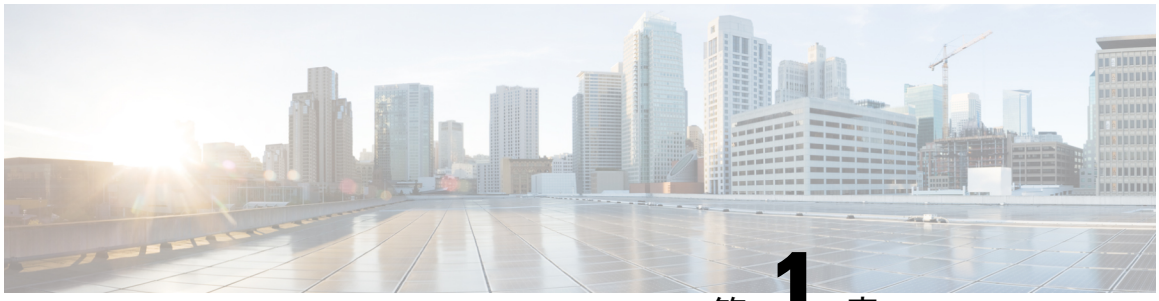
Cisco IOS XE Fuji 16.8.x（Catalyst 9300 スイッチ）IP コンフィギュレーション ガイド

初版：2018 年 7 月 18 日

最終更新：2019 年 5 月 23 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 の設定

HSRP の設定

この章では、ホットスタンバイルータプロトコル（HSRP）を使用する方法について説明します。これによって、IP トラフィック ルーティングに冗長性を提供し、個々のルータのアベイラビリティに依存しないルーティングを実現します。

レイヤ 2 モードの HSRP のバージョンを使用すると、クラスタ コマンド スイッチが故障した場合、クラスタ管理を引き継ぐ冗長コマンド スイッチを設定することもできます。

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。最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、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。

HSRP の設定に関する情報

HSRP の概要

HSRP は、デフォルト ゲートウェイ IP アドレスが設定された IEEE 802 LAN 上の IP ホストにファーストホップ冗長性を確保することでネットワークのアベイラビリティを高めるシスコの標準方式です。HSRP を使用すると、特定のルータのアベイラビリティに依存せず IP トラフィックをルーティングできます。また、一連のルータ インターフェイスを組み合わせることで、1 台の仮想ルータ、または LAN 上のホストへのデフォルト ゲートウェイのように機能させるこ

とができます。ネットワークまたはセグメント上に HSRP を設定すると、仮想 MAC（メディア アクセス コントロール）アドレス、および設定されたルータ グループ間で共有される IP アドレスを使用できるようになりHSRP が設定された複数のルータは、仮想ルータの MAC アドレスおよび IP ネットワーク アドレスを使用できるようになります。仮想ルータは、実際には存在しません。仮想ルータは、相互にバックアップ機能を提供するように設定されている複数のルータの共通のターゲットを表します。1 台のルータがアクティブなルータとして、もう 1 台のルータがスタンバイ ルータとして選択されます。スタンバイ ルータは、指定されたアクティブ ルータが故障した場合に、グループのMACアドレスおよびIPアドレスを制御するルータです。

（注） HSRP グループ内のルータには、ルーテッド ポート、スイッチ仮想インターフェイス（SVI）など、HSRP をサポートする任意のルータ インターフェイスを指定できます。

HSRPは、ネットワーク上のホストからのIPトラフィックに冗長性を提供することで、ネットワークのアベイラビリティを高めます。アクティブ ルータは、ルータ インターフェイスのグループ内でパケットのルーティングを実行するために選択されたルータです。スタンバイ ルータは、アクティブ ルータが故障した場合、または事前に設定した条件が満たされた場合に、ルーティング作業を引き継ぐルータです。

HSRPは、ホストがルータ ディスカバリ プロトコルをサポートしておらず、選択されたルータのリロードや電源故障時に新しいルータに切り替えることができない場合に有効です。HSRP をネットワーク セグメントに設定すると、HSRP は仮想 MAC アドレスと IP アドレスを 1 つずつ提供します。このアドレスは、HSRPが動作するルータ インターフェイス グループ内のルータ インターフェイス間で共有できます。プロトコルによってアクティブ ルータとして選択されたルータは、グループの MAC アドレス宛てのパケットを受信し、ルーティングします。n 台のルータで HSRP が稼働している場合、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。

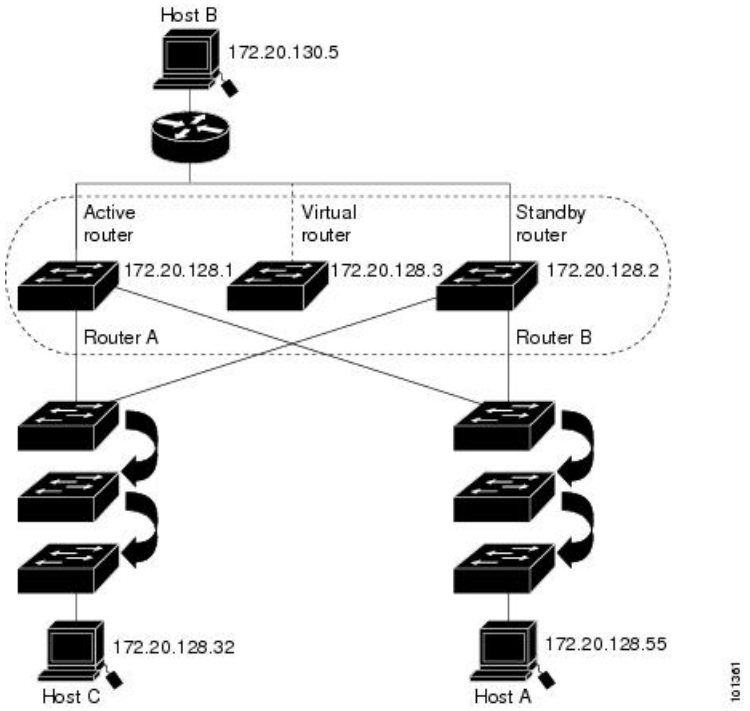
指定されたアクティブ ルータの故障を HSRP が検出すると、選択されているスタンバイ ルータがホットスタンバイ グループの MAC アドレスおよび IP アドレスの制御を引き継ぎます。この時点で新しいスタンバイ ルータも選択されます。HSRPが稼働しているデバイスは、マルチキャスト UDP ベースの hello パケットを送受信することにより、ルータ障害の検出、アクティブ ルータおよびスタンバイ ルータの指定を行います。インターフェイスに HSRP が設定されている場合、そのインターフェイスではインターネット制御メッセージプロトコル（ICMP）のリダイレクト メッセージが自動的にイネーブルになっています。

レイヤ 3 で動作するスイッチおよびスイッチ スタック間で複数のホット スタンバイ グループを設定すると、冗長ルータをさらに活用できます。

そのためには、インターフェイスに設定するホットスタンバイ コマンド グループごとにグループ番号を指定します。たとえば、スイッチ1のインターフェイスをアクティブルータ、スイッチ2のインターフェイスをスタンバイ ルータとして設定できます。また、スイッチ2の別のインターフェイスをアクティブ ルータ、スイッチ 1 の別のインターフェイスをスタンバイ ルータとして設定することもできます。

次の図に、HSRP 用に設定されたネットワークのセグメントを示します。各ルータには、仮想ルータの MAC アドレスおよび IP ネットワーク アドレスが設定されています。ルータ A の IP アドレスをネットワーク上のホストに設定する代わりに、デフォルトルータとして仮想ルータの IP アドレスを設定します。ホスト C からホスト B にパケットが送信される場合、ホスト C は仮想ルータの MAC アドレスにパケットを送信します。何らかの理由により、ルータ A がパケットの転送を停止すると、ルータ B が仮想 IP アドレスおよび仮想 MAC アドレスに応答してアクティブ ルータとなり、アクティブ ルータの作業を行います。ホスト C は引き続き仮想ルータの IP アドレスを使用し、ホスト B 宛のパケットをアドレッシングします。ルータ B はそのパケットを受信し、ホスト B に送信します。ルータ B は HSRP の機能を使用し、ルータ A が動作を再開するまで、ホスト B のセグメント上のユーザーと通信する必要があるホスト C のセグメント上のユーザーに連続的にサービスを提供します。また、ホスト A セグメントとホスト B の間で、引き続き通常のパケット処理機能を実行します。

図 *1 : HSRP* の一般的な構成



HSRP のバージョン

Cisco IOS XE Everest 16.5.1a 以降のスイッチでサポートされている Hot Standby Router Protocol（HSRP）のバージョンは次のとおりです。

スイッチでは、次の HSRP バージョンがサポートされます。

- HSRPv1：HSRP のバージョン 1（デフォルトのバージョン）。次の機能があります。
  - HSRP グループ番号は 0 ～ 255 まで使用できます。

- HSRPv1 は 224.0.0.2 のマルチキャスト アドレスを使用して hello パケットを送信しますが、これは Cisco Group Management Protocol（CGMP）の脱退処理と競合します。HSRPv1 と CGMP は相互に排他的なため、同時には使用できません。

- HSRPv2：HSRP のバージョン 2。このバージョンには次の機能があります。
  - HSRPv2 は 224.0.0.102 のマルチキャスト アドレスを使用して hello パケットを送信します。HSRPv2 と CGMP 脱退処理は相互に排他的ではありません。同時に使用できます。
  - HSRPv2 のパケット形式は、HSRPv1 とは異なります。

HSRPv1 を実行しているスイッチは、ルータの送信元 MAC アドレスが仮想 MAC アドレスのため、hello パケットを送信した物理的なルータを特定できません。

HSRPv2 のパケット形式は、HSRPv1 とは異なります。HSRPv2 パケットは、パケットを送信した物理ルータの MAC アドレスを格納できる 6 バイトの識別子フィールドを持った、Type Length Value（TLV）形式を使用します。

HSRPv1 を実行しているインターフェイスが HSRPv2 パケットを取得した場合、このタイプ フィールドは無視されます。

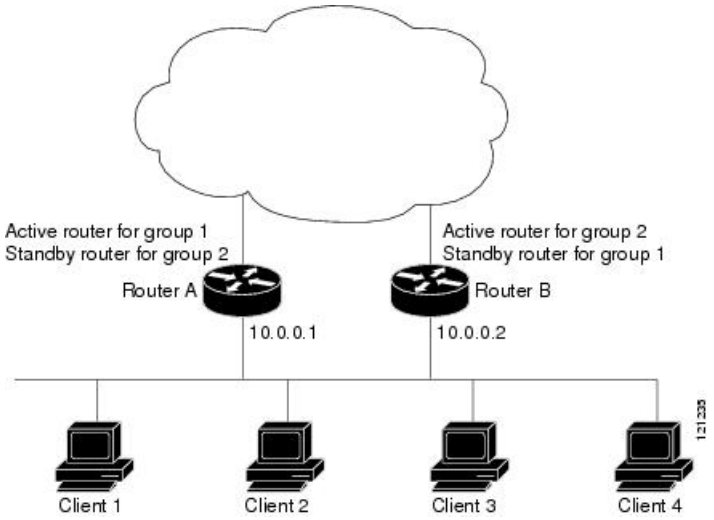
MHSRP

スイッチは、Multiple HSRP（MHSRP）をサポートします。MHSRP は HSRP の拡張版で、複数の HSRP グループ間でのロード シェアリングが可能です。ホスト ネットワークからサーバー ネットワークまで、ロードバランシングを実現して複数のスタンバイ グループ（およびパス）を使用するために、MHSRP を設定できます。

下の図では、半分のクライアントがルータ A に設定されており、もう半分はルータ B に設定されています。ルータ A およびルータ B の設定により、合計 2 つの HSRP グループが確立されています。グループ 1 では、ルータ A に最高のプライオリティが割り当てられているので、ルータ A がデフォルトのアクティブ ルータになり、ルータ B がスタンバイ ルータとなります。グループ 2 では、ルータ B に最も高いプライオリティが割り当てられているため、ルータ B がデフォルトのアクティブ ルータであり、ルータ A がスタンバイ ルータです。通常の運用では、2 つのルータが IP トラフィック負荷を分散します。いずれかのルータが使用できなくなると、もう一方のルータがアクティブになり、使用できないルータのパケット転送機能を引き継ぎます。

（注） MHSRP では、ルータに障害が発生して正常に戻った場合にプリエンプションによりロード シェアリングを復元するために、**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 HSRP インターフェイスで入力する必要があります。

図 *2 : MHSRP* ロード シェアリング



SSO HSRP

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

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

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

HSRP およびスイッチ スタック

HSRP の hello メッセージは、アクティブなスイッチで生成されます。アクティブなスイッチの HSRP に障害が発生すると、HSRP アクティブ状態のフラッピングが生じることがあります。これは、新規のアクティブなスイッチが選択および初期化されている間に HSRP hello メッセージが生成されず、アクティブなスイッチが故障した後でないとスタンバイスイッチがアクティブにならない可能性があるためです。

IPv6 の HSRP の設定

Network Advantage ライセンスを実行中のスイッチは、IPv6 の Hot Standby Router Protocol（HSRP）をサポートします。HSRP は、任意の単一のルータのアベイラビリティに依存せず、ルーティング IPv6 トラフィックにルーティング冗長性を提供します。IPv6 ホストは、IPv6 ネイバー探

索ルータのアドバタイズメントメッセージによって使用可能なルータを学習します。これらのメッセージは定期的にマルチキャストされるか、ホストにより送信請求されます。

HSRP IPv6 グループには、HSRP グループ番号に基づく仮想 MAC アドレス、およびデフォルトで HSRP 仮想 MAC アドレスに基づく HSRP の仮想 IPv6 リンクローカル アドレスがあります。

HSRP グループがアクティブな場合、定期的なメッセージが HSRP 仮想 IPv6 リンクローカル アドレスに送信されます。グループがアクティブ ステートでなくなった場合、これらのメッセージは最後のメッセージが送信されたあとで停止します。

（注） IPv6 の HSRP を設定する場合、インターフェイス上で HSRP version 2（HSRPv2）をイネーブルにする必要があります。

HSRP の設定方法

HSRP のデフォルト設定

表 *1: HSRP* のデフォルト設定

機能	デフォルト設定
HSRP バージョン	バージョン 1
HSRP グループ	未設定
スタンバイ グループ番号	0
スタンバイ MAC アドレス	0000.0c07.acXX に指定されたシステム。XX は、HSRP グループ番号
スタンバイ プライオリティ	100
スタンバイ遅延	0（遅延なし）
スタンバイでのインターフェイス プライオリティの追跡	10
スタンバイ hello 時間	3 秒
スタンバイ ホールドタイム	10 秒

HSRP 設定時の注意事項

- HSRPv2 および HSRPv1 は相互に排他的です。HSRPv2 は、同じインターフェイス上で HSRPv1 と一緒には動作しません（その逆も同様）。
- 以下の手順では、次に示すレイヤ 3 インターフェイスの 1 つを指定する必要があります。
  - ルーテッドポート：インターフェイス コンフィギュレーション モードで **no switchport** コマンドを入力することにより、レイヤ 3 ポートとして設定された物理ポート。
  - SVI：グローバル コンフィギュレーション モードで **interface vlan** *vlan_id* を使用して作成された VLAN インターフェイス。デフォルトではレイヤ 3 インターフェイスです。
  - レイヤ 3 モードの Etherchannel ポートチャネル：グローバル コンフィギュレーション モードで **interface port-channel** *port-channel-number* を使用し、イーサネット インターフェイスをチャネルグループにバインドして作成されたポートチャネル論理インターフェイス。
- すべてのレイヤ 3 インターフェイスに IP アドレスを割り当てる必要があります。

（注） HSRP のミリ秒タイマーはサポートされません。

HSRP のイネーブル化

standby ip インターフェイス コンフィギュレーション コマンドは、設定されているインターフェイスで HSRP をアクティブにします。IP アドレスを指定した場合は、IP アドレスがホットスタンバイ グループの指定アドレスとして使用されます。IP アドレスを指定しなかった場合は、スタンバイ機能によってアドレスが学習されます。指定アドレスを使用し、LAN 上に少なくとも 1 つのレイヤ 3 ポートを設定する必要があります。IP アドレスを設定すると、常に、現在使用されている別の指定アドレスが、設定した IP アドレスに変更されます。

standby ip コマンドがインターフェイス上で有効にされており、プロキシ ARP が有効な場合、インターフェイスのホットスタンバイ状態がアクティブになると、プロキシ ARP 要求に対する応答は、ホットスタンバイグループの MAC アドレスを使用して実行されます。インターフェイスが別のステートの場合、プロキシ ARP の応答は抑制されます。

手順の概要

1. **configure terminal**
2. **interface** *interface-id*
3. **standby version** { **1** | **2** }
4. **standby** [*group-number*] **ip** [*ip-address* [**secondary**]]
5. **end**
6. **show standby** [*interface-id* [*group*]]
7. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch(config)# 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 2	**interface** *interface-id* 例： `Switch(config)# interface gigabitethernet1/0/1`	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、HSRP をイネーブルにするレイヤ 3 インターフェイスを入力します。
ステップ 3	**standby version** ｛ **1** ｜ **2** ｝ 例： `Switch(config-if)# standby version 1`	（任意）インターフェイスに HSRP バージョンを設定します。 • 1：HSRPv1 を選択します。 • 2：HSRPv2 を選択します。 このコマンドを入力しない場合、またはキーワードを指定しない場合、インターフェイスはデフォルトの HSRP バージョンである HSRPv1 を実行します。
ステップ 4	**standby** ［*group-number*］**ip** ［*ip-address* ［**secondary**］］ 例： `Switch(config-if)# standby 1 ip`	HSRP グループの番号および仮想 IP アドレスを使用して、HSRP グループを作成（またはイネーブルに）します。 • （任意）group-number：HSRP をイネーブルにするインターフェイスのグループ番号を指定します。指定できる範囲は 0 ～ 255 です。デフォルトは 0 です。HSRP グループが 1 つしかない場合は、グループ番号を入力する必要はありません。 • （1 つのインターフェイスで必須、それ以外は任意）ip-address：ホットスタンバイ ルータ インターフェイスの仮想 IP アドレスを指定します。少なくとも 1 つのインターフェイスに対して仮想 IP アドレスを入力する必要があります。他のインターフェイスは、その仮想 IP アドレスを学習します。 • （任意）**secondary**：IP アドレスがセカンダリ ホット スタンバイ ルータ インターフェイスであることを指定します。ルータがセカンダリ ルータとスタンバイ ルータのいずれにも指定されず、かつプライオリティも設定されていない場合は、プライマリ IP アドレスが比較され、IP アドレスが大きいルータがアクティブ ルータ、

	コマンドまたはアクション	目的
		IP アドレスが 2 番めに大きいルータがスタンバイ ルータになります。
ステップ 5	**end** 例： `Switch(config-if)# end`	特権 EXEC モードに戻ります
ステップ 6	**show standby** [*interface-id* [*group*]] 例： `Switch # show standby`	スタンバイ グループの設定を確認します。
ステップ 7	**copy running-config startup-config** 例： `Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

HSRP のプライオリティの設定

standby priority, **standby preempt**、および **standby track** インターフェイス コンフィギュレーション コマンドはいずれも、アクティブ ルータとスタンバイ ルータを検索するための特性、および新しいアクティブ ルータが処理を引き継いだ場合の動作を設定するために使用できます。

HSRP プライオリティを設定する場合の注意事項は、次のとおりです。

- プライオリティを割り当てておくと、アクティブ ルータおよびスタンバイ ルータを選択できます。プリエンプションがイネーブルの場合は、プライオリティが最高のルータがアクティブルータになります。プライオリティが等しい場合は、現在アクティブなルータに変更はありません。
- 最大の値（1 ～ 255）が、最高のプライオリティ（アクティブ ルータになる確率が最も高い）を表します。
- プライオリティ、プリエンプト、またはその両方を設定するときは、少なくとも 1 つのキーワード（**priority**、**preempt**、または両方）を指定する必要があります。
- インターフェイスが **standby track** コマンドによって設定されている場合、ルータ上の別のインターフェイスがダウンすると、デバイスのプライオリティが動的に変更されることもあります。
- **standby track** インターフェイス コンフィギュレーション コマンドを実行すると、ルータのホットスタンバイ プライオリティとインターフェイスのアベイラビリティが関連付けられます。この機能は、HSRP 用に設定されていないインターフェイスを追跡する場合に有効です。追跡対象のインターフェイスが故障すると、トラッキングが設定されているデバイスのホットスタンバイ プライオリティが 10 減少します。追跡対象でないインターフェイスの場合は、そのステートが変わっても、設定済みデバイスのホットスタンバイ プライ

オリティは変わりません。ホットスタンバイ用に設定されたインターフェイスごとに、追跡するインターフェイスのリストを個別に設定できます。

- **standby track** *interface-priority* インターフェイス コンフィギュレーション コマンドを実行すると、追跡対象のインターフェイスがダウンした場合のホットスタンバイ優先順位の減少幅を指定できます。インターフェイスが稼働状態に戻ると、プライオリティは同じ分だけ増加します。
- *interface-priority* 値が設定されている場合に、複数の追跡対象インターフェイスがダウンすると、設定済みプライオリティの減少幅が累積されます。プライオリティ値が設定されていない追跡対象インターフェイスが故障した場合、デフォルトの減少幅は 10 です。この値は累積されません。
- インターフェイスに対してルーティングを最初にイネーブルにした時点で、完全なルーティングテーブルは存在しません。このインターフェイスがプリエンプトに設定されている場合はアクティブルータになりますが、十分なルーティング処理はできません。この問題を解決するには、ルータがルーティングテーブルを更新できるように遅延時間を設定します。

インターフェイスに HSRP プライオリティ特性を設定するには、特権 EXEC モードで次の手順を実行します。

手順の概要

1. **configure terminal**
2. **interface** *interface-id*
3. **standby** ［*group-number*］ **priority***priority*
4. **standby** ［*group-number*］ **preempt** ［**delay** ［**minimum***seconds*］ ［**reload***seconds*］ ［**sync***seconds*］］
5. **standby** ［*group-number*］ **track** *type number* ［*interface-priority*］
6. **end**
7. **show running-config**
8. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch # 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 2	**interface** *interface-id* 例： `Switch(config)# interface gigabitethernet1/0/1`	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、プライオリティを設定する HSRP インターフェイスを入力します。
ステップ 3	**standby** ［*group-number*］ **priority***priority* 例：	アクティブ ルータを選択するときに使用される **priority** 値を設定します。指定できる範囲は 1 ～ 255 です。デフォルト プライオリティは 100 です。最大の値が、最高のプライオリティを表します。

