。

どのような場合でも、テキスト認証を MD5 認証と組み合わせて VRRP グループに使用することはできません。MD5 認証が設定されている場合、VRRP hello メッセージのテキスト認証のフィールドはすべてゼロ（0）に設定されて送信され、受信時には無視されます（受信側のルータでも MD5 認証が有効になっている場合）。

キー ストリングを使用した VRRP MD5 認証の設定

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

手順の概要

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

手順の詳細

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

	コマンド	目的
ステップ 6	**vrrp** *group* **authentication md5 key-string** [**0** | **7**] *key-string* [**timeout** *seconds*] **例：** `Router(config-if)# vrrp 1 authentication md5 key-string d00b4r987654321a timeout 30`	VRRP MD5 認証の認証文字列を設定します。 • *key* 引数には最大 64 文字を設定できます。16 文字以上を使用することを推奨します。 • *key* 引数にはプレフィクスを指定しません。**0** を指定すると、キーは暗号化されないことを示します。 • **7** を指定するとキーは暗号化されます。**service password-encryption** グローバル コンフィギュレーション コマンドがイネーブルになっていると、key-string 認証キーは自動的に暗号化されます。 • タイムアウト値は、古いキー ストリングが受け入れられ、新しいキーを使用してグループ内のすべてのルータを設定できる時間です。 **（注）** VRRP グループ内のすべてのルータは、同じ認証文字列を使用して設定する必要があります。同じ認証文字列が設定されていないと、VRRP グループ内のルータが相互通信せず、正しく設定されていないいずれかのルータのステートがマスターに変わります。
ステップ 7	**vrrp** *group* **ip** [*ip-address* [**secondary**]] **例：** `Router(config-if)# vrrp 1 ip 10.0.0.3`	インターフェイス上で VRRP をイネーブルにし、仮想ルータのプライマリ IP アドレスを指定します。
ステップ 8	通信を行う各ルータ上でステップ 1 ～ 7 を繰り返します。	—
ステップ 9	**end** **例：** `Router(config-if)# end`	特権 EXEC モードに戻ります。

キー チェーンを使用した VRRP MD5 認証の設定

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

手順の概要

1. **enable**
2. **configure terminal**
3. **key chain** *name-of-chain*
4. **key** *key-id*
5. **key-string** *string*
6. **exit**

7. **interface** *type number*
8. **ip address** *ip-address mask* [**secondary**]
9. **vrrp** *group* **priority** *priority*
10. **vrrp** *group* **authentication md5 key-chain** *key-chain*
11. **vrrp** *group* **ip** [*ip-address* [**secondary**]]
12. 通信を行う各ルータ上でステップ 1 ～ 11 を繰り返します。
13. **end**

手順の詳細

	コマンド	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**key chain** *name-of-chain* 例： `Router(config)# key chain vrrp1`	ルーティング プロトコルの認証をイネーブルにし、認証キーのグループを識別します。
ステップ 4	**key** *key-id* 例： `Router(config-keychain)# key 100`	キー チェーンの認証キーを識別します。 • *key-id* は、数値で指定する必要があります。
ステップ 5	**key-string** *string* 例： `Router(config-keychain-key)# key-string mno172`	キーの認証文字列を指定します。 • *string* には、1 ～ 80 文字の大文字と小文字の英数字を指定できます。ただし、最初の文字を数値にすることはできません。
ステップ 6	**exit** 例： `Router(config-keychain-key)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 7	**interface** *type number* 例： `Router(config)# interface Ethernet0/1`	インターフェイス タイプを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 8	**ip address** *ip-address mask* [**secondary**] 例： `Router(config-if)# ip address 10.21.8.32 255.255.255.0`	インターフェイスのプライマリ IP アドレスまたはセカンダリ IP アドレスを指定します。
ステップ 9	**vrrp** *group* **priority** *priority* 例： `Router(config-if)# vrrp 1 priority 110`	VRRP プライオリティを設定します。

