Cisco IOS XE 17（Cisco NCS 520 シリーズ）ファーストホップ冗長性プロトコル設定ガイド

初版：2019 年 11 月 26 日

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

目 次

第 1 章

HSRP について 1

HSRP の制約事項 1

HSRP に関する情報 2

HSRP の動作 2

HSRP の利点 3

HSRP グループとグループの属性 3

HSRP のプリエンプション 3

HSRP のプライオリティとプリエンプション 4

オブジェクト トラッキングが HSRP デバイスのプライオリティに及ぼす影響 4

HSRP のアドレス指定 5

HSRP 仮想 MAC アドレスと BIA MAC アドレス 5

HSRP MAC アドレス 6

HSRP MAC の更新間隔 6

HSRP のテキスト認証 6

HSRP MD5 認証 6

HSRP の設定方法 7

HSRP の設定 7

HSRP 情報の表示 8

第 2 章

VRRP の設定 11

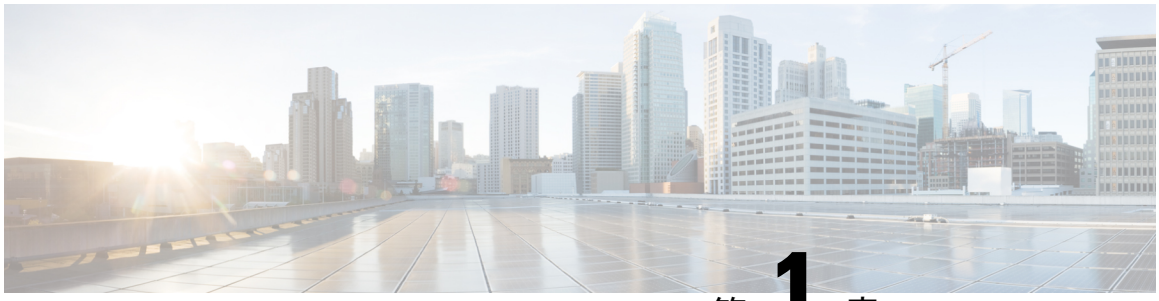
VRRP の制約事項 11

NCS 520 の VRRP の制約事項 11

VRRP の概要 12

VRRP MAC アドレス 12

VRRP の動作 12
VRRP の利点 14
複数の仮想ルータのサポート 15
VRRP ルータのプライオリティおよびプリエンプション 15
VRRP のアドバタイズメント 16
VRRP の設定方法 16
VRRP の 設定 16
VRRP の有効化 18
インターフェイスでの VRRP グループの無効化 20
VRRP テキスト認証の設定 21
IPV4 の VRRP v3 の設定 22
VRRP の設定例 23
例：VRRP の設定 23
例：VRRP テキスト認証 24
例：インターフェイス上での VRRP グループのディセーブル化 24



第 1 章

HSRP について

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

- HSRP の制約事項 （1 ページ）
- HSRP に関する情報 （2 ページ）
- HSRP の設定方法 （7 ページ）

HSRP の制約事項

- HSRP をサポートするには、ASIC が IPv4 VMAC の下を宛先とするパケットを受信できる必要があります。

  HSRP は、MAC アドレス **00:00:0C:07:xx** でサポートされています

- HSRP バージョン 2 は、NCS520 ルータではサポートされていません。
- HSRP と VRRP は、両方ともブリッジ ドメイン インターフェイス（BDI）でのみサポートされています。
- HSRP でサポートされているタイマーの値は、hello 間隔は 0.3 秒、dead 間隔は 1 秒です。

HSRP に関する情報

HSRP の動作

ほとんどの IP ホストには、デフォルト ゲートウェイとして設定されている単一のデバイスの IP アドレスがあります。HSRP を使用すると、デバイスの IP アドレスではなく、HSRP 仮想 IP アドレスがホストのデフォルト ゲートウェイとして設定されます。