	コマンドまたはアクション	目的
	`Switch(config-if)# standby 120 priority 50`	• （任意）group-number：コマンドが適用されるグループ番号です。 デフォルト値に戻すには、このコマンドの **no** 形式を使用します。
ステップ 4	**standby** ［*group-number*］ **preempt** ［**delay** ［**minimum***seconds*］ ［**reload***seconds*］ ［**sync***seconds*］］ 例： `Switch(config-if)# standby 1 preempt delay 300`	ルータを **preempt** に設定し、ローカル ルータのプライオリティがアクティブ ルータよりも高い場合は、アクティブ ルータとなります。 • （任意）group-number：コマンドが適用されるグループ番号です。 • （任意）**delay minimum**：ローカル ルータがアクティブ ルータの役割を引き継ぐまでの時間を、指定された秒数だけ延期します。指定できる範囲は 0 ～ 3600 秒（1 時間）で、デフォルトは 0 です（引き継ぐ前の遅延はありません）。 • （任意）**delay reload**：ローカル ルータがリロードの後アクティブ ルータの役割を引き継ぐまでの時間を、指定された秒数だけ延期します。指定できる範囲は 0 ～ 3600（1 時間）で、デフォルトは 0 です（リロードの後、引き継ぐ前の遅延はありません）。 • （任意）**delay sync**：IP 冗長性クライアントが応答できるように（ok または wait 応答）、ローカル ルータがアクティブ ルータの役割を引き継ぐまでの時間を、指定された秒数だけ延期します。指定できる範囲は 0 ～ 3600 秒（1 時間）で、デフォルトは 0 です（引き継ぐ前の遅延はありません）。 デフォルト値に戻すには、このコマンドの **no** 形式を使用します。
ステップ 5	**standby** ［*group-number*］ **track** *type number* ［*interface-priority*］ 例： `Switch(config-if)# standby track interface gigabitethernet1/1/1`	他のインターフェイスを追跡するようにインターフェイスを設定します。この設定により、他のインターフェイスの 1 つがダウンした場合は、そのデバイスのホットスタンバイ プライオリティが減少します。 • （任意）group-number：コマンドが適用されるグループ番号です。 • type：追跡対象のインターフェイス タイプを（インターフェイス番号とともに）入力します。

	コマンドまたはアクション	目的
		• number：追跡対象のインターフェイス番号を（インターフェイス タイプとともに）入力します。 • （任意）interface-priority：インターフェイスがダウンした場合、または稼働状態に戻った場合に、ルータのホットスタンバイ プライオリティを減少または増加させる幅を入力します。デフォルト値は 10 です。
ステップ 6	**end** 例： `Switch(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 7	**show running-config**	スタンバイ グループの設定を確認します。
ステップ 8	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

MHSRP の設定

MHSRP およびロード バランシングをイネーブルにするには、MHSRP の項の *MHSRP* ロード シェアリングの図に示したように、グループのアクティブ ルータとして 2 つのルータを設定し、スタンバイ ルータとして仮想ルータを設定します。ルータに障害が発生して正常に戻った場合、プリエンプションを発生させてロードバランシングを復元するために、**standby preempt** インターフェイス コンフィギュレーション コマンドをそれぞれの HSRP インターフェイスで入力する必要があります。

ルータ A はグループ 1 のアクティブ ルータとして、ルータ B はグループ 2 のアクティブ ルータとして設定されています。ルータ A の HSRP インターフェイスの IP アドレスは 10.0.0.1、グループ 1 のスタンバイ プライオリティは 110（デフォルトは 100）です。ルータ B の HSRP インターフェイスの IP アドレスは 10.0.0.2、グループ 2 のスタンバイ プライオリティは 110 です。

グループ 1 は仮想 IP アドレス 10.0.0.3 を使用し、グループ 2 は仮想 IP アドレス 10.0.0.4 を使用します。

ルータ A の設定

手順の概要

1. **configure terminal**
2. **interface** *type number*
3. **no switchport**
4. **ip address** *ip-address mask*
5. **standby** [*group-number*] **ip** [*ip-address* [**secondary**]]

6. **standby** ［*group-number*］ **priority** *priority*
7. **standby** ［*group-number*］**preempt**［**delay**［**minimum** *seconds*］［**reload** *seconds*］［**sync** *seconds*］］
8. **standby**［*group-number*］**ip**［*ip-address*［**secondary**］］
9. **standby** ［*group-number*］**preempt**［**delay**［**minimum** *seconds*］［**reload** *seconds*］［**sync** *seconds*］］
10. **end**
11. **show running-config**
12. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch # 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 2	**interface** *type number* 例： `Switch (config)# interface gigabitethernet1/0/1`	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 3	**no switchport** 例： `Switch (config)# no switchport`	レイヤ 2 モードになっているインターフェイスを、レイヤ 3 設定用にレイヤ 3 モードに切り替えます。
ステップ 4	**ip address** *ip-address mask* 例： `Switch (config-if)# ip address 10.0.0.1 255.255.255.0`	インターフェイスの IP アドレスを指定します。
ステップ 5	**standby**［*group-number*］**ip**［*ip-address*［**secondary**］］ 例： `Switch (config-if)# standby 1 ip 10.0.0.3`	HSRP グループの番号および仮想 IP アドレスを使用して、HSRP グループを作成します。 • （任意）*group-number*：HSRP をイネーブルにするインターフェイスのグループ番号を指定します。指定できる範囲は 0 ～ 255 です。デフォルトは 0 です。HSRP グループが 1 つしかない場合は、グループ番号を入力する必要はありません。 • （1 つのインターフェイスで必須、それ以外は任意）*ip-address*：ホットスタンバイ ルータ インターフェイスの仮想 IP アドレスを指定します。少なくとも 1 つのインターフェイスに対して仮想 IP アドレスを入力する必要があります。他のインターフェイスは、その仮想 IP アドレスを学習します。

	コマンドまたはアクション	目的
		• （任意）**secondary**：IP アドレスがセカンダリ ホット スタンバイ ルータ インターフェイスであることを指定します。ルータがセカンダリ ルータとスタンバイ ルータのいずれにも指定されず、かつプライオリティも設定されていない場合は、プライマリ IP アドレスが比較され、IP アドレスが大きいルータがアクティブ ルータ、IP アドレスが 2 番めに大きいルータがスタンバイ ルータになります。
ステップ 6	**standby** ［*group-number*］ **priority** *priority* 例： `Switch(config-if)# standby 1 priority 110`	アクティブ ルータを選択するときに使用される **priority** 値を設定します。指定できる範囲は 1 ～ 255 です。デフォルト プライオリティは 100 です。最大の値が、最高のプライオリティを表します。 • （任意）*group-number*：コマンドが適用されるグループ番号です。 デフォルト値に戻すには、このコマンドの **no** 形式を使用します。
ステップ 7	**standby** ［*group-number*］ **preempt** ［**delay** ［**minimum** *seconds*］ ［**reload** *seconds*］ ［**sync** *seconds*］］ 例： `Switch(config-if)# standby 1 preempt delay 300`	ルータを **preempt** に設定し、ローカル ルータのプライオリティがアクティブ ルータよりも高い場合は、アクティブ ルータとなります。 • （任意）group-number：コマンドが適用されるグループ番号です。 • （任意）**delay minimum**：ローカル ルータがアクティブ ルータの役割を引き継ぐまでの時間を、指定された秒数だけ延期します。指定できる範囲は 0 ～ 3600 秒（1 時間）で、デフォルトは 0 です（引き継ぐ前の遅延はありません）。 • （任意）**delay reload**：ローカル ルータがリロードの後アクティブ ルータの役割を引き継ぐまでの時間を、指定された秒数だけ延期します。指定できる範囲は 0 ～ 3600（1 時間）で、デフォルトは 0 です（リロードの後、引き継ぐ前の遅延はありません）。 • （任意）**delay sync**：IP 冗長性クライアントが応答できるように（ok または wait 応答）、ローカル ルータがアクティブ ルータの役割を引き継ぐまでの時間を、指定された秒数だけ延期します。指定できる範囲は 0 ～ 3600 秒（1 時間）

	コマンドまたはアクション	目的
		で、デフォルトは0です（引き継ぐ前の遅延はありません）。 デフォルト値に戻すには、このコマンドの **no** 形式を使用します。
ステップ **8**	**standby** [*group-number*] **ip** [*ip-address* [**secondary**]] 例： `Switch (config-if)# standby 2 ip 10.0.0.4`	HSRP グループの番号および仮想 IP アドレスを使用して、HSRP グループを作成します。 • （任意）*group-number*：HSRP をイネーブルにするインターフェイスのグループ番号を指定します。指定できる範囲は0～255です。デフォルトは 0 です。HSRP グループが 1 つしかない場合は、グループ番号を入力する必要はありません。 • （1つのインターフェイスで必須、それ以外は任意）*ip-address*：ホットスタンバイ ルータ インターフェイスの仮想 IP アドレスを指定します。少なくとも1つのインターフェイスに対して仮想IPアドレスを入力する必要があります。他のインターフェイスは、その仮想 IP アドレスを学習します。 • （任意）**secondary**：IP アドレスがセカンダリ ホット スタンバイ ルータ インターフェイスであることを指定します。ルータがセカンダリ ルータとスタンバイ ルータのいずれにも指定されず、かつプライオリティも設定されていない場合は、プライマリ IPアドレスが比較され、IP アドレスが大きいルータがアクティブ ルータ、IP アドレスが 2 番めに大きいルータがスタンバイ ルータになります。
ステップ **9**	**standby** [*group-number*] **preempt** [**delay** [**minimum** *seconds*] [**reload** *seconds*] [**sync** *seconds*]] 例： `Switch(config-if)# standby 2 preempt delay 300`	ルータを **preempt** に設定し、ローカル ルータのプライオリティがアクティブ ルータよりも高い場合は、アクティブ ルータとなります。 • （任意）group-number：コマンドが適用されるグループ番号です。 • （任意）**delay minimum**：ローカル ルータがアクティブ ルータの役割を引き継ぐまでの時間を、指定された秒数だけ延期します。指定できる範囲は 0 ～ 3600 秒（1 時間）で、デフォルトは 0 です（引き継ぐ前の遅延はありません）。

	コマンドまたはアクション	目的
		• （任意）**delay reload**：ローカル ルータがリロードの後アクティブ ルータの役割を引き継ぐまでの時間を、指定された秒数だけ延期します。指定できる範囲は 0 ～ 3600（1 時間）で、デフォルトは 0 です（リロードの後、引き継ぐ前の遅延はありません）。 • （任意）**delay sync**：IP 冗長性クライアントが応答できるように（ok または wait 応答）、ローカル ルータがアクティブ ルータの役割を引き継ぐまでの時間を、指定された秒数だけ延期します。指定できる範囲は 0 ～ 3600 秒（1 時間）で、デフォルトは 0 です（引き継ぐ前の遅延はありません）。 デフォルト値に戻すには、このコマンドの **no** 形式を使用します。
ステップ 10	**end** 例： `Switch(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 11	**show running-config**	スタンバイ グループの設定を確認します。
ステップ 12	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

ルータ B の設定

手順の概要

1. **configure terminal**
2. **interface** *type number*
3. **no switchport**
4. **ip address** *ip-address mask*
5. **standby** ［*group-number*］ **ip** ［*ip-address* ［**secondary**］］
6. **standby** ［*group-number*］ **priority** *priority*
7. **standby** ［*group-number*］ **preempt** ［**delay** ［**minimum** *seconds*］ ［**reload** *seconds*］ ［**sync** *seconds*］］
8. **standby** ［*group-number*］ **ip** ［*ip-address* ［**secondary**］］
9. **standby** ［*group-number*］ **preempt** ［**delay** ［**minimum** *seconds*］ ［**reload** *seconds*］ ［**sync** *seconds*］］
10. **end**
11. **show running-config**
12. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch # 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 2	**interface** *type number* 例： `Switch (config)# interface gigabitethernet1/0/1`	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 3	**no switchport** 例： `Switch (config)# no switchport`	レイヤ 2 モードになっているインターフェイスを、レイヤ 3 設定用にレイヤ 3 モードに切り替えます。
ステップ 4	**ip address** *ip-address mask* 例： `Switch (config-if)# ip address 10.0.0.2 255.255.255.0`	インターフェイスの IP アドレスを指定します。
ステップ 5	**standby** [*group-number*] **ip** [*ip-address* [**secondary**]] 例： `Switch (config-if)# standby 1 ip 10.0.0.3`	HSRP グループの番号および仮想 IP アドレスを使用して、HSRP グループを作成します。 • （任意）*group-number*：HSRP をイネーブルにするインターフェイスのグループ番号を指定します。指定できる範囲は 0 ～ 255 です。デフォルトは 0 です。HSRP グループが 1 つしかない場合は、グループ番号を入力する必要はありません。 • （1 つのインターフェイスで必須、それ以外は任意）*ip-address*：ホット スタンバイ ルータ インターフェイスの仮想 IP アドレスを指定します。少なくとも 1 つのインターフェイスに対して仮想 IP アドレスを入力する必要があります。他のインターフェイスは、その仮想 IP アドレスを学習します。 • （任意）**secondary**：IP アドレスがセカンダリ ホット スタンバイ ルータ インターフェイスであることを指定します。ルータがセカンダリ ルータとスタンバイ ルータのいずれにも指定されず、かつプライオリティも設定されていない場合は、プライマリ IP アドレスが比較され、IP アドレスが大きいルータがアクティブ ルータ、IP アドレスが 2 番めに大きいルータがスタンバイ ルータになります。

	コマンドまたはアクション	目的
ステップ 6	**standby** ［*group-number*］ **priority** *priority* 例： `Switch(config-if)# standby 2 priority 110`	アクティブ ルータを選択するときに使用される **priority** 値を設定します。指定できる範囲は 1 ～ 255 です。デフォルト プライオリティは 100 です。最大の値が、最高のプライオリティを表します。 • （任意）*group-number*：コマンドが適用されるグループ番号です。 デフォルト値に戻すには、このコマンドの **no** 形式を使用します。
ステップ 7	**standby** ［*group-number*］ **preempt** ［**delay** ［**minimum** *seconds*］ ［**reload** *seconds*］ ［**sync** *seconds*］］ 例： `Switch(config-if)# standby 1 preempt delay 300`	ルータを **preempt** に設定し、ローカル ルータのプライオリティがアクティブ ルータよりも高い場合は、アクティブ ルータとなります。 • （任意）group-number：コマンドが適用されるグループ番号です。 • （任意）**delay minimum**：ローカル ルータがアクティブ ルータの役割を引き継ぐまでの時間を、指定された秒数だけ延期します。指定できる範囲は 0 ～ 3600 秒（1 時間）で、デフォルトは 0 です（引き継ぐ前の遅延はありません）。 • （任意）**delay reload**：ローカル ルータがリロードの後アクティブ ルータの役割を引き継ぐまでの時間を、指定された秒数だけ延期します。指定できる範囲は 0 ～ 3600（1 時間）で、デフォルトは 0 です（リロードの後、引き継ぐ前の遅延はありません）。 • （任意）**delay sync**：IP 冗長性クライアントが応答できるように（ok または wait 応答）、ローカル ルータがアクティブ ルータの役割を引き継ぐまでの時間を、指定された秒数だけ延期します。指定できる範囲は 0 ～ 3600 秒（1 時間）で、デフォルトは 0 です（引き継ぐ前の遅延はありません）。 デフォルト値に戻すには、このコマンドの **no** 形式を使用します。
ステップ 8	**standby** ［*group-number*］ **ip** ［*ip-address* ［**secondary**］］ 例： `Switch (config-if)# standby 2 ip 10.0.0.4`	HSRP グループの番号および仮想 IP アドレスを使用して、HSRP グループを作成します。 • （任意）*group-number*：HSRP をイネーブルにするインターフェイスのグループ番号を指定します。指定できる範囲は 0 ～ 255 です。デフォ

	コマンドまたはアクション	目的
		ルトは 0 です。HSRP グループが 1 つしかない場合は、グループ番号を入力する必要はありません。 • （1 つのインターフェイスで必須、それ以外は任意）*ip-address*：ホットスタンバイ ルータ インターフェイスの仮想 IP アドレスを指定します。少なくとも 1 つのインターフェイスに対して仮想 IP アドレスを入力する必要があります。他のインターフェイスは、その仮想 IP アドレスを学習します。 • （任意）**secondary**：IP アドレスがセカンダリ ホット スタンバイ ルータ インターフェイスであることを指定します。ルータがセカンダリ ルータとスタンバイ ルータのいずれにも指定されず、かつプライオリティも設定されていない場合は、プライマリ IP アドレスが比較され、IP アドレスが大きいルータがアクティブ ルータ、IP アドレスが 2 番めに大きいルータがスタンバイ ルータになります。
ステップ 9	**standby** ［*group-number*］ **preempt** ［**delay** ［**minimum** *seconds*］ ［**reload** *seconds*］ ［**sync** *seconds*］］ 例： `Switch(config-if)# standby 2 preempt delay 300`	ルータを **preempt** に設定し、ローカル ルータのプライオリティがアクティブ ルータよりも高い場合は、アクティブ ルータとなります。 • （任意）group-number：コマンドが適用されるグループ番号です。 • （任意）**delay minimum**：ローカル ルータがアクティブ ルータの役割を引き継ぐまでの時間を、指定された秒数だけ延期します。指定できる範囲は 0 ～ 3600 秒（1 時間）で、デフォルトは 0 です（引き継ぐ前の遅延はありません）。 • （任意）**delay reload**：ローカル ルータがリロードの後アクティブ ルータの役割を引き継ぐまでの時間を、指定された秒数だけ延期します。指定できる範囲は 0 ～ 3600（1 時間）で、デフォルトは 0 です（リロードの後、引き継ぐ前の遅延はありません）。 • （任意）**delay sync**：IP 冗長性クライアントが応答できるように（ok または wait 応答）、ローカル ルータがアクティブ ルータの役割を引き継ぐまでの時間を、指定された秒数だけ延期します。指定できる範囲は 0 ～ 3600 秒（1 時間）

	コマンドまたはアクション	目的
		で、デフォルトは0です（引き継ぐ前の遅延はありません）。 デフォルト値に戻すには、このコマンドの **no** 形式を使用します。
ステップ 10	**end** 例： `Switch(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 11	**show running-config**	スタンバイ グループの設定を確認します。
ステップ 12	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

HSRP 認証およびタイマーの設定

HSRP認証ストリングを設定したり、helloタイムインターバルやホールドタイムを変更することもできます。

これらの属性を設定する場合の注意事項は次のとおりです。

- 認証ストリングはすべてのHSRPメッセージで暗号化されずに送信されます。相互運用できるように、接続されたすべてのルータおよびアクセス サーバーに同じ認証ストリングを設定する必要があります。認証ストリングが一致しないと、HSRP によって設定された他のルータから、指定されたホットスタンバイ IP アドレスおよびタイマー値を学習できません。
- スタンバイ タイマー値が設定されていないルータまたはアクセス サーバーは、アクティブ ルータまたはスタンバイ ルータからタイマー値を学習できます。アクティブ ルータに設定されたタイマーは、常に他のタイマー設定よりも優先されます。
- ホットスタンバイ グループのすべてのルータで、同じタイマー値を使用する必要があります。通常、*holdtime* は *hellotime* の 3 倍以上です。

インターフェイスにHSRPの認証とタイマーを設定するには、特権EXECモードで次の手順を実行します。

手順の概要

1. **configure terminal**
2. **interface** *interface-id*
3. **standby**［*group-number*］ **authentication** *string*
4. **standby**［*group-number*］**timers** *hellotime holdtime*
5. **end**
6. **show running-config**
7. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch # 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 2	**interface** *interface-id* 例： `Switch(config) # interface gigabitethernet1/0/1`	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、プライオリティを設定する HSRP インターフェイスを入力します。
ステップ 3	**standby** [*group-number*] **authentication** *string* 例： `Switch(config-if) # standby 1 authentication word`	（任意）**authentication** *string*：すべての HSRP メッセージで伝達されるストリングを入力します。認証ストリングには 8 文字までを指定できます。デフォルトのストリングは **cisco** です。 （任意）*group-number*：コマンドが適用されるグループ番号です。
ステップ 4	**standby** [*group-number*] **timers** *hellotime holdtime* 例： `Switch(config-if) # standby 1 timers 5 15`	（任意）hello パケット間隔、およびアクティブ ルータのダウンを他のルータが宣言するまでの時間を設定します。 • *group-number*：コマンドが適用されるグループ番号です。 • *hellotime*：連続する hello パケット間のインターバルを秒単位で設定します。範囲は、1 ～ 255 秒です。デフォルトは 3 です。 • *holdtime*：ローカル ルータがリロードの後アクティブ ルータの役割を引き継ぐまでの時間を、指定された秒数だけ延期します。範囲は 0 ～ 3600 秒（1 時間）です。デフォルトは 0 です（リロードの後、引き継ぐ前の遅延はありません）。
ステップ 5	**end** 例： `Switch(config-if) # end`	特権 EXEC モードに戻ります。
ステップ 6	**show running-config**	スタンバイ グループの設定を確認します。
ステップ 7	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

ICMP リダイレクト メッセージの HSRP サポートのイネーブル化

HSRP が設定されたインターフェイスでは、ICMP リダイレクト メッセージが自動的にイネーブルになります。ICMP は、エラーをレポートするためのメッセージ パケットや IP 処理に関連する他の情報を提供する、ネットワーク層インターネット プロトコルです。ICMP には、ホストへのエラーパケットの方向付けや送信などの診断機能があります。この機能は、HSRP を介した発信 ICMP リダイレクト メッセージをフィルタリングします。HSRP では、ネクストホップ IP アドレスが HSRP 仮想 IP アドレスに変更される可能性があります。詳細については、『Cisco IOS IP Configuration Guide, Release 12.4』を参照してください。