	コマンド	目的
ステップ 10	**vrrp** *group* **authentication md5 key-chain** *key-chain* 例： `Router(config-if)# vrrp 1 authentication md5 key-chain vrrp1`	VRRP MD5 認証の認証 MD5 キー チェーンを設定します。 • キー チェーン名は、ステップ 3 で指定した名前と一致する必要があります。 （注） VRRP グループ内のすべてのルータは、同じ認証文字列を使用して設定する必要があります。同じ認証文字列が設定されていないと、VRRP グループ内のルータが相互通信せず、正しく設定されていないいずれかのルータのステートがマスターに変わります。
ステップ 11	**vrrp** *group* **ip** [*ip-address* [**secondary**]] 例： `Router(config-if)# vrrp 1 ip 10.21.8.12`	インターフェイス上で VRRP をイネーブルにし、仮想ルータのプライマリ IP アドレスを指定します。
ステップ 12	通信を行う各ルータ上でステップ 1 ～ 11 を繰り返します。	—
ステップ 13	**end** 例： `Router(config-if)# end`	特権 EXEC モードに戻ります。

VRRP MD5 認証設定の確認

MD5 認証設定を確認するには、次の手順を実行します。

手順の概要

1. **show vrrp**
2. **debug vrrp authentication**

手順の詳細

ステップ 1 **show vrrp**

このコマンドを使用して、認証が正しく設定されていることを確認します。

```
Router# show vrrp

Ethernet0/1 - Group 1
State is Master
Virtual IP address is 10.21.0.10
Virtual MAC address is 0000.5e00.0101
Advertisement interval is 1.000 sec
Preemption is enabled
 min delay is 0.000 sec
Priority is 100
  Authentication MD5, key-string, timeout 30 secs
Master Router is 10.21.0.1 (local), priority is 100
Master Advertisement interval is 1.000 sec
Master Down interval is 3.609 sec
```

出力には、MD5 認証が設定されていることと、f00d4s キー ストリングが使用されていることが表示されます。タイムアウト値は 30 秒に設定されます。

ステップ 2　debug vrrp authentication

このコマンドを使用して、両方のルータに認証が設定されていること、各 ルータの MD5 キー ID が同じであること、各 ルータの MD5 キー ストリングが同じであることを確認します。

```
Router1#: debug vrrp authentication

VRRP: Sent: 21016401FE050000AC1801FE0000000000000000
VRRP: HshC: B861CBF1B9026130DD34AED849BEC8A1

VRRP: Rcvd: 21016401FE050000AC1801FE0000000000000000
VRRP: HshC: B861CBF1B9026130DD34AED849BEC8A1
VRRP: HshR: C5E193C6D84533FDC750F85FCFB051E1
VRRP: Grp 1 Adv from 172.24.1.2 has failed MD5 auth

Router2#: debug vrrp authentication

VRRP: Sent: 21016401FE050000AC1801FE0000000000000000
VRRP: HshC: C5E193C6D84533FDC750F85FCFB051E1

VRRP: Rcvd: 21016401FE050000AC1801FE0000000000000000
VRRP: HshC: C5E193C6D84533FDC750F85FCFB051E1
VRRP: HshR: B861CBF1B9026130DD34AED849BEC8A1
VRRP: Grp 1 Adv from 172.24.1.1 has failed MD5 auth
```

VRRP テキスト認証の設定

VRRP テキスト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. **vrrp** *group* **authentication text** *text-string*
6. **vrrp** *group* **ip** *ip-address*
7. 通信を行う各ルータ上でステップ 1 ～ 6 を繰り返します。
8. **end**

手順の詳細

	コマンド	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードなど、高位の権限レベルをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* **例：** `Router(config)# interface Ethernet0/1`	インターフェイス タイプを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ip address** *ip-address mask* [**secondary**] **例：** `Router(config-if)# ip address 10.0.0.1 255.255.255.0`	インターフェイスのプライマリ IP アドレスまたはセカンダリ IP アドレスを指定します。
ステップ 5	**vrrp** *group* **authentication text** *text-string* **例：** `Router(config-if)# vrrp 1 authentication text textstring1`	グループ内の他のルータから受信した VRRP パケットを認証します。 • 認証を設定する場合、VRRP グループ内のすべてのルータで同じ認証文字列を使用する必要があります。 • デフォルトの文字列は「cisco」です。 **（注）** VRRP グループ内のすべてのルータは、同じ認証文字列を使用して設定する必要があります。同じ認証文字列が設定されていないと、VRRP グループ内のルータが相互通信せず、正しく設定されていないいずれかのルータのステートがマスターに変わります。
ステップ 6	**vrrp** *group* **ip** *ip-address* **例：** `Router(config-if)# vrrp 1 ip 10.0.1.20`	インターフェイス上で VRRP をイネーブルにし、仮想ルータのプライマリ IP アドレスを指定します。
ステップ 7	通信を行う各ルータ上でステップ 1 ～ 6 を繰り返します。	—
ステップ 8	**end** **例：** `Router(config-if)# end`	特権 EXEC モードに戻ります。