HSRP は、ディスカバリ プロトコル（ICMP Router Discovery Protocol [IRDP] など）をサポートしないホスト、および選択したデバイスがリロードしたときやデバイスの電源が失われたときに新しいデバイスに切り替えることができないホストに便利です。また、既存の TCP セッションはフェールオーバーが発生しても存続するため、このプロトコルでは IP トラフィックをルーティングするためにネクストホップを動的に選択するホストの回復をさらに透過的に実行できます。

HSRP をネットワーク セグメントに設定すると、HSRP が動作するデバイスのグループ間で仮想 MAC アドレスと IP アドレスを共有できるようになります。この HSRP グループのアドレスが仮想 IP アドレスと呼ばれます。このようなデバイスの 1 つが、アクティブ デバイスとしてプロトコルによって選択されます。アクティブ デバイスは、グループの MAC アドレス宛のパケットを受信してルーティングします。n 台のデバイスで HSRP が稼動している場合、n+ 1 個の IP アドレスおよび MAC アドレスが割り当てられます。

指定されたアクティブ デバイスの障害を HSRP が検出すると、選択されているスタンバイ デバイスがホット スタンバイ グループの MAC アドレスと IP アドレスの制御を引き継ぎます。この時点で新しいスタンバイ デバイスも選択されます。

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

HSRP を実行しているデバイスは、UDP ベースのマルチキャスト hello メッセージを送信および受信して、デバイスの障害を検出したり、アクティブ デバイスとスタンバイ デバイスを割り当てたりします。アクティブ デバイスが設定された時間内に hello メッセージを送信できなかった場合は、最高のプライオリティのスタンバイ デバイスがアクティブ デバイスになります。このようにパケット転送機能が別のデバイスに移行しても、ネットワークのいずれのホストにもまったく影響はありません。

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

次の図は、HSRP 用に設定されたネットワークを示しています。仮想 MAC アドレスおよび IP アドレスを共有することによって、複数台のデバイスが 1 台の仮想ルータとして機能します。仮想デバイスは物理的には存在しませんが、互いのバックアップになるように設定されている複数のデバイスの共有のデフォルト ゲートウェイになります。アクティブ デバイスの IP アド

レスを使用して、LAN 上でホストを設定する必要はありません。その代わりに、仮想デバイスの IP アドレス（仮想 IP アドレス）をデフォルト ゲートウェイとして使用して設定します。設定した時間内にアクティブ デバイスが hello メッセージを送信できない場合、スタンバイ デバイスが処理を引き継いで仮想アドレスに対応するアクティブ デバイスになり、アクティブ デバイスの役割を引き受けます。

HSRP の利点

- 冗長性：

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

- 高速フェールオーバー：

  HSRP はファースト ホップ デバイスの透過的なフェールオーバーを提供します。

- プリエンプション：

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

- 認証：

  HSRP のメッセージ ダイジェスト 5（MD5）アルゴリズム認証は、HSRP スプーフィング ソフトウェアから保護し、業界標準の MD5 アルゴリズムを使用して信頼性とセキュリティを向上させています。

HSRP グループとグループの属性

CLI を使用して、次のものにグループ属性を適用できます。

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

HSRP のプリエンプション

新規にリロードされたデバイスが HSRP アクティブ デバイスになったとき、HSRP アクティブ デバイスがすでに存在していた場合は、HSRP のプリエンプションが機能していないように見えることがあります。HSRP のプリエンプションが正しく機能していないように見える原因は、新しい HSRP アクティブ デバイスが現在の HSRP アクティブ デバイスから hello パケットを受信しておらず、プリエンプション設定が新しいデバイスの決定で考慮されないためです。

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

通常は、すべての HSRP デバイスを **standby delay minimum 30 reload 60** のように設定することを推奨します。

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

これは、HSRP プリエンプション遅延を有効にするインターフェイス コンフィギュレーション コマンド **standby preempt delay** とは異なるコマンドです。