HSRP グループおよびクラスタリングの設定

デバイスが HSRP スタンバイ ルーティングに参加し、クラスタリングがイネーブルの場合は、同じスタンバイ グループを使用して、コマンド スイッチの冗長性および HSRP の冗長性を確保できます。同じ HSRP スタンバイ グループをイネーブルにし、コマンドスイッチおよびルーティングの冗長性を確保するには、**cluster standby-group** *HSRP-group-name* [**routing-redundancy**] グローバル コンフィギュレーション コマンドを使用します。**routing-redundancy** キーワードを指定せずに同じ HSRP スタンバイ グループ名でクラスタを作成すると、そのグループに対する HSRP スタンバイ ルーティングはディセーブルになります。

HSRP の確認

HSRP コンフィギュレーションの確認

HSRP 設定を表示するには、次の特権 EXEC モードで次のコマンドを使用します。

show standby ［*interface-id*［*group*］］［**brief**］［**detail**］

スイッチ全体、特定のインターフェイス、HSRP グループ、またはインターフェイスの HSRP グループに関する HSRP 情報を表示できます。HSRP 情報の概要または詳細のいずれを表示するかを指定することもできます。デフォルトの表示は **detail** です。多数の HSRP グループがある場合に、修飾子を指定しないで **show standby** コマンドを使用すると、正確に表示されないことがあります。

例

```
Switch #show standby
VLAN1 - Group 1
Local state is Standby, priority 105, may preempt
Hellotime 3 holdtime 10
Next hello sent in 00:00:02.182
Hot standby IP address is 172.20.128.3 configured
Active router is 172.20.128.1 expires in 00:00:09
Standby router is local
Standby virtual mac address is 0000.0c07.ac01
Name is bbb

VLAN1 - Group 100
Local state is Standby, priority 105, may preempt
Hellotime 3 holdtime 10
Next hello sent in 00:00:02.262
```

```
Hot standby IP address is 172.20.138.51 configured
Active router is 172.20.128.1 expires in 00:00:09
Active router is local
Standby router is unknown expired
Standby virtual mac address is 0000.0c07.ac64
Name is test
```

HSRP の設定例

HSRP のイネーブル化：例

次に、インターフェイスのグループ 1 で HSRP をアクティブにする例を示します。ホットスタンバイ グループで使用される IP アドレスは、HSRP を使用して学習されます。

（注） これは、HSRP をイネーブルにするために必要な最小限の手順です。その他の設定は任意です。

```
Switch # configure terminal
Switch(config) # interface gigabitethernet1/0/1
Switch(config-if)# no switchport
Switch(config-if)# standby 1 ip
Switch(config-if)# end
Switch # show standby
```

HSRP のプライオリティの設定：例

次に、ポートをアクティブにして、IP アドレスおよびプライオリティ 120（デフォルト値よりも高いプライオリティ）を設定して、アクティブ ルータになるまで 300 秒（5 分間）待機する例を示します。

```
Switch # configure terminal
Switch(config) # interface gigabitethernet1/0/1
Switch(config-if)# no switchport
Switch(config-if)# standby ip 172.20.128.3
Switch(config-if)# standby priority 120 preempt delay 300
Switch(config-if)# end
Switch # show standby
```

MHSRP の設定：例

次に、*MHSRP* ロード シェアリングの図で示した MHSRP 設定をイネーブルにする例を示します。

ルータ A の設定

```
Switch # configure terminal
Switch(config) # interface gigabitethernet1/0/1
Switch(config-if)# no switchport
Switch(config-if)# ip address 10.0.0.1 255.255.255.0
Switch(config-if)# standby ip 10.0.0.3
```

```
Switch(config-if)# standby 1 priority 110
Switch(config-if)#  standby 1 preempt
Switch(config-if)# standby 2 ip 10.0.0.4
Switch(config-if)#  standby 2 preempt
Switch(config-if)# end
```

ルータ B の設定

```
Switch # configure terminal
Switch(config) # interface gigabitethernet1/0/1
Switch(config-if)# no switchport
Switch(config-if)# ip address 10.0.0.2 255.255.255.0
Switch(config-if)# standby ip 10.0.0.3
Switch(config-if)#  standby 1 preempt
Switch(config-if)# standby 2 ip 10.0.0.4
Switch(config-if)# standby 2 priority 110
Switch(config-if)#  standby 2 preempt
Switch(config-if)# end
```

HSRP 認証およびタイマーの設定：例

次に、グループ 1 のホットスタンバイ ルータを相互運用させるために必要な認証ストリングとして、word を設定する例を示します。

```
Switch # configure terminal
Switch(config) # interface gigabitethernet1/0/1
Switch(config-if)# no switchport
Switch(config-if)# standby 1 authentication word
Switch(config-if)# end
```

次に、hello パケット間隔が 5 秒、ルータがダウンしたと見なされるまでの時間が 15 秒となるように、スタンバイ グループ 1 のタイマーを設定する例を示します。

```
Switch # configure terminal
Switch(config) # interface gigabitethernet1/0/1
Switch(config-if)# no switchport
Switch(config-if)# standby 1 ip
Switch(config-if)# standby 1 timers 5 15
Switch(config-if)# end
```

HSRP グループおよびクラスタリングの設定：例

次に、スタンバイ グループ my_hsrp をクラスタにバインドし、同じ HSRP グループをイネーブルにしてコマンド スイッチおよびルータの冗長性に使用する例を示します。このコマンドを実行できるのは、コマンド スイッチに対してだけです。スタンバイ グループの名前または番号が存在しない場合、またはスイッチがクラスタ メンバー スイッチである場合は、エラー メッセージが表示されます。

```
Switch # configure terminal
Switch(config) # cluster standby-group my_hsrp routing-redundancy
Switch(config-if)# end
```

HSRP の設定に関する追加情報

標準および RFC

標準/RFC	タイトル
RFC 2281	『Cisco Hot Standby Router Protocol』

MIB

MIB	MIB のリンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

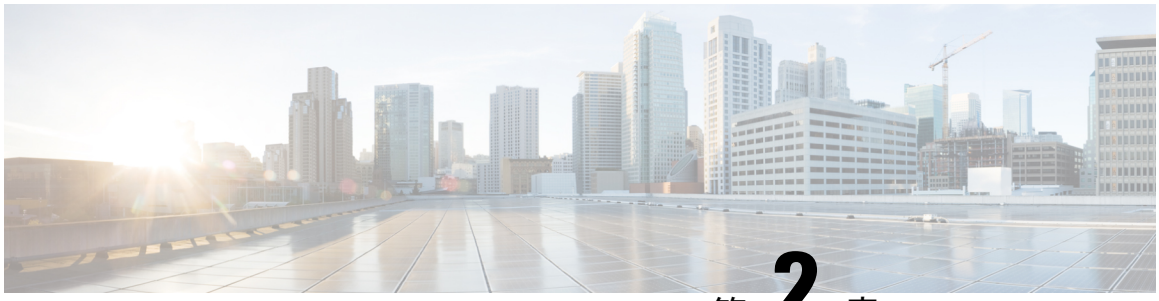
シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

HSRP の設定に関する機能情報

表 *2 : HSRP* の設定に関する機能情報

リリース	機能情報
Cisco IOS XE Everest 16.5.1a	この機能が導入されました。



第 2 章

NHRP の設定

NHRP の設定

Next Hop Resolution Protocol（NHRP）は、すべてのトンネル エンド ポイントを手動で設定するのではなく、ノンブロードキャストマルチアクセス（NBMA）ネットワークをダイナミックにマッピングする Address Resolution Protocol（ARP）と同様のプロトコルです。NHRP を使用すると、NBMA ネットワークに接続されたシステムは、そのネットワークに参加している他のシステムの NBMA（物理）アドレスをダイナミックに学習でき、これらのシステムが直接通信できるようになります。このプロトコルでは、ステーションのデータリンク アドレスを動的に決定することができる ARP と同様のソリューションが提供されます。

NHRP は、ハブがネクスト ホップ サーバ（NHS）であり、スポークがネクスト ホップ クライアント（NHC）である、クライアントおよびサーバのプロトコルです。ハブには、各スポークのパブリック インターフェイス アドレスが格納された NHRP データベースが保持されます。各スポークでは、起動時に NBMA 以外の（実際の）アドレスが登録され、ダイレクト トンネルを確立する場合は、NHRPデータベースに対し、宛先スポークのアドレスに関する照会が行われます。

このモジュールでは、Generic Routing Encapsulation（GRE）によって NHRP を設定する方法について説明します。Cisco IOS XE Denali 16.3.1 では、NHRP はスポーク設定のみをサポートします。

NHRP の設定に関する情報

NHRP および NBMA のネットワークの相互作用

WAN ネットワークのほとんどは、ポイントツーポイント リンクの集まりです。仮想トンネル ネットワーク（総称ルーティング カプセル化（GRE）トンネルなど）もまた、ポイントツーポイント リンクの集まりです。これらのポイントツーポイント リンクの接続を効率的にスケーリングするために、通常は、単一またはマルチレイヤのハブアンドスポーク ネットワークにグループ化します。マルチポイント インターフェイス（GRE トンネル インターフェイスなど）

を使用して、このようなネットワークのハブルータの設定を減らすことができます。その結果として生じるネットワークが NBMA ネットワークです。

単一のマルチポイント インターフェイスを通って到達可能なトンネル エンドポイントが複数あるため、この NBMA ネットワークを介してトンネル インターフェイスからパケットを転送するには、論理トンネル エンドポイントの IP アドレスから物理トンネル エンドポイントの IP アドレスへのマッピングが必要です。このマッピングはスタティックに設定することが可能ですが、これは、マッピングがダイナミックに検出または学習できる場合に推奨します。

NHRP は、これらの NBMA ネットワークの問題を軽減する ARP と同様のプロトコルです。NHRP を使用すると、NBMA ネットワークに接続されているシステムは、ネットワークの一部である他のシステムの NBMA アドレスをダイナミックに学習します。このため、これらのシステムは、トラフィックに中間ホップを使用せずに直接通信できるようになります。

ルータ、アクセス サーバ、およびホストは、NHRP を使用して、NBMA ネットワークに接続された他のルータおよびホストのアドレスを検出できます。部分メッシュ NBMA ネットワークには通常、NBMA ネットワークの背後に複数の論理ネットワークがあります。このような構成において、NBMA ネットワークを通るパケットは、出口ルータ（宛先ネットワークに最も近いルータ）に到着するまでに、NBMA ネットワーク上で複数のホップを発生させる必要がある場合があります。

NHRP 登録によって、これらの NBMA ネットワークのサポートが可能になります。

- NHRP 登録：NHRP を使用して、ネクスト ホップ クライアント（NHC）がネクスト ホップ サーバ（NHS）にダイナミックに登録されます。この登録機能により、特に、NHC がダイナミック物理 IP アドレスを持つか、物理 IP アドレスをダイナミックに変更するネットワーク アドレス変換（NAT）ルータの背後にある場合には、NHS で設定を変更しなくても、NHC が NBMA ネットワークに参加できるようになります。この場合、NHC の論理（VPN IP アドレス）と物理（NBMA IP）のマッピングを NHS で事前に設定することができません。

ダイナミックに構築されたハブアンドスポーク ネットワーク

NHRP により、NBMA ネットワークは最初、スポークの NHC とハブの NHS から複数の階層レイヤを構成できるハブアンドスポーク ネットワークとして配置されます。NHC は、NHS に到達するためのスタティック マッピング情報を使用して設定され、NHS に接続して NHRP 登録を NHS に送信します。この設定により、NHS はスポークのマッピング情報をダイナミックに学習できるため、ハブで必要な設定が減り、さらにスポークでダイナミック NBMA（物理）IP アドレスを取得できるようになります。

NHRP の設定方法

インターフェイス上での NHRP のイネーブル化

スイッチ上のインターフェイスに対して NHRP をイネーブルにするには、次の作業を行います。一般に、論理 NBMA ネットワーク内のすべての NHRP ステーションは、同じネットワーク ID を使用して設定する必要があります。

2 つ以上の NHRP ドメイン（GRE トンネル インターフェイス）が同じ NHRP ノード（スイッチ）で使用可能な場合は、NHRP ネットワーク ID を使用して、NHRP インターフェイスの NHRP ドメインを定義し、複数の NHRP ドメイン間またはネットワーク間で区別します。NHRP ネットワーク ID を使用すると、2 つの NHRP ネットワーク（クラウド）を同じスイッチ上に設定する場合に、それぞれを分けるのに役立ちます。

NHRP ネットワーク ID はローカル専用のパラメータです。これは、ローカル スイッチだけに対して意味があり、NHRP パケットで他の NHRP ノードに送信されることはありません。この理由から、2 台のスイッチが同じ NHRP ドメインに存在する場合、スイッチで設定される NHRP ネットワーク ID の実際の値は、もう一方のスイッチの NHRP ネットワーク ID と一致する必要はありません。NHRP パケットが GRE インターフェイス上に到着すると、そのインターフェイスで設定されている NHRP ネットワーク ID のローカル NHRP ドメインに割り当てられます。

同じ NHRP ネットワークに存在するすべてのスイッチ上の GRE インターフェイスでは、同じ NHRP ネットワーク ID を使用することを推奨します。こうすると、どの GRE インターフェイスがどの NHRP ネットワークのメンバであるかを追跡しやすくなります。

NHRP ドメイン（ネットワーク ID）は、スイッチ上の各 GRE トンネル インターフェイスで固有に設定できます。NHRP ドメインは、ルート上の GRE トンネル インターフェイス間をまたぐことができます。この場合、GRE トンネル インターフェイスで同じ NHRP ネットワーク ID を使用する効果は、2 つの GRE インターフェイスが単一の NHRP ネットワークに統合されることです。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip address** *ip-address network-mask*
5. **ip nhrp network-id** *number*
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> 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： `Switch# 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	**interface** *type number* 例： `Switch(config)# interface tunnel 100`	インターフェイスを設定し、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 network-mask* 例： `Switch(config-if)# ip address 10.0.0.1 255.255.255.0`	IP をイネーブルにし、インターフェイスに IP アドレスを提供します。
ステップ 5	**ip nhrp network-id** *number* 例： `Switch(config-if)# ip nhrp network-id 1`	インターフェイスで NHRP を有効にします。
ステップ 6	**end** 例： `Switch(config)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

マルチポイント動作のための GRE トンネルの設定

マルチポイント（NMBA）動作のためのGREトンネルを設定するには、次の作業を行います。

マルチポイント トンネル インターフェイスのトンネル ネットワークは、NBMA ネットワークと見なすことができます。同じスイッチ上で複数の GRE トンネルを設定する場合は、固有のトンネル ID キーまたは固有のトンネル送信元アドレスのいずれかを持っている必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip address** *ip-address*
5. **ip mtu** *bytes*
6. **ip pim sparse-dense-mode**
7. **ip nhrp map** *ip-address nbma-address*
8. **ip nhrp map multicast** *nbma-address*
9. **ip nhrp network-id** *number*
10. **ip nhrp nhs** *nhs-address*
11. **tunnel source vlan** *interface-number*
12. **tunnel destination** *ip-address*
13. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> 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： `Switch# 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： `Switch(config)# interface tunnel 100`	インターフェイスを設定し、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* 例： `Switch(config-if)# ip address 172.16.1.1 255.255.255.0`	インターフェイスに IP アドレスを設定します。
ステップ 5	**ip mtu** *bytes* 例： `Switch(config-if)# ip mtu 1400`	各インターフェイスにおいて送信される IP パケットの最大伝送単位（MTU）サイズを設定します。
ステップ 6	**ip pim sparse-dense-mode** 例： `Switch(config-if)# ip pim sparse-dense-mode`	インターフェイスで Protocol Independent Multicast（PIM）をイネーブルにし、マルチキャスト グループの動作モードに応じて、インターフェイスをスパース モード動作またはデンス モード動作で処理します。
ステップ 7	**ip nhrp map** *ip-address nbma-address* 例： `Switch(config-if)# ip nhrp map 172.16.1.2 10.10.10.2`	非ブロードキャストマルチアクセス（NBMA）ネットワークに接続する宛先 IP アドレスの IP/NBMA アドレスマッピングをスタティックに設定します。 • *ip-address*：NBMA ネットワークを介して到達可能な宛先の IP アドレス。このアドレスは、NBMA アドレスにマッピングされます。 • *nbma-address*：NBMA ネットワークを介して直接到達可能な NBMA アドレス。アドレスの形式は、使用しているメディアによって異なります。たとえば、ATM はネットワーク サービス アクセス ポイント（NSAP）アドレスを所有し、イーサネットはMACアドレスを所有し、

	コマンドまたはアクション	目的
		Switched Multimegabit Data Service（SMDS）は E.164 アドレスを所有しています。このアドレスは、IP アドレスにマッピングされます。
ステップ 8	**ip nhrp map multicast** *nbma-address* 例： `Switch(config-if)# ip nhrp map multicast 10.10.10.2`	ブロードキャストの接続先として、またはトンネルネットワークを介して送信されるマルチキャストパケットとして使用されるノンブロードキャストマルチアクセス（NBMA）アドレスを設定します。
ステップ 9	**ip nhrp network-id** *number* 例： `Switch(config-if)# ip nhrp network-id 1`	インターフェイスで Next Hop Resolution Protocol（NHRP）を有効にします。 • *number*：非ブロードキャスト マルチアクセス（NBMA）ネットワークからの、グローバルに一意である 32 ビットのネットワーク ID。範囲は 1 ～ 4294967295 です。
ステップ 10	**ip nhrp nhs** *nhs-address* 例： `Switch(config-if)# ip nhrp nhs 172.16.1.2`	1 つ以上の NHRP サーバのアドレスを指定します。 • *nhs-address*：指定したネクストホップ サーバのアドレス。
ステップ 11	**tunnel source vlan** *interface-number* 例： `Switch(config-if)# tunnel source vlan 1`	トンネル インターフェイスの送信元アドレスを設定します。
ステップ 12	**tunnel destination** *ip-address* 例： `Switch(config-if)# tunnel destination 10.10.10.2`	トンネル インターフェイスの宛先アドレスを設定します。
ステップ 13	**end** 例： `Switch(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

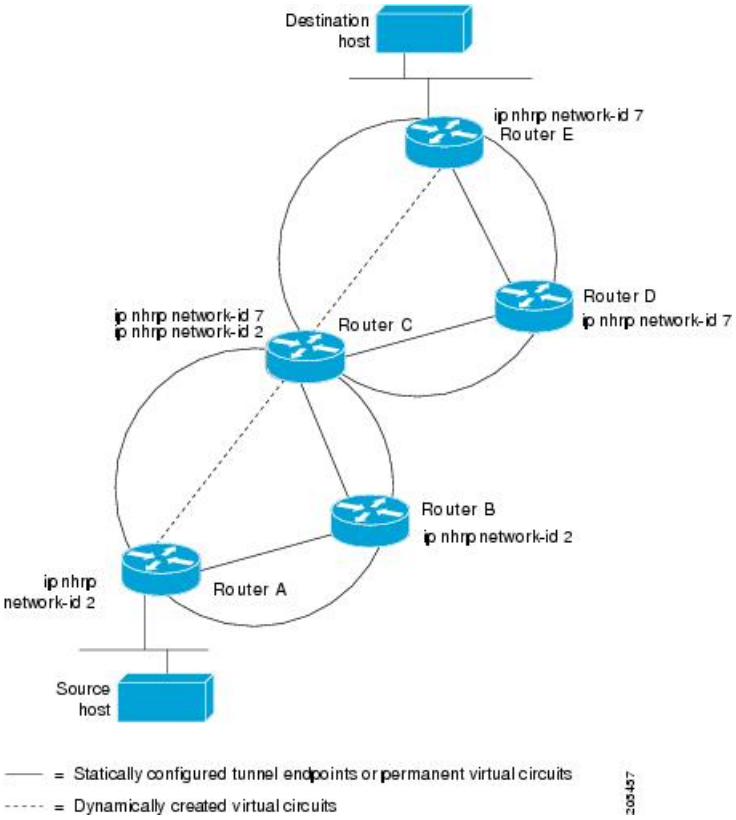
NHRP の設定例

論理 NBMA の物理ネットワーク設計の例

論理 NBMA ネットワークは、NHRP に参加し、同じネットワーク ID を持つインターフェイスおよびホストのグループと考えられます。次の図に、単一の物理 NBMA ネットワーク上に設

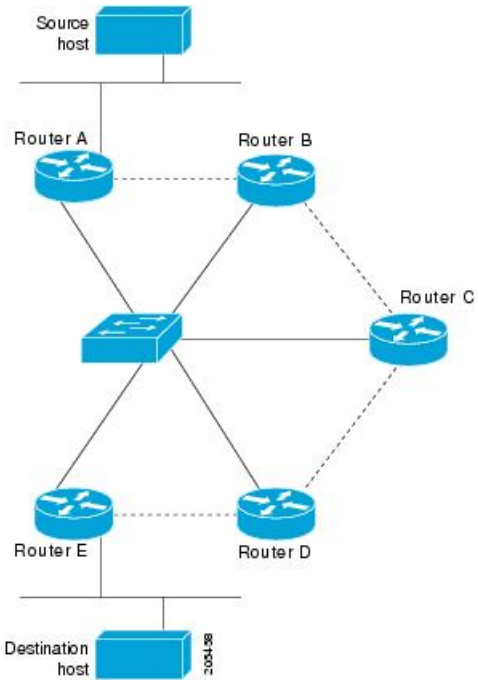
定された（円で示される）2 つの論理 NBMA ネットワークを示します。ルータ A はルータ B およびルータ C と通信できます。それらが同じネットワーク ID（2）を共有するためです。また、ルータ C はルータ D およびルータ E とも通信できます。それらがネットワーク ID 7 を共有するためです。アドレス解決が完了した後、点線で示すように、ルータ A は IP パケットをホップ 1 回でルータ C に送信でき、ルータ C はそれをホップ 1 回でルータ E に送信できます。

図 *3 : 1* つの物理 *NBMA* ネットワーク上の *2* つの論理 *NBMA* ネットワーク



上図の 5 台のルータによる物理構成は、実際には下図のような構成である場合もあります。送信元ホストはルータ A に接続されており、宛先ホストはルータ E に接続されています。同じスイッチが 5 つのすべてのルータにサービスを提供し、1 つの物理 NBMA ネットワークを構成しています。

図 *4: NBMA* ネットワーク例の物理構成



ここでも、上の最初の図を参照してください。最初、送信元ホストから宛先ホストへの IP パケットは、NHRP が NBMA アドレスでも解決するようになるまで、スイッチに接続された 5 台すべてのルータを通過して宛先に到達します。ルータ A は、IP パケットを初めて宛先ホストに向けて転送したときに、宛先ホストの IP アドレスに対する NHRP 要求も生成します。その要求がルータ C に転送され、応答が生成されます。2 つの論理 NBMA ネットワーク間の出力ルータであるため、ルータ C が応答します。