SNMP VRRP 通知を送信するようにルータをイネーブル化

VRRP MIB は、SNMP GET 操作をサポートします。この操作により、ネットワーク デバイスがネットワーク管理ステーションからネットワークの VRRP グループについてのレポートを受け取ることができるようになります。

VRRP MIB トラップ サポートを有効にする操作は、CLI から行います。そして、MIB を使用してレポートを取得します。あるルータがマスターまたはバックアップ ルータになると、トラップがネットワーク管理ステーションに通知します。CLI からエントリを設定すると、直ちに、MIB でのそのグループの RowStatus がアクティブ ステートになります。

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**snmp-server enable traps vrrp** 例： `Router(config)# snmp-server enable traps vrrp`	SNMP VRRP 通知（トラップおよび応答要求）を送信するように、ルータを設定します。
ステップ 4	**snmp-server host** *host community-string* **vrrp** 例： `Router(config)# snmp-server host myhost.comp.com public vrrp`	SNMP 通知動作の指定

VRRP の設定例

ここでは、次の設定例について説明します。

VRRP の設定：例

次の例では、ルータ A とルータ B はそれぞれ 3 つの VRRP グループに属しています。

各グループには次のプロパティが設定されています。

- グループ 1：
  - バーチャル IP アドレスは 10.1.0.10 です。
  - ルータ A は、プライオリティが 120 のときにこのグループのマスターになります。
  - アドバタイズ インターバルは 3 秒です。
  - プリエンプションはイネーブルになっています。
- グループ 5：
  - ルータ B は、プライオリティが 200 のときにこのグループのマスターになります。
  - アドバタイズ インターバルは 30 秒です。
  - プリエンプションはイネーブルになっています。
- グループ 100：
  - ルータ A は、より高い IP アドレス（10.1.0.2）が設定されているため、最初にこのグループのマスターになります。
  - アドバタイズ インターバルはデフォルトで 1 秒に設定されます。
  - プリエンプションはディセーブルになっています。

ルータ A

```
interface ethernet 1/0
 ip address 10.1.0.2 255.0.0.0
 vrrp 1 priority 120
 vrrp 1 authentication cisco
 vrrp 1 timers advertise 3
 vrrp 1 timers learn
 vrrp 1 ip 10.1.0.10
 vrrp 5 priority 100
 vrrp 5 timers advertise 30
 vrrp 5 timers learn
 vrrp 5 ip 10.1.0.50
 vrrp 100 timers learn
 no vrrp 100 preempt
 vrrp 100 ip 10.1.0.100
 no shutdown
```

ルータ B

```
interface ethernet 1/0
 ip address 10.1.0.1 255.0.0.0
 vrrp 1 priority 100
 vrrp 1 authentication cisco
 vrrp 1 timers advertise 3
 vrrp 1 timers learn
 vrrp 1 ip 10.1.0.10
 vrrp 5 priority 200
 vrrp 5 timers advertise 30
 vrrp 5 timers learn
 vrrp 5 ip 10.1.0.50
 vrrp 100 timers learn
 no vrrp 100 preempt
```

```
 vrrp 100 ip 10.1.0.100
 no shutdown
```

VRRP オブジェクト トラッキング：例

次の例では、トラッキング プロセスはシリアル インターフェイス 0/1 上でライン プロトコルのステートを追跡するように設定されています。イーサネット インターフェイス 1/0 の VRRP は、シリアル インターフェイス 0/1 のライン プロトコル ステートに何らかの変更が生じた場合には通知されるように、トラッキング プロセスに登録します。シリアル インターフェイス 0/1 のライン プロトコル ステートがダウンになると、VRRP グループのプライオリティは 15 減じられます。

```
track 1 interface Serial0/1 line-protocol
!
interface Ethernet1/0
 ip address 10.0.0.2 255.0.0.0
 vrrp 1 ip 10.0.0.3
 vrrp 1 priority 120
 vrrp 1 track 1 decrement 15
```

VRRP オブジェクト トラッキングの検証：例

次に、「VRRP オブジェクト トラッキング：例」で説明した設定を確認する例を示します。

```
Router# show vrrp

Ethernet1/0 - Group 1
  State is Master
  Virtual IP address is 10.0.0.3
  Virtual MAC address is 0000.5e00.0101
  Advertisement interval is 1.000 sec
  Preemption is enabled
   min delay is 0.000 sec
  Priority is 105
   Track object 1 state Down decrement 15
  Master Router is 10.0.0.2 (local), priority is 105
  Master Advertisement interval is 1.000 sec
  Master Down interval is 3.531 sec

Router# show track

Track 1
  Interface Serial0/1 line-protocol
  Line protocol is Down (hw down)
   1 change, last change 00:06:53
  Tracked by:
   VRRP Ethernet1/0 1
```