HSRP のプライオリティとプリエンプション

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

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

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

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

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

デバイスがオブジェクト トラッキング対応として設定されていて、なおかつトラッキング対象のオブジェクトがダウンした場合、デバイスのプライオリティはダイナミックに変更されます。トラッキング プロセスは定期的に、トラッキング対象オブジェクトをポーリングし、値の変更を確認します。トラッキング対象のオブジェクトの変化は、すぐに HSRP に伝えられるか、指定した遅延時間が経過してからHSRP に伝えられます。オブジェクトの値は、アップまたはダウンとして報告されます。トラッキング可能なオブジェクトには、インターフェイスのライン プロトコル ステートや IP ルートの到達可能性などがあります。指定したオブジェクトがダウンすると、HSRP プライオリティが引き下げられます。より優先順位の高い HSRP デバイスは、**standby preempt** コマンドが設定されている場合にはアクティブなデバイスになることができます。

HSRP のアドレス指定

HSRP デバイスが互いに通信するときは、HSRP hello パケットをやり取りします。これらのパケットは、UDP ポート 1985 上の宛先 IP マルチキャスト アドレス 224.0.0.2（すべてのデバイスと通信するための予約済みマルチキャスト アドレス）に送信されます。アクティブ デバイスは、それ自身に設定されている IP アドレスと HSRP 仮想 MAC アドレスを hello パケットの送信元とし、スタンバイ デバイスは、それ自身に設定されている IP アドレスとインターフェイス MAC アドレスを hello パケットの送信元とします。この MAC アドレスは、バーンドイン MAC アドレス（BIA）である場合も、そうでない場合もあります。

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

HSRP バージョン 2 では新しい IP マルチキャスト アドレス 224.0.0.102 を使用して hello パケットを送信します。バージョン 1 では、このマルチキャスト アドレスが 224.0.0.2 です。この新しいマルチキャスト アドレスにより、シスコ グループ管理プロトコル（CGMP）の脱退処理を HSRP と同時にイネーブルにすることができます。

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

HSRP 仮想 MAC アドレスと BIA MAC アドレス

各 HSRP デバイスの仮想 MAC アドレスはデバイスで自動的に生成されます。ただし、拡張分散ネットワーク機能（APPN）などの一部のネットワーク実装では、MAC アドレスを使用して、ルーティングのためのファーストホップを特定します。この場合、グループの **standby mac-address** コマンドを使用して、仮想 MAC アドレスを指定します。仮想 IP アドレスは、これらのプロトコルには重要ではありません。

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

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

HSRP MAC アドレス

ASIC は IPV4 仮想 MAC アドレスを使用してパケットを受信できます

HSRP は、MAC アドレス **00:00:0C:07:xx** でサポートされています

HSRP MAC の更新間隔

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

FDDI リングでのリフレッシュ間隔を延長または短縮して、帯域幅をさらに効率的に使用することができます。MAC 更新パケットが必要ない場合（FDDI はあるがラーニング ブリッジやスイッチがない場合）は、送信されないようにできます。

HSRP のテキスト認証

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

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

HSRP パケットが拒否されるのは、次のいずれかの場合です。

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

HSRP MD5 認証

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

MD5 認証を使用すると、別のプレーンテキスト認証方式よりもセキュリティを強化できます。HSRP グループの各メンバーは秘密キーを使用して、発信パケットの一部となるキー付き MD5 ハッシュを生成できます。着信パケットからはキー付きハッシュが生成されますが、このハッシュと着信パケット内のハッシュが一致しない場合は、パケットは無視されます。