同様に、ルータ C は独自の NHRP 要求を生成し、これに対して、ルータ E が応答します。この例でも、送信元と宛先の間に発生する IP トラフィックが NBMA ネットワークを通過するためには、2 回のホップが必要です。これは、2 つの論理 NBMA ネットワーク間で IP トラフィックを転送する必要があるためです。NBMA ネットワークが論理的に分かれていなければ、必要なホップは 1 回だけです。

例：マルチポイント動作のための GRE トンネル

マルチポイント トンネルを使用すると、単一のトンネル インターフェイスを複数のネイバー スイッチに接続できます。ポイントツーポイント トンネルとは異なり、トンネルの宛先を設定する必要がありません。実際に、設定したとしても、トンネルの宛先は IP マルチキャスト アドレスに対応させる必要があります。

次の例では、スイッチ A とルータ B がイーサネット セグメントを共有しています。マルチポイント トンネル ネットワーク上で最小の接続が設定されるため、部分メッシュ NBMA ネットワークとして扱うことができるネットワークが作成されます。スタティック NHRP マップ エントリにより、スイッチ A はスイッチ B への到達方法を理解していて、その逆も同様です。

次に、GRE マルチポイント トンネルを設定する例を示します。

スイッチ A の設定

```
Switch(config)# interface tunnel 100 !Tunnel interface configured for PIM traffic
Switch(config-if)# no ip redirects
Switch(config-if)# ip address 192.168.24.1 255.255.255.252
Switch(config-if)# ip mtu 1400
Switch(config-if)# ip pim sparse-dense-mode
Switch(config-if)# ip nhrp map 192.168.24.3 172.16.0.1 !NHRP may optionally be configured
 to dynamically discover tunnel end points.
Switch(config-if)# ip nhrp map multicast 172.16.0.1
Switch(config-if)# ip nhrp network-id 1
Switch(config-if)# ip nhrp nhs 192.168.24.3
Switch(config-if)# tunnel source vlan 1
Switch(config-if)# tunnel destination 172.16.0.1
Switch(config-if)# end
```

スイッチ B の設定

```
Switch(config)# interface tunnel 100
Switch(config-if)# no ip redirects
Switch(config-if)# ip address 192.168.24.2 255.255.255.252
Switch(config-if)# ip mtu 1400
Switch(config-if)# ip pim sparse-dense-mode
Switch(config-if)# ip nhrp map 192.168.24.4 10.10.0.3
Switch(config-if)# ip nhrp map multicast 10.10.10.3
Switch(config-if)# ip nhrp network-id 1
Switch(config-if)# ip nhrp nhs 192.168.24.4
Switch(config-if)# tunnel source vlan 1
Switch(config-if)# tunnel destination 10.10.10.3
Switch(config-if)# end
```

NHRP の設定に関する追加情報

RFC

RFC	タイトル
RFC 2332	*『NBMA Next Hop Resolution Protocol (NHRP)』*

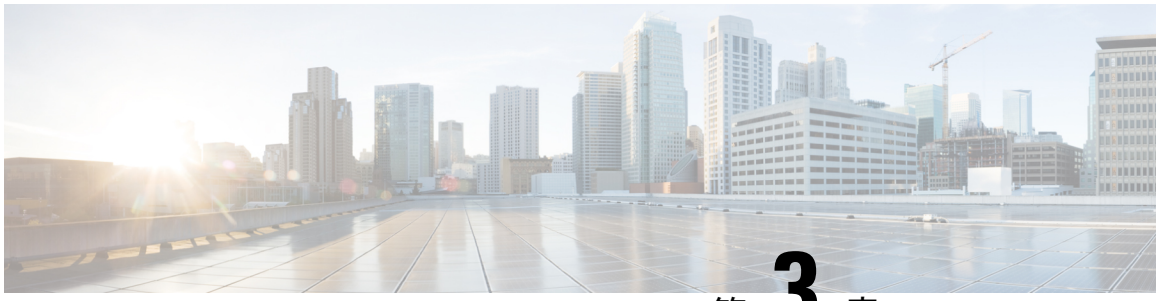
NHRP 設定の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *3 : NHRP* 設定の機能情報

機能名	リリース	機能情報
Next Hop Resolution Protocol：ネクスト ホップ リソリューション プロトコル	Cisco IOS XE Polaris 16.3.1	Next Hop Resolution Protocol（NHRP）は、すべてのトンネル エンドポイントを手動で設定するのではなく、ノンブロードキャスト マルチアクセス（NBMA）ネットワークをダイナミックにマッピングする Address Resolution Protocol（ARP）と同様のプロトコルです。NHRP を使用すると、NBMA ネットワークに接続されたシステムは、そのネットワークに参加している他のシステムの NBMA（物理）アドレスをダイナミックに学習でき、これらのシステムが直接通信できるようになります。
	Cisco IOS XE Everest 16.5.1a	この機能は、次のプラットフォームに実装されていました。 • Cisco Catalyst 3650 シリーズ スイッチ • Cisco Catalyst 3850 シリーズ スイッチ • Cisco Catalyst 9300 シリーズ スイッチ • Cisco Catalyst 9500 シリーズ スイッチ



第 3 章

VRRPv3 プロトコルのサポート

VRRPv3 プロトコルのサポート

Virtual Router Redundancy Protocol（VRRP）は、デバイスのグループを使用して単一の仮想デバイスを形成し、冗長性を実現することができます。これにより、仮想デバイス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。デバイスのグループを表す仮想デバイスは、「VRRP グループ」とも呼ばれます。VRRP バージョン 3（v3）のプロトコル サポート機能は、VRRP バージョン 2（v2）が IPv4 アドレスしかサポートしていないのに対し、IPv4 と IPv6 アドレスをサポートするための機能を提供します。このモジュールでは、VRRPv3 に関連する概念と、ネットワーク内で VRRP グループを作成してカスタマイズする方法について説明します。VRRPv3 プロトコル サポートを使用する利点は次のとおりです。

- マルチベンダー環境での相互運用性。
- VRRPv3 は、VRRPv2 が IPv4 アドレスしかサポートしていないのに対し、IPv4 と IPv6 アドレスの使用をサポートしています。
- VRRS 経路によるスケーラビリティの向上。

（注） このモジュールでは、VRRP と VRRPv3 は同じ意味で使用されています。

VRRPv3 プロトコルのサポートの制限事項

- VRRPv3 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。VRRPv3 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対応イーサネット LAN で使用するために設計されています。

- VRRPv3 は、イーサネット、ファストイーサネット、ブリッジグループ仮想インターフェイス（BVI）、およびギガビット イーサネット インターフェイス、マルチプロトコル ラベル スイッチング（MPLS）バーチャル プライベート ネットワーク（VPN）、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、VRRPv3 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より短く設定する必要があります。VRRPv3 アドバタイズタイマーの時間を BVI インターフェイスでの転送遅延時間以上の値に設定すると、最近初期化された BVI インターフェイス上にある VRRP デバイスが無条件にプライマリロールを引き継ぐことができなくなります。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。
- VRRPv3 は、ステートフル スイッチオーバー（SSO）をサポートしていません。
- VRRP が VRRS 経路の冗長インターフェイスと同じネットワーク パス上で動作する場合にのみ、完全なネットワークの冗長性を実現できます。完全な冗長性のために、次の制約事項が適用されます。
  - VRRS 経路は、親 VRRP グループと異なる物理インターフェイスを共有したり、親 VRRP グループと異なる物理インターフェイスを持つサブインターフェイス上で設定することはできません。
  - VRRS 経路は、関連付けられた VLAN が親 VRRP グループが設定された VLAN と同じトランクを共有していない限り、スイッチ仮想インターフェイス（SVI）に設定することはできません。

VRRPv3 プロトコル サポートについて

VRRPv3 の利点

IPv4 と IPv6 のサポート

VRRPv3 は、VRRPv2 が IPv4 アドレスしかサポートしていないのに対し、IPv4 と IPv6 アドレス ファミリをサポートしています。

（注） VRRPv3 が使用中の場合、VRRPv2 は使用できません。VRRPv3 を設定可能にするには、**fhrp version vrrp v3** コマンドをグローバル コンフィギュレーション モードで使用する必要があります。

冗長性

VRRP により、複数のデバイスをデフォルト ゲートウェイ デバイス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 クライアントとのトラフィックを複数のデバイスで共有するように VRRP を設定できるため、利用可能なデバイス間でより公平にトラフィックの負荷を共有できます。

複数の仮想デバイス

VRRP はデバイスの物理インターフェイス上で（拡張の制限に従って）最大 255 の仮想デバイス（VRRP グループ）をサポートします。複数の仮想デバイス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。拡張環境では、VRRS 経路は VRRP 制御グループと組み合わせて使用する必要があります。

複数の IP アドレス

仮想デバイスは、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。

（注） VRRP グループでセカンダリ IP アドレスを使用するには、プライマリ アドレスを同じグループで設定する必要があります。

プリエンプション

VRRP の冗長性スキームにより、仮想デバイスバックアップのプリエンプションが可能になり、より高い優先順位が設定された仮想デバイスバックアップが、機能を停止した仮想プライマリデバイスを引き継ぐことができます。

（注） 優先順位の低いプライマリデバイスのプリエンプションは、オプションの遅延時間を指定して有効にします。

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 アドレスを使用します。IPv4 では、マルチキャスト アドレスは 224.0.0.18 です。IPv6 では、マルチキャスト アドレスは FF02:0:0:0:0:0:0:12 です。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デバイス数が最小限になり、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 デバイス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 デバイス プライオリティがあります。優先順位により、各 VRRP デバイスが実行する役割と、仮想プライマリデバイス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。

特定の VRRP デバイスが仮想デバイスの 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、このデバイスが仮想プライマリデバイスとして機能します。

特定の VRRP デバイスが仮想デバイスのバックアップとして機能するかどうか、および仮想プライマリデバイスが機能を停止した場合に仮想プライマリデバイスを引き継ぐ順序も、優先順位によって決定されます。各仮想バックアップデバイスの優先順位は、**priority** コマンドを使用して 1 ～ 254 の値に設定できます（**vrrp address-family** コマンドを使用して VRRP 設定モードに入り、**priority** オプションにアクセスします）。

たとえば、LAN トポロジの仮想プライマリデバイスであるデバイス A が機能を停止した場合、選択プロセスが実行され、仮想デバイスバックアップ B または C が引き継ぐかどうかが決定されます。デバイス B とデバイス C がそれぞれ優先順位 101 と 100 に設定されている場合、優先順位の高いデバイス B が仮想プライマリデバイスになります。デバイス B とデバイス C が両方とも優先順位 100 に設定されている場合、IP アドレスが大きい方の仮想デバイスバックアップが選択されて仮想プライマリデバイスになります。

デフォルトでは、プリエンプティブスキームが有効になっています。この場合、プライマリ仮想デバイスになるように選択されている仮想バックアップデバイスの中で、より高い優先順位が設定されている仮想バックアップデバイスが仮想プライマリデバイスになります。このプリエンプティブスキームは、**no preempt** コマンドを使用して無効にできます（**vrrp address-family** コマンドを使用して VRRP 設定モードに入り、**no preempt** コマンドを入力します）。プリエンプションが無効になっている場合は、元の仮想プライマリデバイスが回復して再びプライマリになるまで、仮想プライマリデバイスになるように選択されている仮想デバイスバックアップがプライマリの役割を果たします。

（注） 優先順位の低いプライマリデバイスのプリエンプションは、オプションの遅延時間を指定して有効にします。

VRRP のアドバタイズメント

仮想プライマリデバイスは、同じグループ内の他の VRRP デバイスに 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、仮想プライマリデバイスの優先順位と状態が伝達されます。VRRP アドバタイズメントは、（VRRP グループ設定に基づいて）IPv4 または IPv6 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適切なマルチキャストアドレスに送信されます。IPv4 では、マルチキャスト アドレスは 224.0.0.18 です。IPv6 では、マルチキャスト アドレスは FF02:0:0:0:0:0:0:12 です。アドバタイズメントは、デフォルトでは 1 秒に 1 回送信されますが、この間隔は設定可能です。

シスコデバイスでは、VRRPv2 からの変更点であるミリ秒タイマーを設定できます。ミリ秒タイマー値は、プライマリ デバイスとバックアップ デバイスの両方に手動で設定する必要があります。バックアップデバイス上の **show vrrp** コマンド出力に表示されるプライマリ 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デバイス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。ミリ秒の値は望ましい状況でのみ動作します。ミリ秒のタイマー値の使

用は、VRRPv3 も含めてサポートしている限り、サードパーティ ベンダーと互換性があります。タイマー値は 100 ～ 40000 ミリ秒の範囲で指定できます。

VRRPv3 プロトコル サポートの設定方法

VRRP グループの作成とカスタマイズ

VRRP グループを作成するには、次の手順を実行します。ステップ 6 ～ 14 はそのグループのカスタマイズ オプションで、これらは省略可能です。

手順の概要

1. **enable**
2. **configure terminal**
3. **fhrp version vrrp v3**
4. **interface** *type number*
5. **vrrp** *group-id* **address-family** {**ipv4** | **ipv6**}
6. **address** *ip-address* [**primary** | **secondary**]
7. **description** *group-description*
8. **match-address**
9. **preempt delay minimum** *seconds*
10. **priority** *priority-level*
11. **timers advertise** 間隔
12. **vrrpv2**
13. **vrrs leader** *vrrs-leader-name*
14. **shutdown**
15. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> 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： `Device# 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	**fhrp version vrrp v3** 例：	VRRPv3 および VRRS を設定する機能をイネーブルにします。

	コマンドまたはアクション	目的
	`Device(config)# fhrp version vrrp v3`	（注） VRRPv3 が使用中の場合、VRRPv2 は使用できません。 **fhrp version vrrp v2** コマンドは設定可能ですが、サポートされていません。
ステップ 4	**interface** *type number* 例： `Device(config)# interface GigabitEthernet 0/0/0`	インターフェイス コンフィギュレーション モードを開始します。
ステップ 5	**vrrp** *group-id* **address-family** {**ipv4** | **ipv6**} 例： `Device(config-if)# vrrp 3 address-family ipv4`	VRRP グループを作成し、VRRP 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	**address** *ip-address* [**primary** | **secondary**] 例： `Device(config-if-vrrp)# address 100.0.1.10 primary`	VRRP グループのプライマリ アドレスまたはセカンダリ アドレスを指定します。 （注） IPv6 の VRRPv3 では、グループを動作可能にするため、プライマリ仮想リンクローカル IPv6 アドレスが設定されている必要があります。プライマリ リンク ローカル IPv6 アドレスがグループに確立されると、セカンダリ グローバル アドレスを追加できます。
ステップ 7	**description** *group-description* 例： `Device(config-if-vrrp)# description group 3`	（任意）VRRP グループの説明を指定します。
ステップ 8	**match-address** 例： `Device(config-if-vrrp)# match-address`	（任意）アドバタイズメント パケットのセカンダリ アドレスを設定したアドレスと照合します。 • セカンダリ アドレスの照合は、デフォルトで有効になっています。
ステップ 9	**preempt delay minimum** *seconds* 例： `Device(config-if-vrrp)# preempt delay minimum 30`	（任意）優先順位の低いプライマリデバイスのプリエンプションは、オプションの遅延時間を指定して有効にします。 • プリエンプションはデフォルトでイネーブルです。

	コマンドまたはアクション	目的
ステップ 10	**priority** *priority-level* 例： `Device(config-if-vrrp)# priority 3`	（任意）VRRP グループのプライオリティを指定します。 • VRRP グループの優先度はデフォルトで 100 です。
ステップ 11	**timers advertise** 間隔 例： `Device(config-if-vrrp)# timers advertise 1000`	（任意）アドバタイズメント タイマーをミリ秒で設定します。 • アドバタイズメント タイマーはデフォルトで 1000 ミリ秒に設定されています。
ステップ 12	**vrrpv2** 例： `Device(config-if-vrrp)# vrrpv2`	（任意）互換モードで VRRPv2 設定デバイスのサポートを有効にします。 • VRRPv2 はサポートされていません。
ステップ 13	**vrrs leader** *vrrs-leader-name* 例： `Device(config-if-vrrp)# vrrs leader leader-1`	（任意）VRRS に登録され、フォロワーに使用されるリーダーの名前を指定します。 • 登録済みの VRRS 名はデフォルトで使用不可になっています。
ステップ 14	**shutdown** 例： `Device(config-if-vrrp)# shutdown`	（任意）VRRP グループの VRRP 設定をディセーブルにします。 • VRRP の設定は、VRRP グループに対してはデフォルトでイネーブルになっています。
ステップ 15	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

FHRP クライアントの初期化前の遅延時間の設定

インターフェイス上のすべての FHRP クライアントの初期化の前に遅延期間を設定するには、次のタスクを実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **fhrp version vrrp v3**
4. **interface** *type number*
5. **fhrp delay** {[**minimum**] [**reload**] *seconds*}

6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> 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： `Device# 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	**fhrp version vrrp v3** 例： `Device(config)# fhrp version vrrp v3`	VRRPv3 および VRRS を設定する機能をイネーブルにします。 （注） VRRPv3 が使用中の場合、VRRPv2 は使用できません。
ステップ 4	**interface** *type number* 例： `Device(config)# interface GigabitEthernet 0/0/0`	インターフェイス コンフィギュレーション モードを開始します。
ステップ 5	**fhrp delay** {[**minimum**] [**reload**] *seconds*} 例： `Device(config-if)# fhrp delay minimum 5`	インターフェイスの起動後に、FHRP クライアントの初期化の遅延期間を指定します。 • 範囲は 0 ～ 3600 秒です。
ステップ 6	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

VRRPv3 プロトコル サポートの設定例

例：デバイス上の VRRPv3 のイネーブル化

次の例は、デバイスで VRRPv3 をイネーブルにする方法を示しています。

```
Device> enable
Device# configure terminal
Device(config)# fhrp version vrrp v3
Device(config-if-vrrp)# end
```

例：VRRP グループの作成とカスタマイズ

次に、VRRP グループを作成およびカスタマイズする例を示します。

```
Device> enable
Device# configure terminal
Device(config)# fhrp version vrrp v3
Device(config)# interface GigabitEthernet 1/0/1
Device(config-if)# vrrp 3 address-family ipv4
Device(config-if-vrrp)# address 100.0.1.10 primary
Device(config-if-vrrp)# description group 3
Device(config-if-vrrp)# match-address
Device(config-if-vrrp)# preempt delay minimum 30
Device(config-if-vrrp)# end
```

（注） 上の例では、グローバル コンフィギュレーション モードで **fhrp version vrrp v3** コマンドが使用されています。

例：FHRP クライアントの初期化前の遅延時間の設定

次の例は、FHRP クライアントの初期化前の遅延時間の設定方法を示しています。

```
Device> enable
Device# configure terminal
Device(config)# fhrp version vrrp v3
Device(config)# interface GigabitEthernet 1/0/1
Device(config-if)# fhrp delay minimum 5
Device(config-if-vrrp)# end
```

（注） 上記の例では、インターフェイスが表示されてから FHRP クライアントの初期化に 5 秒間の遅延時間が指定されています。遅延時間は 0 ～ 3600 秒の範囲で指定できます。