キー ストリングを使用した VRRP MD5 認証の設定：例

次に、キー ストリングを使用して MD5 認証を設定し、タイムアウトを 30 秒に設定する例を示します。

```
interface Ethernet0/1
 description ed1-cat5a-7/10
 vrrp 1 ip 10.21.0.10
 vrrp 1 priority 110
 vrrp 1 authentication md5 key-string f00c4s timeout 30
 exit
```

キー チェーンを使用した VRRP MD5 認証の設定：例

次に、キー チェーンを使用して MD5 認証を設定する例を示します。

```
key chain vrrp1
 key 1
 key-string f00c4s
 exit
!
interface ethernet0/1
 description ed1-cat5a-7/10
 vrrp 1 priority 110
 vrrp 1 authentication md5 key-chain vrrp1
 vrrp 1 ip 10.21.0.10
```

この例では、VRRP はキー チェーンを照会し、特定のキー チェーンに対して現在アクティブになっているキーとキー ID を取得します。

VRRP テキスト認証：例

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

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

インターフェイスでの VRRP のディセーブル化：例

次に、イーサネット インターフェイス 0/2 上ではグループ 2 の VRRP を維持しながら、イーサネット インターフェイス 0/1 上にある 1 つの VRRP グループをディセーブルにする例を示します。

```
interface ethernet0/1
 ip address 10.24.1.1 255.255.255.0
 vrrp 1 ip 10.24.1.254
 vrrp 1 shutdown

interface ethernet0/2
 ip address 10.168.42.1 255.255.255.0
 vrrp 2 ip 10.168.42.254
```

VRRP MIB トラップ：例

次に、VRRP MIB トラップ サポート機能をイネーブルにする例を示します。

```
snmp-server enable traps vrrp
snmp-server host 10.1.1.0 community abc vrrp
```

その他の参考資料

VRRP 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
VRRP コマンド：コマンド構文、コマンド モード、コマンド履歴、デフォルト設定、使用に関する注意事項および例	『*Cisco IOS IP Application Services Command Reference*』
キー チェーンおよびキー管理用コマンド：コマンド構文の詳細、コマンド モード、コマンド履歴、デフォルト設定、使用に関する注意事項、例	『*Cisco IOS IP Routing：RIP Command Reference*』
オブジェクト トラッキング	「Configuring Enhanced Object Tracking」モジュール
HSRP	「Configuring HSRP」モジュール
GLBP	「Configuring GLBP」モジュール

規格

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

MIB

MIB	MIB リンク
この機能がサポートする新しい MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択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
RFC 2338	「*Virtual Router Redundancy Protocol*」

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

VRRP の機能情報

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

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。

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。

表 1　　VRRP の機能情報

機能名	リリース	機能設定情報
FHRP—VRF-Aware VRRP	12.2(15)T 12.0(18)ST 12.2(31)SG 12.2(17d)SXB	FHRP—VRF-Aware VRRP 機能により、VRF-Aware MPLS VPN による VRRP サポートが追加されます。
FHRP—VRRP Enhancements	12.3(14)T	FHRP—VRRP Enhancements 機能により、次のサポートが追加されます。 • MD5 認証：VRRP に設定されているルータに追加されます。HSRP と同様に、RFC 2338 に規定されている方法よりも簡単な方法を使用した、ピアの認証方法を提供します。 • Bridged Virtual Interface（BVI）：BVI に VRRP を設定する機能を追加します。この機能は、BVI に既存の HSRP サポートに類似しています。 この機能に関する詳細については、次の各項を参照してください。 • 「VRRP の制約事項」（P.2） • 「VRRP 認証の設定」（P.14） コマンド **debug vrrp authentication** がこの機能により導入されました。 **vrrp authentication** および **show vrrp** の各コマンドがこの機能により変更されました。