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

HSRP には次の 2 つの認証方式があります。

- プレーン テキスト認証
- MD5 認証

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

HSRP パケットが拒否されるのは、次のいずれかの場合です。

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

HSRP の設定方法

Cisco NCS 520 ルータで HSRP を設定するには、次のコマンドを使用します。

HSRP の設定

```
interface GigabitEthernet0/1
  service instance 1 ethernet
    encapsulation dot1q 10
    rewrite ingress tag pop 1 symmetric
    bridge-domain 100

int bdi 100
  ip address 10.1.0.21 255.255.0.0
  standby 1 priority 110
  standby 1 preempt
  standby 1 ip 10.1.0.1
  standby 1 authentication text auth_1

interface GigabitEthernet0/1
  service instance 1 ethernet
    encapsulation dot1q 10
    rewrite ingress tag pop 1 symmetric
    bridge-domain 100
int bdi 100
  ip address 10.1.0.22 255.255.0.0
  standby 1 preempt
  standby 1 priority 105
  standby 1 ip 10.1.0.1
  standby 1 authentication text auth_1
```

HSRP 情報の表示

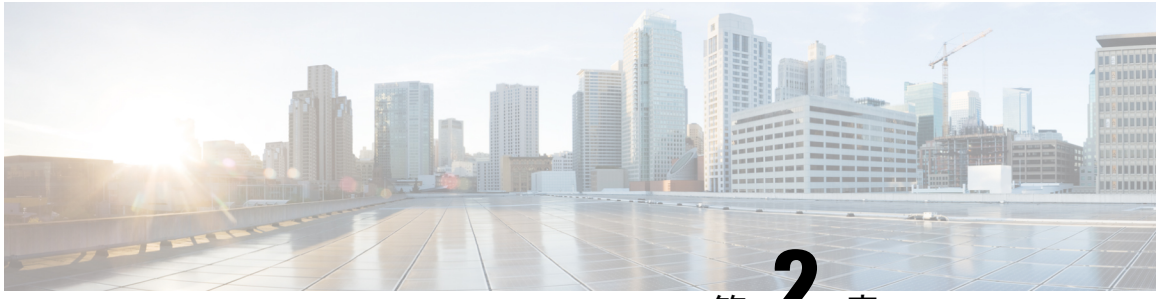
手順

	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 モードを有効にします。 • パスワードを入力します（要求された場合）。

ステップ 2	**show standby brief all**
	例：
	`Router# show standby brief all`
	`P indicates configured to preempt.`
	`|`
	`Interface Grp Pri P State Active Standby Virtual IP`
	`BD101 1 190 P Standby 100.100.1.2 local 100.100.1.10`
	`BD101 2 200 P Active local 100.100.1.2 100.100.1.20`
	`Router#`	

ステップ 3	**show standby**
	例：
	`BDI101 - Group 1`
	`State is Standby`
	`4 state changes, last state change 00:04:24`
	`Virtual IP address is 100.100.1.10`
	`Active virtual MAC address is 0000.0c07.ac01 (MAC Not In Use)`
	`Local virtual MAC address is 0000.0c07.ac01 (v1 default)`
	`Hello time 3 sec, hold time 10 sec`
	`Next hello sent in 1.616 secs`
	`Authentication text, string "auth"`
	`Preemption enabled`
	`Active router is 100.100.1.2, priority 200 (expires in 9.472 sec)`
	`Standby router is local`
	`Priority 190 (configured 190)`
	`Group name is "hsrp-BD101-1" (default)`
	`FLAGS: 0/1`
	`BDI101 - Group 2`
	`State is Active`
	`2 state changes, last state change 00:04:55`
	`Virtual IP address is 100.100.1.20`
	`Active virtual MAC address is 0000.0c07.ac02 (MAC In Use)`
	`Local virtual MAC address is 0000.0c07.ac02 (v1 default)`	

	コマンドまたはアクション	目的
	Hello time 3 sec, hold time 10 sec Next hello sent in 0.256 secs Authentication text, string "auth1" Preemption enabled Active router is local Standby router is 100.100.1.2, priority 190 (expires in 8.960 sec) Priority 200 (configured 200) Group name is "hsrp-BD101-2" (default) FLAGS: 1/1 Router#	
ステップ 4	**exit** 例： Router# end	特権 EXEC モードに戻ります。