例：VRRP ステータス、設定、および統計情報の詳細

以下は、VRRP グループのステータス、設定、および統計情報の詳細の出力例です。

```
Device> enable
Device# show vrrp detail

 GigabitEthernet1/0/1 - Group 3 - Address-Family IPv4
  Description is "group 3"
  State is MASTER
  State duration 53.901 secs
  Virtual IP address is 100.0.1.10
  Virtual MAC address is 0000.5E00.0103
  Advertisement interval is 1000 msec
  Preemption enabled, delay min 30 secs (0 msec remaining)
  Priority is 100
```

```
  Master Router is 10.21.0.1 (local), priority is 100
  Master Advertisement interval is 1000 msec (expires in 832 msec)
  Master Down interval is unknown
  VRRPv3 Advertisements: sent 61 (errors 0) - rcvd 0
  VRRPv2 Advertisements: sent 0 (errors 0) - rcvd 0
  Group Discarded Packets: 0
    VRRPv2 incompatibility: 0
    IP Address Owner conflicts: 0
    Invalid address count: 0
    IP address configuration mismatch : 0
    Invalid Advert Interval: 0
    Adverts received in Init state: 0
    Invalid group other reason: 0
  Group State transition:
    Init to master: 0
    Init to backup: 1 (Last change Sun Mar 13 19:52:56.874)
    Backup to master: 1 (Last change Sun Mar 13 19:53:00.484)
    Master to backup: 0
    Master to init: 0
    Backup to init: 0

Device# exit
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
FHRP コマンド	『First Hop Redundancy Protocols Command Reference』
VRRPv2 の設定	『*Configuring VRRP*』
VRRPv3 コマンド	この章で使用するコマンドの完全な構文および使用方法の詳細。 *Command Reference (Catalyst 9300 Series Switches)*

標準および RFC

標準/RFC	タイトル
RFC5798	『*Virtual Router Redundancy Protocol*』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

VRRPv3 プロトコルのサポートの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *4 : VRRPv3* プロトコルのサポートの機能情報

機能名	リリース	機能情報
VRRPv3 プロトコルのサポート	Cisco IOS XE Everest 16.6.1	VRRP は、デバイスのグループを使用して単一の仮想デバイスを形成し、冗長性を実現します。これにより、仮想デバイスをデフォルト 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。デバイスのグループを表す仮想デバイスは、「VRRP グループ」とも呼ばれます。VRRPv3 プロトコルのサポート機能は、IPv4 と IPv6 アドレスをサポートするための機能を提供します。 この機能が導入されました。

用語集

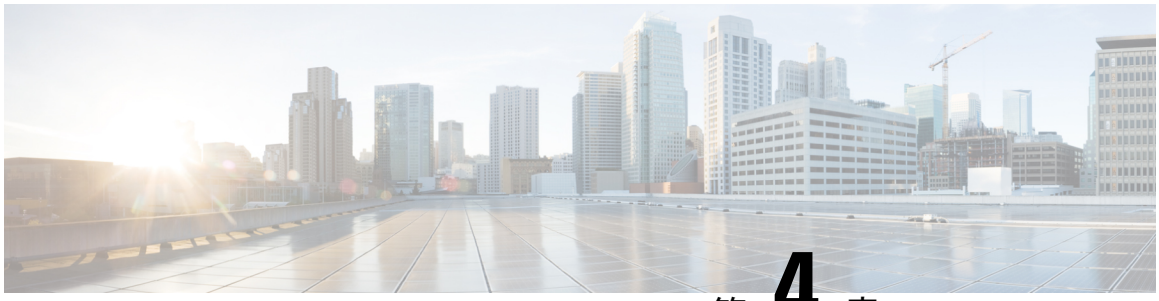
Virtual IP address owner：仮想デバイスの IP アドレスを所有する VRRP デバイス。仮想デバイス アドレスを物理インターフェイス アドレスとして持っているデバイスが所有者になります。

Virtual device：1 つのグループを形成する 1 台または複数台の VRRP デバイス。仮想デバイスは、LAN クライアントのデフォルト ゲートウェイ デバイスとして動作します。仮想デバイスは、VRRP グループとも呼ばれます。

Virtual device backup：仮想プライマリデバイス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られる 1 台以上の VRRP デバイス。

Virtual primary device：仮想デバイスの 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 デバイス。通常、仮想プライマリデバイスは IP アドレス所有者としても機能します。

VRRP device：VRRP を実行しているデバイス。



第 4 章

WCCP の設定

このセクションでは、WCCP の設定について説明します。

はじめに

Web Cache Communication Protocol（WCCP）はシスコが開発したコンテンツルーティング テクノロジーです。IP パケットを代行受信し、IP パケットに指定されている宛先とは別の宛先にそのパケットをリダイレクトします。パケットは、インターネット上にある宛先の Web サーバーから、クライアントのローカルのコンテンツエンジンにリダイレクトされるのが一般的です。WCCP の展開シナリオによっては、Web サーバーからクライアント方向でもトラフィックをリダイレクトする必要があります。WCCP を使用すると、コンテンツエンジンをネットワーク インフラストラクチャに統合できます。

このマニュアルの作業では、ネットワークにコンテンツエンジンが設定済みであることを前提にしています。

WCCP の前提条件

- WCCP を使用するには、インターネットに接続されたインターフェイス上で IP を設定する必要があります。また、別のインターフェイスをコンテンツエンジンに接続する必要があります。
- コンテンツエンジンに接続するインターフェイスは、ファストイーサネットインターフェイスまたはギガビット イーサネット インターフェイスにする必要があります。

WCCP に関する制約事項

General

Web キャッシュ通信プロトコルバージョン 2（WCCPv2）には、次の制限が適用されます。

- WCCP は、IPv4 ネットワークだけで動作します。
- シスコエクスプレス フォワーディングをイネーブルにすると、WCCPによってネットワーク アドレス変換（NAT）がバイパスされます。
- WCCP には、ネットワークで同時に設定された NAT およびゾーンベース ファイアウォールとの相互運用性がありません。
- サービスグループは、最大 32 のコンテンツエンジンおよび 32 のスイッチで構成できます。
- マルチキャストクラスタにサービスを提供するスイッチの場合、存続可能時間（TTL）の値を 15 以下に設定する必要があります。
- クラスタのすべてのコンテンツエンジンは、クラスタにサービスを提供するすべてのデバイスと通信できるように設定する必要があります。
- マルチキャスト アドレスは、224.0.0.0 ～ 239.255.255.255 の範囲にする必要があります。
- 同じクライアント インターフェイスで同時に最大 8 個のサービス グループがサポートされます。
- レイヤ2のリライト転送メソッド方式はサポートされますが、Generic Routing Encapsulation（GRE）はサポートされません。
- コンテンツエンジンにレイヤ 2 を直接接続する必要があります。1 ホップまたは複数ホップ離れたレイヤ 3 接続はサポートされません。
- Ternary CAM（TCAM）フレンドリ マスクベースの割り当てはサポートされますが、ハッシュ バケットベースの方式はサポートされません。
- TCAMの空きがなくなると、トラフィックはリダイレクトされず、通常どおりに転送されます。
- WCCP バージョン 2 規格では、最大 256 個のマスクをサポートします。ただし、Cisco Catalyst 9000 シリーズ スイッチは、単一のマスクへのマスク割り当てテーブルのみをサポートします。
- マスク割り当てに設定されているコンテンツエンジンが、割り当て方式としてハッシュが選択されているファームに参加しようとする場合、キャッシュ エンジンの割り当て方式が既存のファームの方式と一致しない限り、ファームに参加できません。

Catalyst 9000 シリーズ スイッチのアクセス制御リスト

WCCPがマスク割り当てを使用している場合、リダイレクトリストはアプライアンスのマスク情報にマージされ、その結果としてマージされた ACL は Catalyst 9000 シリーズ スイッチ ハードウェアに渡されます。リダイレクト リストのプロトコルが IP であるか、サービス グループ プロトコルと完全に一致する場合、その許可 ACL または拒否 ACL のエントリだけが、アプライアンスのマスク情報にマージされます。

次の制約事項がリダイレクト リスト ACL に適用されます。

- ACL は、IPv4 拡張 ACL にする必要があります。
- 個々の発信元または宛先のポート番号だけを指定できます。ポート範囲は指定できません。
- 個々の発信元または宛先のポート番号以外の有効な一致基準は **dscp** と **tos** のみです。
- **fragments**、**time-range**、**options** キーワードや、TCP フラグは使用できません。
- リダイレクト ACL がこれらの制約事項を満たさない場合、次のエラー メッセージがログに記録されます。