表 1　VRRP の機能情報 （続き）

機能名	リリース	機能設定情報
ISSU と VRRP	12.2(33)SRC	VRRP は In Service Software Upgrade（ISSU; インサービス ソフトウェア アップグレード）をサポートします。ISSU を使用すると、アクティブおよびスタンバイの Route Processor（RP; ルート プロセッサ）またはライン カード上で異なるバージョンの Cisco IOS ソフトウェアが実行されている場合でも、ハイアベイラビリティ（HA）システムをステートフル スイッチオーバー（SSO）モードで実行できるようになります。 この機能は、ソフトウェア アップグレード中に予定されたシステム停止中も同じレベルの HA 機能を提供します。不測のシステム停止が発生した場合も、SSO を使用できます。つまり、システムをセカンダリ RP に切り替えることができ、セッションを切断することなく、またパケットの損失も最小限に抑えながら、継続してパケットを転送できます。 この機能は、デフォルトでイネーブルにされています。 この機能に関する詳細については、次の各項を参照してください。 • 「ISSU と VRRP」（P.7） この機能により、新規追加または変更されたコマンドはありません。
SSO と VRRP	12.2(33)SRC 12.2(33)SXI	VRRP が SSO を認識するようになりました。VRRP は、ルータがセカンダリ RP にフェールオーバーしたことを検出し、VRRP グループの現在の状態を継続することができます。 この機能は、デフォルトでイネーブルにされています。 この機能に関する詳細については、次の各項を参照してください。 • 「SSO と VRRP」（P.7） • 「VRRP のカスタマイズ」（P.8） **debug vrrp ha**、**vrrp sso**、**show vrrp** の各コマンドが、この機能により導入または変更されました。

表 1　VRRP の機能情報 （続き）

機能名	リリース	機能設定情報
Virtual Router Redundancy Protocol	12.2(13)T 12.2(14)S	VRRP は、ルータのグループを使用して単一の仮想ルータを形成し、冗長性を実現します。これにより、仮想ルータをデフォルト ゲートウェイとして使用するように、LAN クライアントを設定できます。ルータのグループを表す仮想ルータは、「VRRP グループ」とも呼ばれます。 この機能に関する詳細については、すべての項に記載しています。 この機能により次のコマンドが導入されました。**debug vrrp all**、**debug vrrp error**、**debug vrrp events**、**debug vrrp packets**、**debug vrrp state**、**show vrrp**、**show vrrp interface**、**vrrp authentication**、**vrrp description**、**vrrp ip**、**vrrp preempt**、**vrrp priority**、**vrrp timers advertise**、**vrrp timers learn**
VRRP オブジェクト トラッキング	12.3(2)T 12.2(25)S	VRRP オブジェクト トラッキング機能により VRRP の機能が拡張され、ルータ内の特定のオブジェクトを追跡して VRRP グループの仮想ルータのプライオリティ レベルを変更できるようになりました。 この機能に関する詳細については、次の各項を参照してください。 • 「VRRP オブジェクト トラッキング」（P.6） • 「VRRP オブジェクト トラッキングの設定」（P.12） コマンド **vrrp track** がこの機能により導入されました。 コマンド **show track** がこの機能により変更されました。
VRRP MIB—RFC 2787	12.3(11)T	VRRP MIB—RFC 2787 機能により、SNMP ベースのネットワーク管理で使用できるように MIB の機能が強化されました。VRRP を使用するルータの設定、モニタ、および制御をサポートするようになりました。 この機能に関する詳細については、次の各項を参照してください。 • 「インターフェイスでの VRRP のディセーブル化」（P.11） • 「SNMP VRRP 通知を送信するようにルータをイネーブル化」（P.20） コマンド **vrrp shutdown** がこの機能により導入されました。 **snmp-server enable traps** および **snmp-server host** の各コマンドがこの機能により変更されました。

用語集

VRRP ルータ：VRRP を実行しているルータ。

仮想ルータ：1 つのグループを形成する 1 台または複数台の VRRP ルータ。仮想ルータは、LAN クライアントのデフォルト ゲートウェイ ルータとして動作します。「VRRP グループ」とも呼ばれます。

仮想ルータ バックアップ：仮想ルータ マスターが機能を停止したときにパケット転送のロールを引き受けることのできる 1 台または複数台の VRRP ルータ。

仮想ルータ マスター：仮想ルータの IP アドレスに送信されるパケットの転送を現在行っている VRRP ルータ。通常、仮想ルータ マスターは IP アドレス所有者としても機能します。

バーチャル IP アドレス所有者：仮想ルータの IP アドレスを所有する VRRP ルータ。仮想ルータ アドレスを物理インターフェイス アドレスとして持っているルータが所有者になります。