第 2 章

VRRP の設定

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

この章では、VRRP に関する概念と、ネットワーク上での VRRP の設定方法について説明します。

- VRRP の制約事項 （11 ページ）
- NCS 520 の VRRP の制約事項 （11 ページ）
- VRRP の概要 （12 ページ）
- VRRP の設定方法 （16 ページ）
- IPV4 の VRRP v3 の設定 （22 ページ）
- VRRP の設定例 （23 ページ）

VRRP の制約事項

NCS 520 の VRRP の制約事項

- 最大 255 の一意の FHRP（HSRP および VRRP）グループがサポートされています。
- ブリッジ ドメイン インターフェイス（BDI）には、HSRP と VRRP の 4 つのインスタンスを組み合わせることができます。
- HSRP と VRRP は、両方ともブリッジ ドメイン インターフェイスでのみサポートされています。
- HSRP および VRRP は、レイヤ 2 ポート上のトランク イーサネット フロー ポイント EFP/TEFP を備えたレイヤ 3 ブリッジ ドメイン インターフェイス（BDI）と、レイヤ 2 ポートチャネル上の EFP/TEFP を備えたレイヤ 3 BDI でサポートされています。

- IPv6 は、HSRP および VRRP ではサポートされていません。

VRRP の概要

VRRP MAC アドレス

ASIC は IPV4 仮想 MAC アドレスを使用してパケットを受信できます

VRRP は、MAC アドレス **00:00:5E:00:xx** でサポートされています

VRRP の動作

LAN クライアントが特定のリモート接続先に対して、どのルータをファースト ホップにすべきかを判断するには、いくつかの方法があります。クライアントは、ダイナミック プロセスまたはスタティック設定を使用できます。ダイナミック ルータ ディスカバリの例を示します。

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

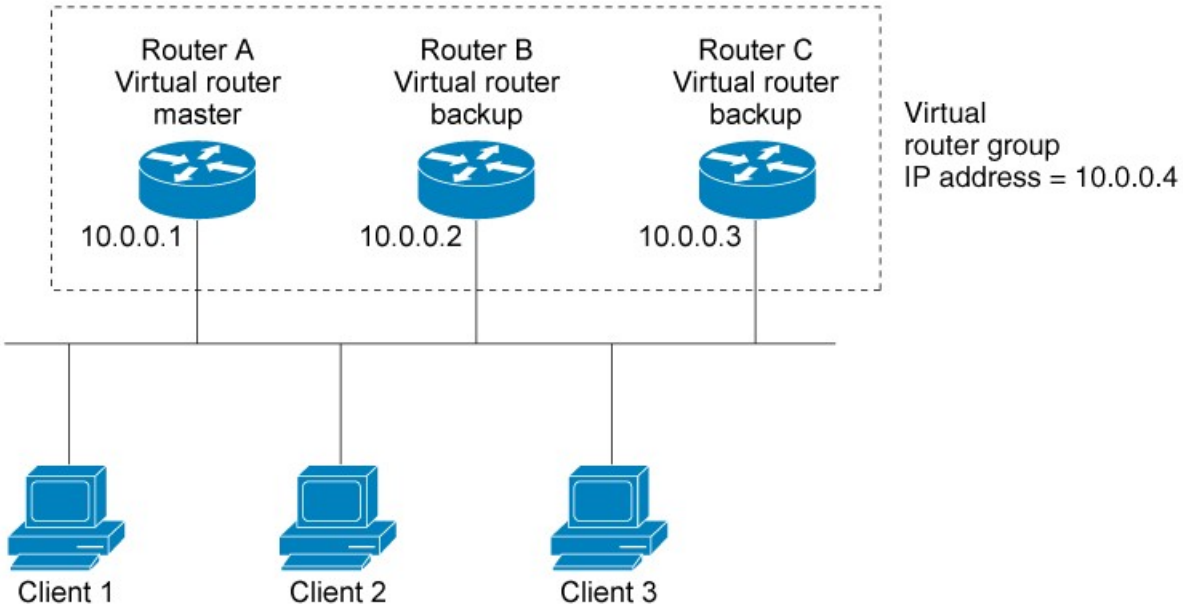
ダイナミック ディスカバリ プロトコルには、LAN クライアントにおいて、設定および処理のオーバーヘッドが発生するという短所があります。また、ルータが機能を停止したときに、別のルータへの切り替え処理が遅くなる可能性があります。