```
WCCP-3-BADACE: Service <service group>, invalid access-list entry (seq:<sequence>,
reason:<reason>)
```

WCCP に関する情報

WCCP の概要

WCCP は、Cisco Content Engine（または WCCP を実行する他のコンテンツエンジン）を使用して、ネットワークのトラフィックパターンをローカライズし、ローカルでコンテンツ要求を実行できるようにします。トラフィックのローカライズによって伝送コストを引き下げ、ダウンロード時間を短縮できます。

WCCP によって、Cisco IOS XE プラットフォームはコンテンツ要求を透過的にリダイレクトできます。透過的リダイレクションを使用すると、ユーザーは、Web プロキシを使用するようにブラウザを設定せずに、コンテンツ要求をローカルで実行できます。ユーザーはターゲット URL を使用してコンテンツを要求できます。また、ユーザーの要求はコンテンツ エンジンに自動的にリダイレクトされます。この場合の「透過的」とは、エンドユーザーが要求したファイル（Web ページなど）が、元々指定していたサーバーからではなく、コンテンツエンジンから送信されることをそのユーザーが意識しないという意味です。

要求を受信したコンテンツエンジンは、独自のローカルキャッシュからサービスを提供しようとします。要求した情報が存在しない場合、コンテンツ エンジンから独自の要求が元のターゲット サーバーに発行され、必要な情報が取得されます。コンテンツエンジンは、要求された情報を取得すると、要求元のクライアントに転送し、以降の要求に対応するためにキャッシュします。その結果、ダウンロードのパフォーマンスが最大になり、送信コストが大幅に削減されます。

WCCPにより、一連のコンテンツエンジン（コンテンツエンジンクラスタと呼ばれる）が1つまたは複数のデバイスにコンテンツを提供できるようになります。ネットワーク管理者は、このようなクラスタ処理機能によって容易にコンテンツエンジンを拡張し、高いトラフィック負荷を管理できます。シスコ クラスタ処理テクノロジーを使用すると、各クラスタ メンバを同時に実行できるため、リニア スケーラビリティが実現します。クラスタ処理コンテンツ エンジンによって、キャッシュ ソリューションのスケーラビリティ、冗長性、および可用性が大幅に改善されます。最大 32 個のコンテンツ エンジンをクラスタ処理し、目的の容量まで拡張できます。

WCCP マスク割り当て

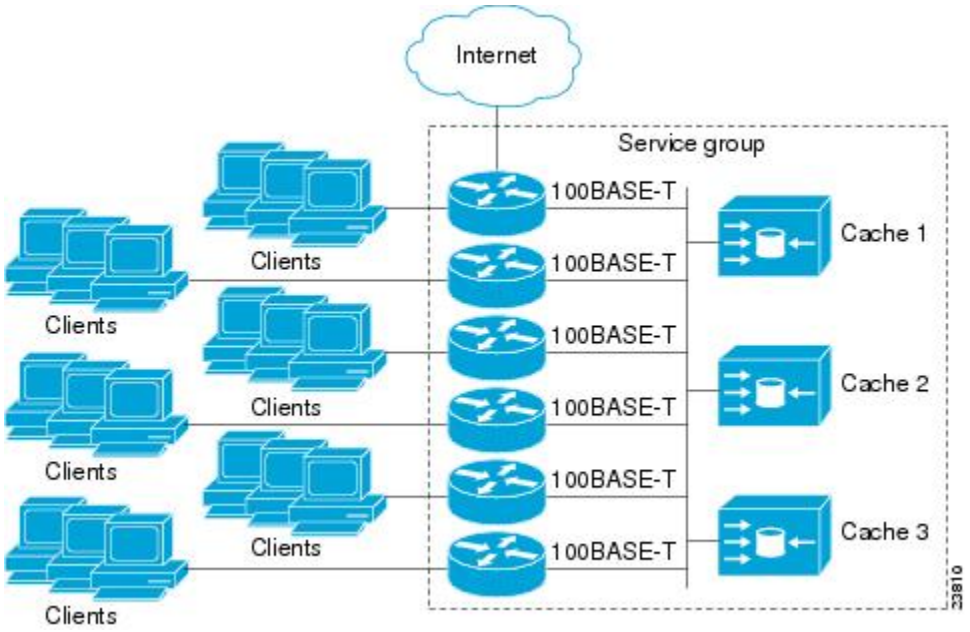
WCCPマスク割り当て機能によって、（デフォルトのハッシュ割り当て方式ではなく）WCCPサービスのロード バランシング方式としてマスク割り当てを使用できます。

Application and Content Networking System（ACNS）ソフトウェアを実行するコンテンツエンジンの場合、**mask-assign** キーワードを指定した **wccp custom-web-cache** コマンドを使用して、マスク割り当てを設定します。Cisco Wide Area Application Services（WAAS）ソフトウェアを実行するコンテンツエンジンの場合、**mask-assign** キーワードを指定した **wccp tcp-promiscuous** コマンドを使用して、マスク割り当てを設定します。

WCCPv2 の設定

複数のデバイスが WCCPv2 を使用して 1 つのコンテンツエンジンクラスタにサービスを提供できます。次の図に、複数のデバイスを使用した設定例を示します。

図 *5 : WCCPv2* を使用した *Cisco* コンテンツ エンジン ネットワーク構成



クラスタ、および同じサービスを実行しているクラスタに接続するデバイス内のコンテンツエンジンのサブセットは、サービスグループと呼ばれます。利用可能なサービスには、TCP および UDP リダイレクションが含まれます。

WCCPv2 の場合、各コンテンツエンジンがサービスグループ内のすべてのデバイスを認識している必要があります。サービスグループ内のすべてのデバイスのアドレスを指定するには、次のいずれかのメソッドを選択する必要があります。

- ユニキャスト：グループ内の各デバイスの IP アドレスリストを、各コンテンツエンジンで設定します。この場合、グループ内の各デバイスのアドレスは、設定の際、コンテンツエンジンごとに明示的に指定する必要があります。
- マルチキャスト：単一のマルチキャストアドレスを各コンテンツエンジンで設定します。マルチキャスト アドレス メソッドの場合、コンテンツエンジンは、サービスグループのすべてのスイッチに提供されるシングルアドレス通知を送信します。たとえば、コンテンツエンジンは、パケットを常にマルチキャストアドレス 224.0.0.100 に送信するように指示できます。その場合、マルチキャストパケットは、WCCP を使用してリッスンしているグループ用に設定されたサービスグループ内のすべてのデバイスに送信されます（詳細については、**ip wccp group-listen** インターフェイス コンフィギュレーション コマンドを参照してください）。

マルチキャスト オプションの場合に必要な操作は、各コンテンツ エンジンで単一のアドレスを指定することだけなので、設定が容易です。このオプションを使用して、サービス グループからルータを動的に追加および削除できます。毎回、異なるアドレス リストを使用してコンテンツ エンジンを再設定する必要はありません。

WCCPv2 での設定は次の順序で行います。

1. 各コンテンツエンジンは、ルータリストを使用して設定されます。
2. 各コンテンツエンジンは、各自の存在と、通信の確立に使用されたすべてのデバイスのリストについて通知します。ルータは、グループ内のコンテンツ エンジンのビュー（リスト）で応答します。
3. そのビューがクラスタ内のすべてのコンテンツエンジンで一貫している場合、1 つのコンテンツエンジンがリードとして指定され、デバイスがパケットのリダイレクト時に展開する必要のあるポリシーが設定されます。

HTTP 以外のサービスの WCCPv2 サポート

WCCPv2 では、さまざまな UDP および TCP トラフィックを含め、HTTP（TCP ポート 80 トラフィック）以外のトラフィックのリダイレクションが可能です。WCCPv2 では他のポート宛てのパケットをリダイレクトできます。たとえば、プロキシ Web キャッシュ処理、ファイル転送プロトコル（FTP）キャッシング、FTP プロキシの処理、80 以外のポートの Web キャッシング、Real Audio、ビデオアプリケーション、およびテレフォニー アプリケーションに使用されるポートなどです。

各種の利用可能なサービスに対応するため、WCCPv2 は複数のサービスグループという概念を導入しました。サービス情報は、ダイナミックサービス識別番号（98 など）または事前定義し

たサービスキーワード（**web-cache** など）を使用して、WCCP コンフィギュレーション コマンドで指定します。この情報は、サービス グループ メンバーが同じサービスを使用または提供していることを確認するために使用されます。

サービス グループのコンテンツ エンジンは、プロトコル（TCP または UDP）によってリダイレクトされるトラフィックと、最大 8 個の発信元ポートまたは宛先ポートを指定します。各サービス グループにはプライオリティ ステータスが割り当てられます。ダイナミック サービスのプライオリティは、コンテンツエンジンによって割り当てられます。プライオリティ値の範囲は、0 ～ 255 です（0 が最も低いプライオリティ）。事前定義した Web キャッシュ サービスには、240 のプライオリティが割り当てられています。

複数デバイスでの WCCPv2 サポート

WCCPv2 では、複数のデバイスをキャッシュエンジンのクラスタに追加できます。サービスグループで複数のデバイスを使用すると、冗長構成、インターフェイスの集約、およびリダイレクトの負荷分散が可能になります。WCCPv2 は、サービスグループごとに最大 32 のデバイスをサポートします。各サービス グループの確立および保守は独立して行われます。

WCCPv2 での MD5 セキュリティ

WCCPv2 には、パスワードとハッシュメッセージ認証コード-メッセージダイジェスト（HMAC MD5）規格を使用して、サービスグループの一部になるスイッチとコンテンツエンジンを制御できる、オプションの認証機能があります。共有秘密キー MD5 ワンタイム認証（**ip wccp password** *password* グローバル コンフィギュレーション コマンドを使用して設定）では、メッセージを代行受信、検査、およびリプレイから保護します。

WCCPv2 での Web キャッシュ パケットのリターン

エラーまたは過負荷のために、コンテンツエンジンが、キャッシュした要求オブジェクトを提供できない場合、コンテンツエンジンは、元々指定されていた宛先サーバーに転送するように、要求をデバイスに返します。WCCPv2 には、機能していないコンテンツ エンジンから返送された要求を判断できるパケットのチェック機能があります。デバイスは、この情報を使用して（要求をコンテンツエンジンクラスタに再送信しようとするのではなく）要求を元の宛先サーバーに転送できます。このプロセスのエラー処理はクライアントに意識されません。

コンテンツエンジンがパケットを拒否し、パケット返送機能を開始する場合、一般的に次のような理由があります。

- コンテンツ エンジンが過負荷になり、パケットを処理する余裕がなくなった場合
- コンテンツエンジンが、パケットのキャッシング機能が低下する特定の条件についてフィルタリングしている場合（たとえば、IP 認証が有効になった場合）

WCCPv2 での負荷分散

WCCPv2 を使用すると、個々のコンテンツエンジンに割り当てる負荷を調整して、空きリソースを効率的に使用できるようになります。さらに、クライアントに対して高い Quality Of Service（QoS）を確保できます。WCCPv2 を使用すると、指定したコンテンツ エンジンが特定のコンテンツ エンジン上の負荷を調整し、クラスタ内のコンテンツ エンジン全体で負荷を分散できます。WCCPv2 では負荷分散を実行するために、次の 3 つの方法を使用します。

- ホットスポット処理：個々のハッシュバケットをすべてのコンテンツエンジンに分散できます。WCCPv2 の登場までは、1 つのハッシュバケットの情報を転送できるのは、1 つのコンテンツエンジンに対してのみでした。
- ロードバランシング：過負荷のコンテンツエンジンから、空き容量がある他のメンバに負荷を移行するように、コンテンツエンジンに割り当てるハッシュバケットセットを調整できます。
- 負荷制限：コンテンツエンジンの容量を超えないように、スイッチが負荷を選択してリダイレクトできるようにします。

これらのハッシュ処理パラメータを使用すると、コンテンツエンジンの過負荷を防ぎ、障害が発生する可能性を軽減します。

WCCP バイパス パケット

WCCP は IP パケットを代行受信し、IP ヘッダーに指定されている宛先以外の宛先に、そのパケットをリダイレクトします。パケットは、インターネット上にある Web サーバーから、宛先のローカルの Web キャッシュにリダイレクトされるのが一般的です。

場合によっては、Web キャッシュでリダイレクトされたパケットを適切に管理できず、パケットを変更せずに元のデバイスに返送することがあります。このようなパケットはバイパスパケットと呼ばれ、カプセル化なしのレイヤ 2 転送（L2）を使用して、発信元のデバイスに返送されます。デバイスはカプセル化を解除し、通常どおりにパケットを転送します。入力インターフェイスと関連付けられている VRF（関連付けられている VRF がない場合はグローバルテーブル）は、パケットを宛先にルーティングするときに使用されます。

WCCP クローズド サービスおよびオープン サービス

パケットを代行受信し、Cisco スイッチまたはルータによって外部 WCCP クライアントデバイスにリダイレクトするアプリケーションの場合、WCCP クライアントデバイスを使用できないと、状況によってはアプリケーションのパケットをブロックする必要があります。このブロックを実行するには、WCCP クローズド サービスを設定します。WCCP サービスがクローズドに設定されている場合、サービスを提供するもののアクティブなクライアントデバイスを持たないパケットは破棄されます。

デフォルトでは、WCCP はオープン サービスとして動作します。この場合、中間デバイスがなくても、クライアントとサーバー間の通信は正常に進行します。

ip wccp service-list コマンドは、クローズドモードとオープンモード両方のサービスに使用できます。アプリケーション プロトコル タイプまたはポート番号を登録するには、**service-list** キーワードと *service-access-list* 引数を使用します。オープンサービスまたはクローズドサービスを選択するには、**mode** キーワードを使用します。

WCCP 発信 ACL チェック

入力インターフェイスで WCCP のリダイレクションが有効になっている場合、パケットは WCCP によってリダイレクトされ、代わりに IP ヘッダーで指定された宛先以外のインターフェイスで出力されます。パケットは、引き続き入力インターフェイスで設定された ACL の影響下にあります。ただし、リダイレクションによって、パケットが元の出力インターフェイスで設定された ACL をバイパスする可能性があります。元の出力インターフェイスで ACL が設定されているためにドロップされたパケットは、リダイレクト出力インターフェイスに送信される場合があります。その結果、セキュリティ上の問題が発生する可能性があります。WCCP アウトバウンド ACL チェック機能を有効にすると、リダイレクトされたパケットは、元の出力インターフェイスで設定された ACL 条件の対象になります。

WCCP サービス グループ

WCCP は、Cisco IOS XE ソフトウェアのコンポーネントで、定義済みの特性を持つトラフィックを元の宛先から代替の宛先へとリダイレクトします。一般的な WCCP アプリケーションには、リモート Web サーバー宛ての発信トラフィックをローカル Web キャッシュにリダイレクトして、応答時間を改善し、ネットワーク リソースの使用状況を最適化する機能があります。

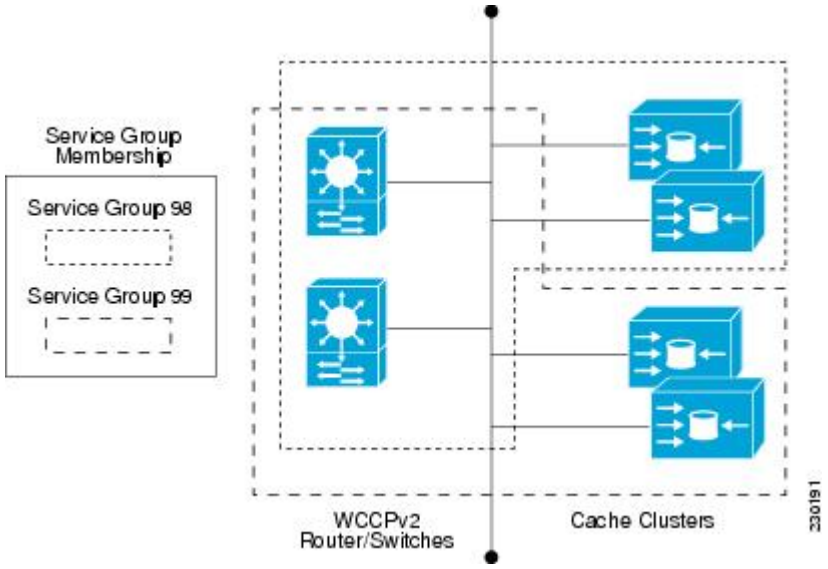
リダイレクトに選択されるトラフィックの性質は、コンテンツエンジンで指定されるサービス グループ（下の図を参照）によって定義され、WCCP を使用してスイッチやルータに伝達されます。

WCCPv2 は、サービスグループごとに最大 32 のスイッチをサポートします。各サービス グループの確立および保守は独立して行われます。

WCCPv2 では、トラフィックの代行受信およびリダイレクションを行うために使用されている論理リダイレクション サービスを基にサービス グループを使用します。標準のサービスは Web キャッシュです。Web キャッシュは TCP ポート 80（HTTP）トラフィックを代行受信し、そのトラフィックをコンテンツ エンジンにリダイレクトします。Web キャッシュ サービスの特徴はスイッチとコンテンツエンジンの両方から認識されているため、このサービスは既知のサービスと呼ばれます。サービスの識別よりも詳細な既知のサービスの説明は必要ありません。標準の Web キャッシュ サービスを指定するには、**ip wccp** コマンドと **web-cache** キーワードを使用します。

（注） スイッチでは同時に複数のサービスが実行できます。また、スイッチとコンテンツエンジンは、同時に複数のサービスグループの一部になることができます。

図 *6 : WCCP* サービス グループ



ダイナミックサービスは、コンテンツエンジンによって定義されます。コンテンツエンジンは、代行受信するプロトコルまたはポート、およびトラフィックの配信方法をスイッチに指示します。ダイナミック サービス グループのトラフィックの特性に関する情報は、スイッチ自体にはありません。この情報は、グループに参加する最初のコンテンツエンジンから提供されるためです。ダイナミック サービスでは、1 つのプロトコルに最大 8 ポートを指定できます。

たとえば、Cisco Content Engine ではダイナミック サービス 99 を使用して、リバース プロキシ サービスを指定します。ただし、他のコンテンツ エンジン デバイスでは、その他のサービスにこのサービス番号を使用する可能性があります。

WCCP：すべてのサービスを確認

インターフェイスは、WCCP サービスを複数使用して設定できます。1 つのインターフェイスに複数の WCCP サービスを設定する場合、サービスの優先順位は、他の設定済みサービスのプライオリティと比較した、そのサービスの相対的なプライオリティによって変わります。各 WCCP サービスには、定義の一部にプライオリティ値があります。複数の WCCP サービスを使用してインターフェイスを設定する場合、パケットの優先順位は、プライオリティ順でサービス グループに対して対応付けられます。

（注） WCCP サービスグループの優先順位は、Cisco IOS XE ソフトウェアで設定できません。

ip wccp check services all コマンドを使用すると、すべての設定済みサービスを一致についてチェックし、必要に応じてそのサービスに関するリダイレクションを実行するように WCCP を設定できます。パケットのリダイレクト先キャッシュは、リダイレクト ACL およびサービスの優先順位で制御できます。複数の WCCP サービスをサポートするには、**ip wccp check services all** コマンドをグローバルレベルで設定する必要があります。

WCCP サービスをリダイレクト ACL を使用して設定する場合、IP パケットに一致するサービスが見つかるまで、プライオリティ順にサービスがチェックされます。パケットに一致するサービスがない場合、パケットはリダイレクトされません。サービスがパケットに一致し、サービスにリダイレクト ACL が設定されている場合、IP パケットは ACL に対してチェックされます。ACL によってパケットが拒否される場合、**ip wccp check services all** コマンドを設定しない限り、低い優先順位のサービスにパケットは渡されません。**ip wccp check services all** コマンドを設定すると、インターフェイスで設定されている残りの低い優先順位のサービスに対して、引き続きパケットのマッチングが試行されます。

WCCP のトラブルシューティングのヒント

WCCP をイネーブルにすると、CPU の使用率が非常に高くなる場合があります。WCCP カウンタを使用すると、直接スイッチでバイパストラフィックを確認できます。また、その原因が WCCP の有効化による CPU の使用率の高さにあるかどうかを示すことができます。場合によっては 10 % のバイパス トラフィックが標準で、他の状況では 10 % が高いこともあります。ただし、25% を超える数値の場合、Web キャッシュの状況をより詳しく調査する必要があります。

バイパス トラフィックのレベルが高いことをカウンタが示している場合、次の手順は、コンテンツ エンジンのバイパス カウンタを確認し、コンテンツ エンジンがトラフィックのバイパスを選択した理由を判定します。さらに詳細に調査するには、コンテンツ エンジン コンソールにログインし、CLI を使用します。カウンタを使用すると、バイパスするトラフィックの割合を決定できます。

特定のサービスに関してデバイスで保持している WCCP 統計情報（カウント）を削除するには、**clear wccp** コマンドを使用します。

すべての WCCP グローバル統計情報（カウント）を表示するには、**show wccp** コマンドを使用します。

WCCP の設定方法

次の設定作業では、ネットワークで使用するコンテンツエンジンのインストールと設定が完了していることを前提としています。クラスタでコンテンツエンジンを設定してから、ルータまたはスイッチの WCCP 機能を設定する必要があります。コンテンツエンジンの設定とセットアップ作業については、『Cisco Cache Engine User Guide』を参照してください。

WCCP の設定

WCCP を設定するには、次の作業を実行します。

ip wccp {**web-cache** | *service-number*} グローバル コンフィギュレーション コマンドを使用して WCCP サービスを設定しない限り、WCCP はデバイスに対して無効です。特定の形式の **ip wccp** コマンドを最初に使用したときに、WCCP が有効になります。

サービスグループのデバイスとコンテンツエンジンのパスワードを設定するには、**ip wccp web-cache password** コマンドを使用します。MD5 パスワードセキュリティの場合、サービスグループのパスワードを使用して、サービスグループに参加させる各デバイスおよびコンテンツエンジンを設定する必要があります。パスワードの長さは、8 文字以下である必要があります。サービスグループの各コンテンツエンジンまたはデバイスは、WCCP メッセージヘッダーの検証後すぐに、受信した WCCP パケットのセキュリティコンポーネントを認証します。認証に失敗したパケットは廃棄されます。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip wccp** {**web-cache** | *service-number*} [**group-address** *multicast-address*] [**redirect-list** *access-list*] [**group-list** *access-list*] [**password** *password* [**0** | **7**]]
4. **interface** *type number*
5. **ip wccp** {**web-cache** | *service-number*} **redirect** {**in** | **out**}
6. **exit**
7. **interface** *type number*
8. **ip wccp redirect exclude in**

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： `Device> 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： `Device# 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	**ip wccp** {**web-cache**	*service-number*} [**group-address** *multicast-address*] [**redirect-list** *access-list*] [**group-list** *access-list*] [**password** *password* [**0**	**7**]] 例： `Device(config)# ip wccp web-cache password pwd`	デバイスで有効にする Web キャッシュまたはダイナミックサービスを指定します。サービスグループで使用する IP マルチキャストアドレスを指定します。使用するアクセスリストを指定します。MD5 認証を使用するかどうかを指定します。WCCP サービスを有効にします。 • （注） パスワードの長さは、8 文字以内にする必要があります。

	コマンドまたはアクション	目的
ステップ 4	**interface** *type number* 例： `Device(config)# interface Gigabitethernet 0/0`	Web キャッシュ サービスを実行するインターフェイス番号を指定し、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 5	**ip wccp** {**web-cache** | *service-number*} **redirect** {**in** | **out**} 例： `Device(config-if)# ip wccp web-cache redirect in`	WCCP を使用して、発信インターフェイスまたは受信インターフェイスでパケットのリダイレクションをイネーブルにします。 • **out** および **in** キーワードオプションに示されているとおり、発信インターフェイスまたは受信インターフェイスのリダイレクションを指定できます。
ステップ 6	**exit** 例： `Device(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 7	**interface** *type number* 例： `Device(config)# interface GigabitEthernet 0/2/0`	リダイレクトからトラフィックを除外するインターフェイス番号を対象として、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 wccp redirect exclude in** 例： `Device(config-if)# ip wccp redirect exclude in`	（任意）指定したインターフェイスのトラフィックをリダイレクションから除外します。

クローズド サービスの設定

WCCP 用のサービス グループの数を指定し、クローズド サービスまたはオープン サービスとしてサービス グループを設定し、オプションで全サーバーのチェックを指定するには、この作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. 次のいずれかのコマンドを入力します。
   - **ip wccp** *service-number* [**service-list** *service-access-list* **mode** {**open** | **closed**}]
   - または
   - **ip wccp web-cache mode** {**open** | **closed**}

4. **ip wccp check services all**
5. **ip wccp** {**web-cache** | *service-number*}
6. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> 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： `Device# 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	次のいずれかのコマンドを入力します。
	• **ip wccp** *service-number* [**service-list** *service-access-list* **mode** {**open** | **closed**}]
	• または
	• **ip wccp web-cache mode** {**open** | **closed**}
	例：
	`Device(config)# ip wccp 90 service-list 120 mode closed`
	または
	`Device(config)# ip wccp web-cache mode closed`
		ダイナミック WCCP サービスをクローズドまたはオープンとして設定します。
		または
		Web キャッシュ サービスをクローズドまたはオープンとして設定します。
		（注） Web キャッシュ サービスをクローズド サービスとして設定する場合、サービス アクセス リストを指定できません。
		（注） ダイナミック WCCP サービスをクローズドサービスとして設定する場合、サービス アクセス リストを指定する必要があります。

ステップ 4	**ip wccp check services all** 例： `Device(config)# ip wccp check services all`	（任意）WCCP サービスのチェックをイネーブルにします。 • このコマンドを使用すると、一致について他の設定済みサービスをチェックし、必要に応じてそのサービスについてリダイレクションを実行するように WCCP を設定できます。パケットのリダイレクト先キャッシュは、サービス記述だけでなく、リダイレクト ACL によって制御できます。

	コマンドまたはアクション	目的
		（注） **ip wccp check services all** コマンドは、すべてのサービスに適用され、単一のサービスには関連付けられないグローバル WCCP コマンドです。
ステップ 5	**ip wccp** {**web-cache** | *service-number*} 例： `Device(config)# ip wccp 201`	WCCP サービス ID を指定します。 • 標準の Web キャッシュ サービスまたはダイナミック サービス番号（0 ～ 255）を指定できます。 • 指定できるサービスの最大数は 256 です。
ステップ 6	**exit** 例： `Device(config)# exit`	特権 EXEC モードに戻ります。

マルチキャストアドレスへのデバイスの登録

サービスグループにマルチキャストアドレスオプションを使用する場合、デバイスがインターフェイスでマルチキャスト ブロードキャストを待ち受けるように設定する必要があります。

リダイレクトされたトラフィックが仲介デバイスを経由する必要のあるネットワーク設定の場合、経由対象のデバイスは、IPマルチキャストルーティングを実行するように設定する必要があります。仲介デバイスの経由を有効にするには、次の2つのコンポーネントを設定してください。

- **ip multicast-routing** グローバル コンフィギュレーション コマンドを使用して、IP マルチキャストルーティングを有効にします。
- **ip wccp group-listen** インターフェイス コンフィギュレーション コマンドを使用して、キャッシュエンジンの接続先のインターフェイスが、マルチキャストの送信を受信できるようにします。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip multicast-routing** [**vrf** *vrf-name*] [**distributed**]
4. **ip wccp** {**web-cache** | *service-number*} **group-address** *multicast-address*
5. **interface** *type number*
6. **ip pim** {**sparse-mode** | **sparse-dense-mode** | **dense-mode** [**proxy-register** { **list** *access-list* | **route-map** *map-name*}]}
7. **ip wccp** {**web-cache** | *service-number*} **group-listen**

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： `Device> 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： `Device# 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	**ip multicast-routing** [**vrf** *vrf-name*] [**distributed**] 例： `Device(config)# ip multicast-routing`	IP マルチキャスト ルーティングを有効にします。
ステップ 4	**ip wccp** {**web-cache** | *service-number*} **group-address** *multicast-address* 例： `Device(config)# ip wccp 99 group-address 239.1.1.1`	サービス グループのマルチキャスト アドレスを指定します。
ステップ 5	**interface** *type number* 例： `Device(config)# interface ethernet 0/0`	コンテンツ エンジンの接続先インターフェイスが、Web キャッシュ サービスが実行するマルチキャスト送信を受信できるようにし、インターフェイス コンフィギュレーション モードを開始します。
ステップ 6	**ip pim** {**sparse-mode** | **sparse-dense-mode** | **dense-mode** [**proxy-register** { **list** *access-list* | **route-map** *map-name*}]} 例： `Device(config-if)# ip pim dense-mode`	（任意）インターフェイスで Protocol Independent Multicast（PIM）をイネーブルにします。 （注） Catalyst 9000 シリーズ スイッチで **ip wccp group-listen** コマンドを適切に動作させるには、**ip wccp group-listen** コマンドに加えて、**ip pim** コマンドを入力する必要があります。
ステップ 7	**ip wccp** {**web-cache** | *service-number*} **group-listen** 例： `Device(config-if)# ip wccp 99 group-listen`	インターフェイスを設定して、WCCP の IP マルチキャスト パケットの受信をイネーブルまたはディセーブルにします。

WCCP サービス グループのアクセス リストの使用

どのトラフィックをどのコンテンツエンジンに送信するかを決定するためにアクセスリストを使用するようにデバイスを設定するには、次の作業を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> 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： `Device# 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	**access-list** *access-list-number* **remark** *remark* 例： `Device(config)# access-list 1 remark Give access to user1`	（任意）アクセスリストエントリに関してユーザーにわかりやすいコメントを追加します。 • 最大 100 文字の注釈をアクセス リスト エントリの前または後に指定できます。
ステップ 4	**access-list** *access-list-number* **permit** {*source* [*source-wildcard*] | **any**} [**log**] 例： `Device(config)# access-list 1 permit 172.16.5.22 0.0.0.0`	キャッシュエンジンへのトラフィックリダイレクトを有効または無効にし、送信元アドレスとワイルドカードマスクに基づいて指定された送信元を許可するアクセスリストを作成します。 • すべてのアクセス リストには、1 つ以上の許可文が必要です。許可文は、最初のエントリである必要はありません。 • 標準 IP アクセス リストには、1 ～ 99 または 1300 ～ 1999 の番号を付けます。 • *source-wildcard* を省略すると、0.0.0.0 というワイルドカードマスクが想定されます（つまり、すべての送信元アドレスに一致します）。 • 必要に応じて、*source source-wildcard* の代わりに、キーワード **any** を使用して、送信元と 0.0.0.0 255.255.255.255 の送信元ワイルドカードを指定できます。 • この例では、ホスト 172.16.5.22 がアクセス リストに合格できます。

	コマンドまたはアクション	目的
ステップ 5	**access-list** *access-list-number* **remark** *remark* 例： `Device(config)# access-list 1 remark Give access to user1`	（任意）アクセス リスト エントリに関してユーザーにわかりやすいコメントを追加します。 • 最大 100 文字の注釈をアクセス リスト エントリの前または後に指定できます。
ステップ 6	**access-list** *access-list-number* **deny** {*source* [*source-wildcard*] | **any**} | [**log**] 例： `Device(config)# access-list 1 deny 172.16.7.34 0.0.0.0`	送信元アドレスおよびワイルドカードマスクに基づいて、指定した送信元を拒否します。 • *source-wildcard* を省略すると、0.0.0.0 というワイルドカードマスクが想定されます（つまり、すべての送信元アドレスに一致します）。 • 必要に応じて、*source source-wildcard* の代わりに省略形 any を使用すると、送信元と 0.0.0.0 255.255.255.255 の送信元ワイルドカードを指定できます。 • この例では、ホスト 172.16.7.34 はアクセス リストへの合格が拒否されます。
ステップ 7	アクセス リストの基礎とする送信元の指定が完了するまで、ステップ 3 ～ 6 の手順を繰り返します。	明示的に許可されていないすべての送信元は、アクセス リストの末尾にある暗黙的な **deny** ステートメントで拒否されます。
ステップ 8	**ip wccp web-cache group-list** *access-list* 例： `Device(config) ip wccp web-cache group-list 1`	パケットを受け入れるコンテンツエンジンの IP アドレスをデバイスに示します。
ステップ 9	**ip wccp web-cache redirect-list** *access-list* 例： `Device(config)# ip wccp web-cache redirect-list 1`	（任意）特定のクライアントのキャッシングをディセーブルにします。

WCCP 発信 ACL チェックのイネーブル化

（注） ハードウェアですべてのリダイレクションを実行する場合、発信 ACL チェック処理をイネーブルにすると、リダイレクションのモードは変わります。ショートカットをインストールする前に、追加の ACL チェックがソフトウェアで実行できるように、最初のパケットは切り替えられます。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip wccp** {**web-cache** | *service-number*} [**group-address** *multicast-address*] [**redirect-list** *access-list*] [**group-list** *access-list*] [**password** *password*]
4. **ip wccp check acl outbound**
5. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> 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： `Device# 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	**ip wccp** {**web-cache** | *service-number*} [**group-address** *multicast-address*] [**redirect-list** *access-list*] [**group-list** *access-list*] [**password** *password*] 例： `Device(config)# ip wccp web-cache`	Cisco Content Engine のサービス グループまたはコンテンツ エンジンのサービス グループのサポートをイネーブルにし、リダイレクト ACL リストまたはグループ ACL を設定します。 （注） **web-cache** キーワードは WCCP バージョン 1 とバージョン 2 に使用することができ、*service-number* 引数は WCCP バージョン 2 のみに使用できます。
ステップ 4	**ip wccp check acl outbound** 例： `Device(config)# ip wccp check acl outbound`	WCCP によってリダイレクトされたパケットの出力インターフェイスのアクセスコントロールリスト（ACL）をチェックします。
ステップ 5	**exit** 例： `Device(config)# exit`	グローバル コンフィギュレーションを終了します。

WCCP 設定の確認およびモニタリング

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> 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 ip wccp** [**web-cache** |*service-number*] [**detail view**] 例： `Device# show ip wccp 24 detail`	WCCP に関連するグローバル情報を表示します。たとえば、実行されているプロトコル バージョン、ルータ サービス グループのコンテンツ エンジンの数、ルータに接続できるコンテンツエンジン グループ、使用するアクセス リストなどです。 • *service-number*：（任意）コンテンツエンジンで制御される Web キャッシュサービスグループのダイナミック番号。有効な範囲は 0 ～ 99 です。Cisco Content Engine を使用する Web キャッシュの場合、逆プロキシ サービスは 99 の値で示されます。 • **web-cache**：（任意）Web キャッシュサービスの統計情報。 • **detail**：（任意）検出済み、または検出されていない特定のサービスグループまたは Web キャッシュの他のメンバ。 • **view**：（任意）ルータまたはすべての Web キャッシュに関する情報。
ステップ 3	**show ip interface** 例： `Device# show ip interface`	「Web Cache Redirect is enabled / disabled」など、いずれかの **ip wccp redirection** コマンドがインターフェイスで設定されているかどうかに関するステータスを表示します。
ステップ 4	**more system:running-config** 例： `Device# more system:running-config`	（任意）実行されている構成ファイルのコンテンツを表示します（**show running-config** コマンドと同じです）。

WCCP の設定例

例：一般的な WCCPv2 セッションの設定

```
Device# configure terminal
Device(config)# ip wccp web-cache group-address 224.1.1.100 password password
Device(config)# ip wccp source-interface GigabitEthernet 0/1/0
Device(config)# ip wccp check services all
! Configures a check of all WCCP services.
Device(config)# interface GigabitEthernet 0/1/0
Device(config-if)# ip wccp web-cache redirect in
Device(config-if)# exit
Device(config)# interface GigabitEthernet 0/2/0
Device(config-if)# ip wccp redirect exclude in
Device(config-if)# exit
```

例：デバイスとコンテンツエンジンのパスワードの設定

```
Device# configure terminal
Device(config)# ip wccp web-cache password password1
```

例：Web キャッシュ サービスの設定

```
Device# configure terminal
Device(config)# ip wccp web-cache
Device(config)# interface GigabitEthernet 0/1/0
Device(config-if)# ip wccp web-cache redirect in
Device(config-if)# exit
Device# copy running-config startup-config
```

次に、ギガビットインターフェイス 0/1/0 に到達する HTTP トラフィックのリダイレクションを有効にするセッションの設定例を示します。

```
Device# configure terminal
Device(config)# interface GigabitEthernet 0/1/0
Device(config-if)# ip wccp web-cache redirect in
Device(config-if)# exit
Device# show ip interface GigabitEthernet 0/1/0
.
.
.
WCCP Redirect inbound is enabled
WCCP Redirect exclude is disabled
.
.
.
```

例：逆プロキシ サービスの実行

次の例では、Cisco Cache Engine を使用してサービス グループを設定し、ダイナミック サービス 99 を使用して逆プロキシ サービスを実行しているという前提です。

```
Device# configure terminal
Device(config)# ip wccp 99
Device(config)# interface gigabitethernet 0/1/0
Device(config-if)# ip wccp 99 redirect out
```

例：マルチキャストアドレスへのデバイスの登録

```
Device# configure terminal
Device(config)# ip wccp web-cache group-address 224.1.1.100
Device(config)# interface gigabitethernet 0/1/0
Device(config-if)# ip wccp web-cache group-listen
```

次に、マルチキャストアドレス 224.1.1.1 を使用してリバースプロキシサービスを実行するようにデバイスを設定する例を示します。リダイレクションは、ギガビットイーサネットインターフェイス 0/1/0 経由で送信されるパケットに適用されます。

```
Device# configure terminal
Device(config)# ip wccp 99 group-address 224.1.1.1
Device(config)# interface gigabitethernet 0/1/0
Device(config-if)# ip wccp 99 redirect out
```

例：アクセス リストの使用

セキュリティを改善するには、標準のアクセスリストを使用して、現在のデバイスに登録するコンテンツエンジンで有効なアドレスがどの IP アドレスかをデバイスに通知します。次に、サンプル ホストのアクセス リスト番号が 10 である標準的なアクセス リストの設定セッション例を示します。

```
Device(config)# access-list 10 permit host 10.1.1.1
Device(config)# access-list 10 permit host 10.1.1.2
Device(config)# access-list 10 permit host 10.1.1.3
Device(config)# ip wccp web-cache group-list 10
```

特定のクライアント、サーバー、またはクライアント/サーバー ペアに対してキャッシングをディセーブルにするには、WCCP アクセス リストを使用します。次に、10.1.1.1 から 10.3.1.1 に送信される要求がキャッシュをバイパスし、その他すべての要求は通常どおりに処理される例を示します。

```
Device(config)# ip wccp web-cache redirect-list 120
Device(config)# access-list 120 deny tcp host 10.1.1.1 any
Device(config)# access-list 120 deny tcp any host 10.3.1.1
Device(config)# access-list 120 permit ip any any
```

次の例では、ギガビットイーサネット 0/1/0 を介して受信した Web 関連のパケットを、209.165.200.224 以外の任意のホストにリダイレクトするようにデバイスを設定します。