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

VRRP を使用すると、スタティックな設定の問題は解消されます。VRRP を使用すると、ルータのグループで 1 つの仮想ルータを形成できます。これにより、仮想ルータをデフォルト ゲートウェイとして使用するように、LAN クライアントを設定できます。ルータのグループを表す仮想ルータは、「VRRP グループ」とも呼ばれます。

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

図 *1* : 基本的な *VRRP* トポロジ

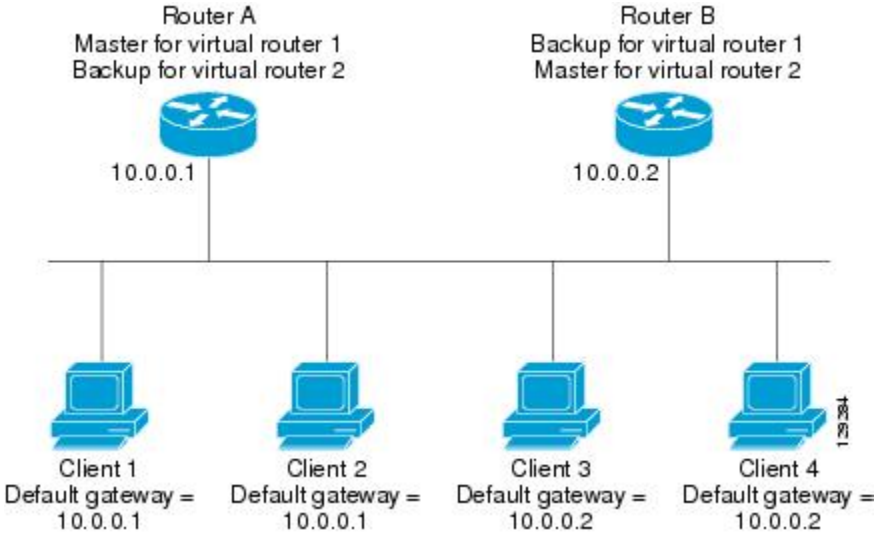


仮想ルータはルータ A の物理イーサネット インターフェイスの IP アドレスを使用するため、ルータ A は仮想ルータ マスターのロールを担い、「IP アドレス所有者」とも呼ばれます。ルータ A は、仮想ルータ マスターとして、仮想ルータの IP アドレスを管理し、この IP アドレスに送信されたパケットの転送を行います。クライアント 1 ～ 3 には、デフォルト ゲートウェイの IP アドレス 10.0.0.1 が設定されています。

ルータ B とルータ C は仮想ルータ バックアップとして機能します。仮想ルータ マスターが機能を停止すると、高いプライオリティに設定されているルータが仮想ルータ マスターとなり、LAN ホストには継続してサービスが提供されます。ルータ A が回復すると、再び仮想ルータ マスターになります。VRRP ルータの役割と、仮想ルータマスターに障害が発生するとどうなるかについての詳細は、「VRRP ルータのプライオリティおよびプリエンプション」の項を参照してください。

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

図 *2:* ロード シェアリングおよび冗長構成の *VRRP* トポロジ



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

仮想ルータ 2 では、ルータ B が IP アドレス 10.0.0.2 の所有者で仮想ルータ マスターです。ルータ A はルータ B に対する仮想ルータ バックアップです。クライアント 3 と 4 にはデフォルト ゲートウェイの IP アドレス 10.0.0.2 が設定されています。

VRRP の利点

冗長性

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

ロード シェアリング

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

複数の仮想ルータ

複数の IP アドレス

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

プリエンプション

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

認証

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

アドバタイズメント プロトコル

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

VRRP オブジェクト トラッキング

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

複数の仮想ルータのサポート

- ルータの処理能力
- ルータのメモリの能力
- 複数の MAC アドレスのルータ インターフェイス サポート

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

VRRP ルータのプライオリティおよびプリエンプション

VRRP冗長性スキームの重要な一面に、VRRPルータ プライオリティがあります。プライオリティにより、各 VRRP ルータが実行する役割と、仮想マスター ルータが機能を停止したときにどのようなことが起こるかが決定されます。

VRRP ルータが仮想ルータの IP アドレスと物理インターフェイスの IP アドレスのオーナーである場合には、このルータが仮想マスター ルータとして機能します。

VRRP ルータが仮想バックアップ ルータとして機能するかどうかや、仮想マスター ルータが機能を停止した場合に仮想マスタールータを引き継ぐ順序も、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優先順位を設定できます。

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

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

VRRP のアドバタイズメント

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

RFC 3768 に従った VRRP プロトコルはミリ秒タイマーをサポートしていませんが、シスコ ルータではミリ秒タイマーを設定することができます。ミリ秒タイマー値は、プライマリ ルータとバックアップ ルータの両方に手動で設定する必要があります。バックアップルータ上の **show vrrp** コマンド出力に表示されるマスターアドバタイズメント値は、常に、1 秒です。これは、バックアップルータ上のパケットでミリ秒値が受け入れられないためです。

ミリ秒タイマーは、絶対に必要な場合以外は使用しないようにし、使用する場合は慎重な検討とテストが必要です。ミリ秒値は順境の下でしか機能しません。そのため、ミリ秒タイマー値の使用は、VRRP の動作をシスコ デバイスに限定することに注意する必要があります。

VRRP の設定方法

VRRP の 設定

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

手順

	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 モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**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)# BDI <interface number>`	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。

	コマンドまたはアクション	目的
ステップ 8	**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 9	**exit** 例： `Router(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了します。
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 の有効化

手順

	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 モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**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 BDI <interface number>`	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 アドレスの指定後は、**secondary** キーワードを指定して **vrrp ip** コマンドを再び使用し、このグループでサポートする他の IP アドレスを指定できます。 （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	**show vrrp** [**brief all**] | interface]
	例：
	`Router(config-if)#show vrrp brief`
	`Interface Grp Pri Time Own Pre State`
	`Master addr Group addr`
	`BD10 1 100 9609 Y Backup 10.1.0.2`
	`10.1.0.10`
	`BD10 5 200 90218 Y Master 10.1.0.1`
	`10.1.0.50`
	`BD10 100 100 3609 Backup 10.1.0.2`
	`10.1.0.100`
		（任意）ルータ上の 1 つまたはすべての VRRP グループについて、簡潔または詳細なステータスを表示します。

ステップ 7	**show vrrp interface** *type number* [**brief**]
	例：
	`Router(config)# interface BDI <interface number>`
	`Router)config-if)#show vrrp interface bdi10`
	`BDI10 - Group 10`
	`G1`
	`State is Master`
	`Virtual IP address is 10.0.0.5`
	`Virtual MAC address is 0000.5e00.010a`
	`Advertisement interval is 10.000 sec`
	`Preemption enabled, delay min 380 secs`
	`Priority is 110`
	`Master Router is 10.0.0.2 (local),`
		（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。

	コマンドまたはアクション	目的
	priority is 110 Master Advertisement interval is 10.000 sec Master Down interval is 30.570 sec FLAGS: 1/1	
ステップ 8	**end** 例： Router(config-if)# end	特権 EXEC モードに戻ります。

インターフェイスでの VRRP グループの無効化

インターフェイスでVRRPグループを無効にすると、そのプロトコルを無効にできますが、設定は保持されます。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。