```
Device(config)# access-list 100 deny ip any host 209.165.200.224
Device(config)# access-list 100 permit ip any any
Device(config)# ip wccp web-cache redirect-list 100
Device(config)# interface gigabitethernet 0/1/0
Device(config-if)# ip wccp web-cache redirect in
```

例：WCCP 発信 ACL チェックの設定

次に、ネットワーク 10.0.0.0 からのトラフィックがギガビットイーサネットインターフェイス 0/1/0 を離れないようにアクセスリストを設定する例を示します。発信 ACL チェックはイネーブルなので、WCCP はそのトラフィックをリダイレクトしません。WCCP は、パケットのリダイレクト前に、ACL に対してパケットをチェックします。

```
Device(config)# ip wccp web-cache
Device(config)# ip wccp check acl outbound
Device(config)# interface gigabitethernet 0/1/0
Device(config-if)# ip access-group 10 out
Device(config-if)# exit
Device(config)# ip wccp web-cache redirect-list redirect-out
Device(config)# access-list 10 deny 10.0.0.0 0.255.255.255
Device(config)# access-list 10 permit any
```

発信 ACL チェックをディセーブルにする場合、ネットワーク 10.0.0.0 からの HTTP パケットを Web キャッシュにリダイレクトします。そのネットワーク アドレスを使用するユーザーは、ネットワーク管理者が回避しようとしても、Web ページを取得できます。

例：WCCP 設定の確認

次に、特権 EXEC モードで **more system:running-config** コマンドを使用して設定の変更を検証する例を示します。次に、Web キャッシュサービスおよびダイナミックサービス 99 の両方をデバイスで有効にする例を示します。

```
Device# more system:running-config

 Building configuration...
 Current configuration:
 !
 version 12.0
 service timestamps debug uptime
 service timestamps log uptime
 no service password-encryption
 service udp-small-servers
 service tcp-small-servers
 !
 hostname router4
 !
 enable secret 5 $1$nSVy$faliJsVQXVPW.KuCxZNTh1
 enable password password1
 !
 ip subnet-zero
 ip wccp web-cache
 ip wccp 99
 ip domain-name cisco.com
 ip name-server 10.1.1.1
```

```
ip name-server 10.1.1.2
ip name-server 10.1.1.3
!
!
!
interface GigabitEthernet0/1/1
ip address 10.3.1.2 255.255.255.0
no ip directed-broadcast
ip wccp web-cache redirect in
ip wccp 99 redirect in
no ip route-cache
no ip mroute-cache
!
interface GigabitEthernet0/1/0
ip address 10.4.1.1 255.255.255.0
no ip directed-broadcast
ip wccp 99 redirect in
no ip route-cache
no ip mroute-cache
!
interface Serial0
no ip address
no ip directed-broadcast
no ip route-cache
no ip mroute-cache
shutdown
!
interface Serial1
no ip address
no ip directed-broadcast
no ip route-cache
no ip mroute-cache
shutdown
!
ip default-gateway 10.3.1.1
ip classless
ip route 0.0.0.0 0.0.0.0 10.3.1.1
no ip http server
!
!
!
line con 0
transport input none
line aux 0
transport input all
line vty 0 4
password password1
login
!
end
```

次に、WCCP に関連したグローバル統計情報を表示する方法の例を示します。

```
Device# show ip wccp web-cache detail

WCCP Client information:
WCCP Client ID:      10.1.1.2
Protocol Version:    2.0
State:               Usable
Redirection:         L2
Packet Return:       L2
Packets Redirected:  0
Connect Time:        00:20:34
Assignment:          MASK
```

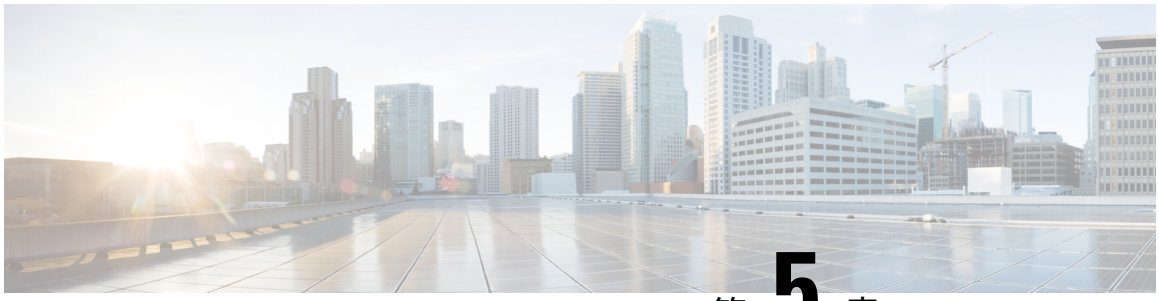
```
Mask  SrcAddr    DstAddr    SrcPort DstPort
----  -------    -------    ------- -------
0000: 0x00000000 0x00001741 0x0000  0x0000
Value SrcAddr    DstAddr   SrcPort DstPort CE-IP
----- -------    -------   ------- ------- -----
0000: 0x00000000 0x00000000 0x0000 0x0000 0x3C010102 (10.1.1.2)
0001: 0x00000000 0x00000001 0x0000 0x0000 0x3C010102 (10.1.1.2)
0002: 0x00000000 0x00000040 0x0000 0x0000 0x3C010102 (10.1.1.2)
0003: 0x00000000 0x00000041 0x0000 0x0000 0x3C010102 (10.1.1.2)
0004: 0x00000000 0x00000100 0x0000 0x0000 0x3C010102 (10.1.1.2)
0005: 0x00000000 0x00000101 0x0000 0x0000 0x3C010102 (10.1.1.2)
0006: 0x00000000 0x00000140 0x0000 0x0000 0x3C010102 (10.1.1.2)
```

show ip wccp web-cache コマンドの詳細については、『*Cisco IOS IP Application Services Command Reference*』を参照してください。

WCCP の機能情報

表 *5 : WCCP* の機能情報

機能名	リリース	機能情報
Cisco Catalyst 9300 シリーズ スイッチでの WCCP サポート	Cisco IOS XE Everest 16.6.1	Web Cache Communication Protocol（WCCP）はシスコが開発したコンテンツルーティングテクノロジーです。IP パケットを代行受信し、IP パケットに指定されている宛先とは別の宛先にそのパケットをリダイレクトします。 WCCP を使用すると、コンテンツエンジンをネットワーク インフラストラクチャに統合できます。 .



第 5 章

拡張オブジェクト トラッキングの設定

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。最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、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。

拡張オブジェクト トラッキングに関する情報

拡張オブジェクト トラッキングの概要

拡張オブジェクト トラッキング機能が導入される前は、ホットスタンバイ ルータ プロトコル（HSRP）に単純なトラッキング メカニズムが内蔵されていますた。このメカニズムでは、インターフェイスのラインプロトコルのステートしか追跡することができませんでした。インターフェイスのラインプロトコル ステートがダウンになった場合、ルータの HSRP 優先度は削減され、より高い優先度のもう 1 つの HSRP ルータがアクティブになることができます。

拡張オブジェクトトラッキング機能は、HSRPからトラッキング メカニズムを分離させて、独立したトラッキングプロセスを別途生成します。これにより、HSRP以外のプロセスがこのトラッキングプロセスを使用できます。この機能を使用すると、インターフェイスのラインプロトコルのステートに加えて他のオブジェクトも追跡できます。

HSRP、仮想ルータ冗長プロトコル（VRRP）、Gateway Load Balancing Protoco（GLBP）などのクライアント プロセスで、トラッキング オブジェクトに対する興味を登録し、追跡対象オブジェクトの状態が変化したときに通知を受け取るようにすることができます。

各追跡対象オブジェクトには、トラッキング コマンドライン インターフェイス（CLI）で指定される一意の番号があります。クライアントプロセスは、この番号を使用して特定のオブジェクトを追跡します。トラッキングプロセスは、追跡対象オブジェクトに値の変化がないかどうかを定期的にポーリングし、（アップまたはダウン値など）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。同じオブジェクトを複数のクライアントが追跡して、オブジェクトのステートが変化した場合に、それぞれが異なるアクションを実行できます。

複数のオブジェクトを組み合わせて1つのリストにして追跡することもできます。このリストの状態判定には、重みしきい値またはパーセンテージを使用します。オブジェクトの組み合わせには、ブールロジックを使用できます。「AND」ブール関数を使用する追跡リストの場合、リスト内の各オブジェクトがアップ ステートでないと追跡対象オブジェクトはアップになりません。「OR」ブール関数を使用する追跡リストの場合、リスト内の 1 つのオブジェクトだけがアップ ステートであれば追跡対象オブジェクトはアップになります。

インターフェイス ラインプロトコルまたは IP ルーティング ステートのトラッキング

インターフェイス ラインプロトコル ステートまたはインターフェイス IP ルーティング ステートのいずれかを追跡できます。IPルーティング ステートを追跡する場合、オブジェクトをアップするには次の 3 つの条件が必要です。

- インターフェイス上で IP ルーティングがイネーブル、かつアクティブになっている。
- インターフェイス ラインプロトコル ステートが使用可能な状態（アップ）にある。
- 既知のインターフェイス IP アドレスを使用している。

この 3 つの条件がすべて合致しないと、IP ルーティング ステートはダウンになります。

追跡リスト

オブジェクトの追跡リストは、ブール式、重みしきい値、またはパーセントしきい値を使用して設定できます。トラッキング対象リストには1つまたは複数のオブジェクトが含まれます。オブジェクトは存在していないと追跡リストに追加できません。

- 設定にブール式による演算を指定する場合は、「AND」または「OR」演算子を使用します。

- 追跡リストのステートを重みしきい値で判定する場合は、追跡リスト内の各オブジェクトに重み番号を割り当てます。追跡リストのステートは、このしきい値に合致したかどうかで判定されます。各オブジェクトのステートは、すべてのオブジェクトの重みの合計と各オブジェクトのしきい値の重みを比較して判定されます。
- 追跡リストをパーセントしきい値で判定する場合は、追跡リスト内のすべてのオブジェクトにパーセントしきい値を割り当てます。各オブジェクトのステートは、各オブジェクトに割り当てたパーセンテージとリストを比較して判定されます。

他の特性のトラッキング

拡張オブジェクト トラッキングを使用して他の特性を追跡することもできます。

- **track ip route reachability** グローバル コンフィギュレーション コマンドを使用すると、IP ルートの到達可能性を追跡できます。
- **track ip route metric threshold** グローバル コンフィギュレーション コマンドを使用すると、ルートがしきい値を超えているか下回っているかを確認できます。
- **track resolution** グローバル コンフィギュレーション コマンドを使用すると、ルーティング プロトコルのメトリック解決のデフォルト値を変更できます。
- **track timer tracking** コンフィギュレーション コマンドを使用すると、トラッキング対象オブジェクトを定期的にポーリングするようにトラッキング プロセスを設定できます。

拡張オブジェクトトラッキング設定を確認する場合は、 **show track** 特権 EXEC コマンドを使用してください。

IP SLA オブジェクト トラッキング

Cisco IOS IP サービス レベル契約（SLA）は、ネットワーク パフォーマンスの測定と診断を行うツールです。ネットワーク パフォーマンスを測定するためのトラフィック生成には、アクティブ モニタリングが使用されます。Cisco IP SLA 動作は、ネットワークのトラブルシューティングや設計、分析に使用できるリアルタイム メトリックを収集します。

IP SLA 動作のオブジェクト トラッキングを活用すると、クライアントは IP SLA オブジェクトの出力を追跡して、その情報をアクションのトリガーに使用できます。各 IP SLA 動作は、OK または OverThreshold のような簡易ネットワーク管理プロトコル（SNMP）動作の戻りコード値を保持しているため、トラッキング プロセス側で解釈できます。ステートと到達可能性という IP SLA 動作の 2 つの側面をトラッキングできます。ステートの場合、戻りコードが OK のとき、トラック ステートがアップします。リターン コードが OK ではないとき、トラック ステートはダウンします。到達可能性の場合、戻りコードが OK または OverThreshold のとき、到達可能性がアップします。リターン コードが OK ではないとき、到達可能性はダウンします。

スタティック ルート オブジェクト トラッキング

拡張オブジェクトトラッキングを使用したスタティック ルーティング サポートにより、device でICMP ping を使用して、設定済みのスタティックルートまたはDHCP ルートがダウンしていることを認識できます。トラッキングを有効にしている場合、システムはルート ステートを追跡し、ステートの変化をクライアントに通知できます。スタティック ルート オブジェクト トラッキングは、プライマリ ゲートウェイへの接続状態をモニターするために、Cisco IP SLA を使用して ICMP ping を生成します。

拡張オブジェクト トラッキングの設定方法

インターフェイスでのライン ステート プロトコルまたは IP ルーティング ステートのトラッキングの設定

インターフェイスのラインプロトコル ステートまたはIP ルーティング ステートを追跡するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **track** *object-number***interface** *interface-id***line-protocol**
4. **delay** { *object-number***up***seconds*[**down***seconds*]|[**up***seconds*]**down***seconds*}
5. **exit**
6. **track** *object-number***interface** *interface-id***ip routing**
7. **delay** { *object-number***up***seconds*[**down***seconds*]|[**up***seconds*]**down***seconds*}
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： `デバイス> 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： `デバイス# 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	**track** *object-number***interface** *interface-id***line-protocol** 例： `デバイス(config)# track 33 interface gigabitethernet 1/0/1 line-protocol`	（任意）インターフェイスのラインプロトコル ステートを追跡するための追跡リストを作成し、トラッキング コンフィギュレーション モードを開始します。 • object-number：追跡対象オブジェクトの番号です。指定できる範囲は 1 ～ 500 です。 • **interface** interface-id は、追跡されるインターフェイスです。
ステップ 4	**delay** { *object-number***up***seconds*[**down***seconds*][**up***seconds*]**down***seconds*}	（任意）追跡対象オブジェクトのステート変更の通信を遅延させる時間（秒）を指定します。指定できる範囲は 1 ～ 180 秒です。
ステップ 5	**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 6	**track** *object-number***interface** *interface-id***ip routing** 例： `デバイス(config)# track 33 interface gigabitethernet 1/0/1 ip routing`	（任意）インターフェイスの IP ルーティング ステートを追跡するための追跡リストを作成し、トラッキング コンフィギュレーション モードを開始します。IP ルート追跡では、ルーティング テーブル内の IP ルートおよびインターフェイスの IP パケット ルーティング機能を追跡します。 • object-number：追跡対象オブジェクトの番号です。指定できる範囲は 1 ～ 500 です。 • **interface** interface-id は、追跡されるインターフェイスです。
ステップ 7	**delay** { *object-number***up***seconds*[**down***seconds*][**up***seconds*]**down***seconds*}	（任意）追跡対象オブジェクトのステート変更の通信を遅延させる時間（秒）を指定します。指定できる範囲は 1 ～ 180 秒です。
ステップ 8	**end**	特権 EXEC モードに戻ります。
ステップ 9	**show track***object-number*	指定したオブジェクトが追跡されているかどうかを確認します。

追跡リストの設定

重みしきい値による追跡リストの設定

重みしきい値による追跡を行うには、複数オブジェクトを含んだ追跡リストを作成し、重みをしきい値として使用することを指定したあと、各オブジェクトに重み値を設定します。各オブジェクトのステートは、アップであるすべてのオブジェクトの重み合計と各オブジェクトのしきい値の重みを比較して判定されます。

重みしきい値のリストには、「NOT」ブール演算子を使用できません。

重みしきい値を使用してオブジェクトの追跡リストを作成し、各オブジェクトに重み値を設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **track** *track-number***list threshold** {**weight**}
4. **object** *object-number*[**weight***weight-number*]
5. **threshold weight** {**up***number*|[**down***number*]}
6. **delay** { **up***seconds*[**down***seconds*]|[**up***seconds*]**down***seconds*}
7. **end**
8. **show track***object-number*
9. **copy running-config startup-config**

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： `デバイス> 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： `デバイス# 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** *track-number***list threshold** {**weight**} 例： `デバイス(config)# track 4 list threshold weight`	トラッキング対象リスト オブジェクトを設定し、トラッキング コンフィギュレーション モードを開始します。指定できる track-number の範囲は 1 ～ 500 です。 • **threshold—**追跡リストのステートがしきい値に基づくことを指定します。

	コマンドまたはアクション	目的
		• **weight—** しきい値が重みに基づくことを指定します。
ステップ 4	**object** *object-number*[**weight***weight-number*] 例： デバイス**(config)# object 2 weight 15**	追跡対象のオブジェクトを指定します。指定できる範囲は 1 ～ 500 です。任意の **weight***weight-number* には、オブジェクトのしきい値の重みを指定します。範囲は 1 ～ 255 です。 （注） オブジェクトは存在していないと追跡リストに追加できません。
ステップ 5	**threshold weight** {**up***number*|[**down***number*]} 例： デバイス**(config-track)# threshold weight up 30 down 10**	（任意）重みしきい値を指定します。 • **up***number*：範囲は 1 ～ 255 です。 • **down***number*：（任意）範囲は **up***number* で選択した数値によって異なります。**up***number* を 25 に設定すると、down number の範囲は 0 ～ 24 になります。
ステップ 6	**delay** { **up***seconds*[**down***seconds*]|[**up***seconds*]**down***seconds*}	（任意）追跡対象オブジェクトのステート変更の通信を遅延させる時間（秒）を指定します。指定できる範囲は 1 ～ 180 秒です。
ステップ 7	**end**	特権 EXEC モードに戻ります。
ステップ 8	**show track***object-number*	指定したオブジェクトが追跡されているかどうかを確認します。
ステップ 9	**copy running-config startup-config** 例： デバイス# **copy running-config startup-config**	（任意）コンフィギュレーションファイルに設定を保存します。

パーセントしきい値による追跡リストの設定

パーセントしきい値による追跡を行うには、複数オブジェクトを含んだ追跡リストを作成し、パーセンテージをしきい値として使用することを指定したあと、リスト内のすべてのオブジェクトにパーセンテージを指定します。リストのステートは、各オブジェクトに割り当てたパーセンテージとリストを比較して判定されます。

パーセントしきい値のリストには、「NOT」ブール演算子を使用できません。

パーセントしきい値を使用してオブジェクトの追跡リストを設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **track** *track-number***list threshold** {**percentage**}
4. **object** *object-number*
5. **threshold percentage** {**up***number*|[**down***number*]}
6. **delay** { **up***seconds*[**down***seconds*]|[**up***seconds*]**down***seconds*}
7. **end**
8. **show track***object-number*
9. **copy running-config startup-config**

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： `デバイス> 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： `デバイス# 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** *track-number***list threshold** {**percentage**} 例： `デバイス(config)# track 4 list threshold percentage`	トラッキング対象リスト オブジェクトを設定し、トラッキング コンフィギュレーション モードを開始します。指定できる track-number の範囲は 1 ～ 500 です。 • **threshold—**追跡リストのステートがしきい値に基づくことを指定します。 • **percentage—** しきい値がパーセンテージに基づくことを指定します。
ステップ 4	**object** *object-number* 例： `デバイス(config)# object 1`	追跡対象のオブジェクトを指定します。指定できる範囲は 1 ～ 500 です。 （注） オブジェクトは存在していないと追跡リストに追加できません。
ステップ 5	**threshold percentage** {**up***number*|[**down***number*]} 例：	（任意）パーセントしきい値を指定します。 • **up***number*：範囲は 1 ～ 100 です。

	コマンドまたはアクション	目的
	デバイス(config)# threshold percentage up 51 down 10	• **down***number*：（任意）範囲は **up***number* で選択した数値によって異なります。**up***number* を 25 に設定すると、down number の範囲は 0 ～ 24 になります。
ステップ 6	**delay** { **up***seconds*[**down***seconds*]|[**up***seconds*]**down***seconds*}	（任意）追跡対象オブジェクトのステート変更の通信を遅延させる時間（秒）を指定します。指定できる範囲は 1 ～ 180 秒です。
ステップ 7	**end**	特権 EXEC モードに戻ります。
ステップ 8	**show track***object-number*	指定したオブジェクトが追跡されているかどうかを確認します。
ステップ 9	**copy running-config startup-config** 例： デバイス# copy running-config startup-config	（任意）コンフィギュレーション ファイルに設定を保存します。

HSRP オブジェクト トラッキングの設定

特定のオブジェクトを追跡し、そのオブジェクトのステートに基づいてHSRPプライオリティを変更できるようにスタンバイ HSRP グループを設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **track** *object-number*{**interface** *interface-id*{**line-protocol**|**ip routing**}|**ip route***ip address/prefix-length*{**metric threshold**|**reachability**}**list**{**boolean**{**and**|**or**}}|{**threshold**{**weight**|**percentage**}}}
4. **exit**
5. **interface** { *interface-id*
6. **standby**[*group-number*]**ip**[*ip-address***secondary**]]
7. **standby**[*group-number*]**track**[*object-number*[**decrement** *priority-decrement*]]
8. **end**
9. **show standby**
10. **copy running-config startup-config**

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： デバイス> **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： デバイス# **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** *interface-id*{**line-protocol**|**ip routing**}|**ip route***ip address/prefix-length*{**metric threshold**|**reachability**}}**list**{**boolean**{**and**|**or**}}{**threshold**{**weight**|*percentage*}}}	（任意）設定されたステートを追跡するための追跡リストを作成し、トラッキング コンフィギュレーション モードを開始します。 • object-number：追跡対象オブジェクトの番号です。指定できる範囲は 1 ～ 500 です。 • 追跡するインターフェイスを指定するには、**interface** *interface-id* を入力します。 • インターフェイス ライン プロトコルの状態を追跡するには **line-protocol** を入力します。また、インターフェイス IP ルーティングの状態を追跡するには、**ip routing** を入力します。 • IP ルートの状態を追跡するには、**ip route***ip-address/prefix-length* を入力します。 • しきい値メトリックを追跡する場合は **metric threshold**、ルートが到達可能かどうかを追跡するには **reachability** を入力します。 デフォルトの up しきい値は 254、デフォルトの down しきい値は 255 です。 • リスト内の一連のオブジェクトを追跡するには、**list** を入力します。 （注） 追跡するインターフェイスごとにこの手順を繰り返してください。
ステップ 4	**exit**	グローバル コンフィギュレーション モードに戻ります。

	コマンドまたはアクション	目的
ステップ 5	**interface** { *interface-id*	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	**standby**[*group-number*]**ip**[*ip-address***secondary**]]	HSRP グループの番号および仮想 IP アドレスを使用して、HSRP グループを作成（またはイネーブルに）します。 • （任意）*group-number*：HSRP をイネーブルにするインターフェイスのグループ番号を入力します。指定できる範囲は 0 ～ 255 です。デフォルトは 0 です。HSRP グループが 1 つしかない場合は、グループ番号を入力する必要はありません。 • （1 つのインターフェイスで必須、それ以外は任意）*ip-address*：ホットスタンバイ ルータ インターフェイスの仮想 IP アドレスを指定します。少なくとも 1 つのインターフェイスに対して仮想 IP アドレスを入力する必要があります。他のインターフェイスは、その仮想 IP アドレスを学習します。 • （任意）**secondary**：IP アドレスがセカンダリ ホット スタンバイ ルータ インターフェイスであることを指定します。このキーワードが省略された場合、設定されたアドレスはプライマリ IP アドレスになります。
ステップ 7	**standby**[*group-number*]**track**[*object-number*[**decrement** *priority-decrement*]]	特定のオブジェクトを追跡し、そのオブジェクト ステートに基づいてホットスタンバイ プライオリティを変更できるように HSRP を設定します。 • （任意）*group-number*：追跡が適用されるグループ番号を入力します。 • *object-number*：追跡対象のオブジェクト番号を入力します。指定できる範囲は 1 ～ 500 で、デフォルトは 1 です。 • （任意）**secondary**：IP アドレスがセカンダリ ホット スタンバイ ルータ インターフェイスであることを指定します。このキーワードが省略された場合、設定されたアドレスはプライマリ IP アドレスになります。 • （任意）**decrement***priority-decrement*：追跡対象のオブジェクトがダウンになった場合（また

	コマンドまたはアクション	目的
		はアップに戻った場合）に、ルータのホットスタンバイの優先順位を減少（または増加）させる幅を指定します。指定できる範囲は 1 ～ 255 で、デフォルトは 10 です。
ステップ 8	**end**	特権 EXEC モードに戻ります。
ステップ 9	**show standby**	スタンバイ ルータの IP アドレスおよび追跡ステートを確認します。
ステップ 10	**copy running-config startup-config** 例： `デバイス# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

IP SLA オブジェクト トラッキングの設定

IP SLA 動作のステートまたは IP SLA IP ホストの到達可能性を追跡するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **track** *object-number* **ip sla** *operation-number* {**state** | **reachability**}
4. **delay** { **up***seconds*[**down***seconds*]|[**up***seconds*]**down***seconds*}
5. **end**
6. **show track***object-number*
7. **copy running-config startup-config**

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： `デバイス> 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：	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
	デバイス# **configure terminal**	
ステップ 3	**track** *object-number* **ip sla** *operation-number* {**state** | **reachability**} 例： デバイス**(config)# track 2 ip sla 123 state**	トラッキング コンフィギュレーション モードを開始し、IP SLA 動作のステートを追跡します。 • *object-number* の範囲は 1 ～ 500 です。 • *operation-number* の範囲は 1 ～ 2147483647 です。
ステップ 4	**delay** { **up***seconds*[**down***seconds*]|[**up***seconds*]**down***seconds*}	（任意）追跡対象オブジェクトのステート変更の通信を遅延させる時間（秒）を指定します。指定できる範囲は 1 ～ 180 秒です。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show track***object-number*	指定したオブジェクトが追跡されているかどうかを確認します。
ステップ 7	**copy running-config startup-config** 例： デバイス# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

スタティック ルート オブジェクト トラッキングの設定

スタティック ルーティング用のプライマリ インターフェイスの設定

スタティック ルーティングのプライマリ インターフェイスを設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface***interface-id*
4. **description***string*
5. **ip address***ip-address mask*[**secondary**]
6. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： デバイス> **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： デバイス# **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***interface-id*	プライマリまたはセカンダリ インターフェイスを選択し、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	**description***string*	インターフェイスに説明を追加します。
ステップ 5	**ip address***ip-address mask*[**secondary**]	インターフェイスのプライマリまたはセカンダリ IP アドレスを設定します。
ステップ 6	**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。

DHCP のプライマリ インターフェイスの設定

DHCP のプライマリ インターフェイスを設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface***interface-id*
4. **description***string*
5. **ip dhcp client route track***number*
6. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例：	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）。

	コマンドまたはアクション	目的
	デバイス> **enable**	
ステップ 2	**configure terminal** 例： デバイス# **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***interface-id*	プライマリまたはセカンダリ インターフェイスを選択し、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	**description***string*	インターフェイスに説明を追加します。
ステップ 5	**ip dhcp client route track***number*	DHCP クライアントを設定し、追加されたルートを指定の追跡番号に関連付けます。有効な数値は 1 ～ 500 です。
ステップ 6	**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。

IP SLA モニタリング エージェントの設定

プライマリ インターフェイスおよびエージェント状態をモニターするトラック オブジェクトを使用して、IP アドレスの ping を実行するように IP SLA エージェントを設定することができます。

Cisco IP SLA でネットワーク モニタリングを設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip sla***operation number*
4. **icmp-echo**{ *destination ip-address*|*destination hostname*[**source - ipaddr**{*ip-address*|*hostname***source-interface***interface-id*]
5. **timeout***milliseconds*
6. **frequency***seconds*
7. **threshold***milliseconds*
8. **exit**
9. **ip sla schedule** *operation-number*[**life** {**forever**|*seconds*}]**start-time***time*|**pending**|**now**|**after***time*]**ageout***seconds*][**recurring**]
10. **track** *object-number***rtr** *operation-number***statereachability**
11. **end**
12. **show track***object-number*

13. **copy running-config startup-config**

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： デバイス> **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： デバイス# **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	**ip sla***operation number*	Cisco IP SLA 動作の設定を開始し、IP SLA 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	**icmp-echo**{ *destination ip-address*|*destination hostname*[**source - ipaddr**{*ip-address*|*hostname***source-interface***interface-id*]	Cisco IP SLA エンドツーエンド ICMP エコー応答時間動作を設定し、IP SLA ICMP エコー 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	**timeout***milliseconds*	要求パケットの応答に対する動作の待機時間を設定します。
ステップ 6	**frequency***seconds*	動作がネットワークに送信される頻度を設定します。
ステップ 7	**threshold***milliseconds*	反応イベントを生成し、その動作の履歴情報を保存するしきい値（ヒステリシス）の上限を設定します。
ステップ 8	**exit**	IP SLA ICMP エコー コンフィギュレーション モードを終了します。
ステップ 9	**ip sla schedule** *operation-number*[**life** {**forever**|*seconds*}][**start-time***time*|**pending**|**now**|**after***time*][**ageout***seconds*][**recurring**] 例： デバイス(config)# track 2 200 state	単一の IP SLA 動作のスケジューリング パラメータを設定します。 • *object-number* の範囲は 1 ～ 500 です。 • *operation-number* の範囲は 1 ～ 2147483647 です。
ステップ 10	**track** *object-number***rtr** *operation-number***statereachability**	Cisco IOS IP SLA 動作の状態を追跡し、トラッキング コンフィギュレーション モードを開始します。
ステップ 11	**end**	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 12	**show track***object-number*	指定したオブジェクトが追跡されているかどうかを確認します。
ステップ 13	**copy running-config startup-config** 例： デバイス# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

ルーティング ポリシーおよびデフォルト ルートの設定

オブジェクト トラッキングを使用してバックアップ スタティック ルーティングのルーティング ポリシーを設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **access-list***access-list-number*
4. **route-map***map tag*[**permit**|**deny**][*sequence-number*]
5. **match ip address**{*access-list number*[**permit**|**deny**][*sequence-number*]
6. **set ip next-hop dynamic dhcp**
7. **set interface***interface-id*
8. **exit**
9. **ip local policy route-map***map tag*
10. **ip route***prefix mask*{*ip address*|*interface-id*[*ip address*]}[*distance*][*name*][**permanent**|**track***track-number*][*tag tag*]
11. **end**
12. **show ip route track table**
13. **copy running-config startup-config**

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： デバイス> **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： デバイス# **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	**access-list***access-list-number*	拡張 IP アクセス リストを定義します。オプションの文字を設定します。
ステップ 4	**route-map***map tag*[**permit**|**deny**][*sequence-number*]	ルートマップ コンフィギュレーション モードを開始し、特定のルーティングから別のルーティングへの再配信ルートの条件を定義します。
ステップ 5	**match ip address**{*access-list number*[**permit**|**deny**][*sequence-number*]	標準または拡張アクセス リストに許可された宛先ネットワーク番号アドレスを持つルートを配信し、パケットのポリシー ルーティングを実行します。複数の番号または名前を入力できます。
ステップ 6	**set ip next-hop dynamic dhcp**	DHCP ネットワーク専用。DHCP クライアントが学んだ最新のゲートウェイへのネクスト ホップを設定します。
ステップ 7	**set interface***interface-id*	スタティック ルーティング ネットワーク専用。ポリシー ルーティングのルート マップ一致条件をパスした出力パケットの送信場所を指定します。
ステップ 8	**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 9	**ip local policy route-map***map tag*	ルート マップを特定し、ローカル ポリシー ルーティングに使用します。
ステップ 10	**ip route***prefix mask*{*ip address*|*interface-id*[*ip address*]}[*distance*][*name*][**permanent**|**track***track-number*][*tag tag*]	スタティック ルーティング ネットワーク専用。スタティック ルートを確立します。**track***track-number* を入力し、設定したトラックオブジェクトがアップの場合に限り、静的ルートがインストールされるように指定します。
ステップ 11	**end**	特権 EXEC モードに戻ります。
ステップ 12	**show ip route track table**	IP ルート トラック テーブルの情報を表示します。
ステップ 13	**copy running-config startup-config** 例： デバイス# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

拡張オブジェクト トラッキングのモニタリング

下の表に示す特権EXECコマンドまたはユーザーEXECコマンドを使用して、拡張オブジェクトの追跡情報を表示します。

。

表 *6*：追跡情報を表示するコマンド

コマンド	目的
show ip route track table	IP ルート トラック テーブルの
show track [*object-number*]	すべての追跡リストまたは指定
show track brief	すべてのインターフェイスまた テータスおよび設定を表示しま
show track interface [brief]	追跡対象のインターフェイス ス
show track ip [*object-number*][**brief**]**route**	追跡対象 IP ルート オブジェク
show track resolution	追跡対象パラメータの解像度を
show track timer	追跡対象のポーリング インター

その他の参考資料

MIB

MIB	MIB のリンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
シスコのサポートWebサイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

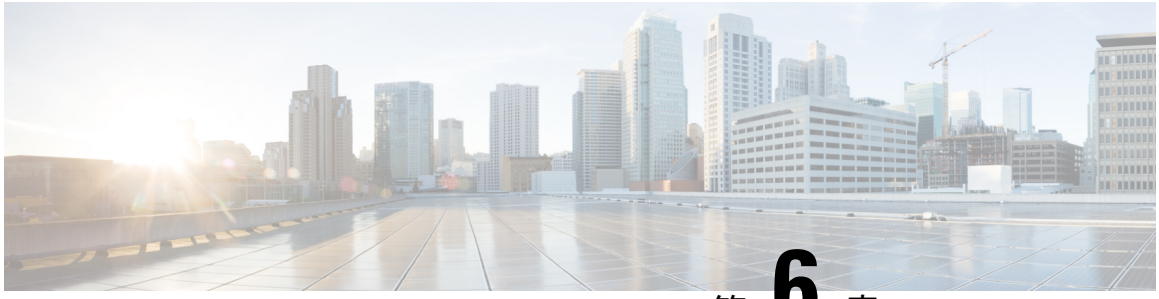
拡張オブジェクト トラッキングの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 7: 拡張オブジェクト トラッキングの機能情報

機能名	リリース	機能情報
拡張オブジェクト トラッキング	Cisco IOS XE Everest 16.6.1	この機能が導入されました。



第 6 章

TCP MSS 調整の設定

TCP MSS 調整の制約事項

- サブインターフェイスは TCP MSS 調整をサポートしません。
- TCP MSS 調整は、レイヤ 3 GRE トンネルでの TCP ストリームの入力パケットキャプチャでのみ機能し、出力パケットキャプチャでは機能しません。

TCP MSS 調整に関する情報

トランスミッション コントロール プロトコル（TCP）最大セグメントサイズ（MSS）調整機能では、ルータを通過する一時的なパケット（特に SYN ビットが設定された TCP セグメント）の最大セグメントサイズを設定することができるようになります。切り捨てを回避するために、SYN パケットの中間ルータで MSS 値を指定するには、インターフェイス コンフィギュレーション モードで ip tcp adjust-mss コマンドを使用します。

ホスト（通常は PC）がサーバーと TCP セッションを開始するときは、TCP SYN パケットの MSS オプション フィールドを使って IP セグメント サイズをネゴシエートします。MSS フィールドの値は、ホスト上の MTU 設定によって決まります。PC のデフォルト MSS 値は 1500 バイトです。

PPP over Ethernet（PPPoE）標準は、1,492 バイトのみの MTU をサポートします。ホストと PPPoE での MTU サイズの不一致は、ホストとサーバーの間にあるルータで 1500 バイトのパケットが損失し、PPPoE を介した TCP セッションが終了する原因となる場合があります。ホ

ストでパスMTU（パス全体で正しいMTUを検出）が有効になっていても、システム管理者がパス MTU を機能させるためにホストからリレーする必要がある ICMP エラーメッセージを無効にすることがあるため、セッションがドロップされることがあります。

ip tcp adjust-mss コマンドで TCP SYN パケットの MSS 値を調整すると、TCP セッション損失防止の役に立ちます。

ip tcp adjust-mss コマンドは、ルータを通過する TCP 接続に対してのみ有効です。

ほとんどの場合、ip tcp adjust-mss コマンドの max-segment-size 引数の最適値は 1,452 バイトです。この値に、20 バイトの IP ヘッダー、20 バイトの TCP ヘッダー、および 8 バイトの PPPoE ヘッダーが追加されて、イーサネット リンクの MTU サイズと同じ 1500 バイトのパケットになります。

サポートされるインターフェイス

TCP MSS 調整は、次のインターフェイスでのみサポートされます。

- 物理層 3 インターフェイス
- SVI
- レイヤ 3 ポートチャネル
- レイヤ 3 GRE トンネル

一時的な TCP SYN パケットの MSS 値の設定

始める前に

ルータを通過する一時的なパケット（特に SYN ビットが設定された TCP セグメント）の MSS を設定するには、この作業を実行します。

ip tcp adjust-mss 1452 コマンドを使用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 tcp adjust-mss** *max-segment-size*
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例：	特権 EXEC モードをイネーブルにします。

	コマンドまたはアクション	目的
	デバイス>**enable**	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： デバイス#**config 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： デバイス(config)#**interface GigabitEthernet 1/0/0**	インターフェイス タイプを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ip tcp adjust-mss** *max-segment-size* 例： デバイス(config-if)#**ip tcp adjust-mss 1452**	ルータを通過する TCP SYN パケットの MSS 値を調整します。 max-segment-size 引数には、MSS をバイト単位で指定します。範囲は 500 ～ 1460 です。
ステップ 5	**end** 例： デバイス(config-if)#**end**	グローバル コンフィギュレーション モードに戻ります。

IPv6 トラフィックの MSS 値の設定

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ipv6 tcp adjust-mss** *max-segment-size*
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： デバイス>**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： デバイス#**config 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	**interface** *type number* 例： `デバイス(config)#interface GigabitEthernet 1/0/0`	インターフェイスタイプを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ipv6 tcp adjust-mss** *max-segment-size* 例： `デバイス(config-if)#ipv6 tcp adjust-mss 1440`	デバイスを通過する TCP DF パケットの MSS 値を調整します。 max-segment-size 引数には、MSS をバイト単位で指定します。指定できる範囲は 40 ～ 1440 です。
ステップ 5	**end** 例： `デバイス(config-if)#end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

例：TCP MSS 調整の設定