簡易ネットワーク管理プロトコル（SNMP）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 のコマンド ライン インターフェイス（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、および有効と無効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有効になります。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、**no vrrp shutdown** コマンドを入力すると、VRRP グループが再び有効になります。

手順

	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 モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**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：	インターフェイス コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
	`Router(config)# interface BDI <interface number>`	
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 グループを無効にします。 • 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 テキスト認証の設定

始める前に

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

どのような場合でも、テキスト認証を MD5 認証と組み合わせて VRRP グループに使用することはできません。MD5 認証が設定されている場合、受信側のルータの MD5 認証がイネーブルになっていれば、VRRP hello メッセージのテキスト認証フィールドは転送時にすべてゼロに設定され、受信時に無視されます。

手順

	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 モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**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。

	コマンドまたはアクション	目的
ステップ 3	**terminal interface** *type number* 例： `Router(config)# interface BDI <interface number> 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	**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	**end** 例： `Router(config-if)# end`	特権 EXEC モードに戻ります。

IPV4 の VRRP v3 の設定

```
Fhrp version vrrp v3
Int bdi< >
```

```
Vrrp 1 address-family ipv4
Priority 190
Preempt delay minimum 10
Address <ipv4-address> primary
```

VRRP の設定例

例：VRRP の設定

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

コンフィギュレーションにおいて、各グループのプロパティは次のとおりです。

- グループ 1：
  - 仮想 IP アドレスは 10.1.0.10 です。
  - ルータ A はプライオリティ 120 で、このグループのマスターになります。
  - アドバタイズ インターバルは 3 秒です。
  - プリエンプションはイネーブルです。
- グループ 5：
  - ルータ B はプライオリティ 200 で、このグループのマスターになります。
  - アドバタイズ インターバルは 30 秒です。
  - プリエンプションはイネーブルです。
- グループ 100：
  - ルータ A は、IP アドレスが上位（10.1.0.2）なので、このグループのマスターになります。
  - アドバタイズ インターバルはデフォルトの 1 秒です。
  - プリエンプションはディセーブルです。

ルータ A

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

ルータ B

```
Router(config)# BDI <interface number>
Router(config-if)# ip address 10.1.0.1 255.0.0.0
Router(config-if)# vrrp 1 priority 100
Router(config-if)# vrrp 1 authentication text cisco
Router(config-if)# vrrp 1 timers advertise 3
Router(config-if)# vrrp 1 timers learn
Router(config-if)# vrrp 1 ip 10.1.0.10
Router(config-if)# vrrp 5 priority 200
Router(config-if)# vrrp 5 timers advertise 30
Router(config-if)# vrrp 5 timers learn
Router(config-if)# vrrp 5 ip 10.1.0.50
Router(config-if)# vrrp 100 timers learn
Router(config-if)# no vrrp 100 preempt
Router(config-if)# vrrp 100 ip 10.1.0.100
Router(config-if)# no shutdown
```

例：VRRP テキスト認証

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

```
Router(config)# BDI <interface number>
Router(config)# ip address 10.21.8.32 255.255.255.0
Router(config-if)# vrrp 10 authentication text stringxyz
Router(config-if)# vrrp 10 ip 10.21.8.10
```

例：インターフェイス上での VRRP グループのディセーブル化

次に、BDI インターフェイスではグループ 2 の VRRP を維持しながら、BDI インターフェイス上にある 1 つの VRRP グループを無効にする例を示します。

```
Router(config)# BDI <interface number>
Router(config-if)# ip address 10.24.1.1 255.255.255.0
Router(config-if)# vrrp 1 ip 10.24.1.254
Router(config-if)# vrrp 1 shutdown
Router(config-if)# exit
Router(config)#  BDI <interface number>
Router(config-if)# ip address 10.168.42.1 255.255.255.0
Router(config-if)# vrrp 2 ip 10.168.42.254
```