```
Device(config)#vpdn enable
Device(config)#no vpdn logging
Device(config)#vpdn-group 1
Device(config-vpdn)#request-dialin
Device(config-vpdn-req-in)#protocol pppoe
Device(config-vpdn-req-in)#exit
Device(config-vpdn)#exit
Device(config)#interface GigabitEthernet 0/0/0
Device(config-if)#ip address 192.168.100.1.255.255.255.0
Device(config-if)#ip tcp adjust-mss 1452
Device(config-if)#ip nat inside
Device(config-if)#exit
```

例：IPv6 トラフィックの TCP MSS 調整の設定

```
Device>enable
Device#configure terminal
Device(config)#interface GigabitEthernet 0/0/0
Device(config)#ipv6 tcp adjust-mss 1440
Device(config)#end
```

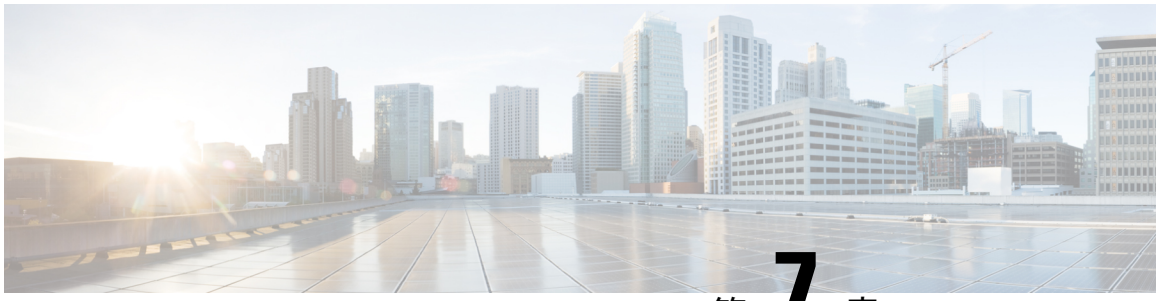
TCP MSS 調整の機能履歴

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能	機能情報
Cisco IOS XE Fuji 16.8.1a	トランスミッション コントロール プロトコル（TCP）最大セグメントサイズ（MSS）調整	TCP MSS 調整機能では、ルータを通過する一時的なパケット（特にSYNビットが設定されたTCPセグメント）の最大セグメントサイズを設定することができるようになります。この機能は、TCP SYNパケットのMSS値を調整することでTCPセッション損失防止の役に立ちます。

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には、http://www.cisco.com/go/cfn [英語] からアクセスします。



第 7 章

IPv6 の拡張ネイバー探索キャッシュ管理

IPv6 の拡張ネイバー探索キャッシュ管理

ネイバー探索プロトコルは、障害のあるノードまたはデバイス、およびリンク層アドレスの変更を検出できるネイバー到達不能検出を実行します。ネイバー到達不能検出プロセスは、ホストからホスト、ホストからデバイス、デバイスからホストへの通信など、ホストとネイバーノード間の全パスの到達可能性情報を保持します。

ネイバーキャッシュは、リンクレイヤアドレスへの IPv6 リンクローカルアドレスまたはグローバルアドレスに関するマッピング情報を保持します。ネイバーキャッシュは、ネイバー到達不能検出プロセスを使用して、ネイバーの到達可能性の状態に関する情報も保持します。ネイバーは、次の 5 つのうちいずれかの状態になります。

- DELAY：ネイバーは再解決を保留中で、このネイバーへのトラフィックフローは制限されています。
- INCOMPLETE：アドレス解決中であり、リンク層アドレスはまだ不明です。
- PROBE：ネイバーの再解決が進行中で、このネイバーへのトラフィックフローが制限されています。
- REACHABLE：最後の到達可能な時間間隔内に近隣ノードが検出されました。
- STALE：ネイバーは、このネイバーへのトラフィックフローを制限して再解決する必要があります。

非送信要求ネイバーアドバタイズメントからエントリを収集するネイバー探索プロトコルを設定するには、**ipv6 nd na glean** コマンドを使用します。

ネットワークの中断時にネイバーのネイバー探索キャッシュエントリを保持するようにネイバー探索プロトコルを設定するには、**ipv6 nd nud retry** コマンドを使用します。

ネイバーへのトラフィックフローがない場合でも、ネイバー探索キャッシュエントリを保持するようにネイバー探索プロトコルを設定するには、**ipv6 nd cache expire refresh** コマンドを使用します。

IPv6 ネイバー探索のパラメータのカスタマイズ

IPv6 ネイバー探索のパラメータをカスタマイズするには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 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： `Device# 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： `Device(config)# interface gigabitethernet 1/1/4`	インターフェイスタイプと ID を指定します。インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ipv6 nd nud retry** *base interval max-attempts* [*final-wait-time*] 例： `Device(config-if)# ipv6 nd nud retry 1 1000 3`	ネイバー到達不能検出でネイバー送信要求を再送信する回数を設定します。
ステップ 5	**ipv6 nd cache expire** *expire-time-in-seconds* [**refresh**] 例： `Device(config-if)# ipv6 nd cache expire 7200`	IPv6 ネイバー探索キャッシュエントリの期限が切れるまでの時間を設定します。
ステップ 6	**ipv6 nd na glean** 例： `Device(config-if)# ipv6 nd na glean`	IPv6 ネイバー探索キャッシュエントリの期限が切れるまでの時間を設定します。
ステップ 7	**end** 例： `Device(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 8	**show ipv6 interface** 例： `Device# show ipv6 interface`	（任意）ネイバー探索キャッシュ管理と IPv6 用に設定されたインターフェイスのユーザビリティのステータスを表示します。

例：IPv6 ネイバー探索のパラメータのカスタマイズ

次の例では、IPv6 ネイバーアドバタイズメントの収集が有効になっており、IPv6 ネイバー探索キャッシュの有効期限は 7200 秒（2 時間）に設定されています。

```
Device> enable
Device# configure terminal
Device(config)# interface Port-channel 189
Device(config-if)# no ip address
Device(config-if)# ipv6 address 2001:BD8::/64
Device(config-if)# ipv6 nd reachable-time 2700000
Device(config-if)# ipv6 nd na glean
Device(config-if)# ipv6 nd cache expire 7200
Device(config-if)# no ipv6 redirects
Device(config-if)# end
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
この章で使用するコマンドの完全な構文および使用方法の詳細。	「*IP* アドレッシングサービス」のセクションを参照 *Command Reference (Catalyst 9300 Series Switches)*
IPv6 ネイバー探索インスペクションの詳細	「セキュリティ」のセクションを参照*Software Configuration Guide (Catalyst 9300 Switches)*

IPv6 ネイバー探索に関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 *8 : IPv6* ネイバー探索に関する機能情報

機能名	リリース	機能情報
IPv6 の拡張ネイバー探索キャッシュ管理	Cisco IOS XE Everest 16.5.1a	ネイバー探索プロトコルは、障害のあるノードまたはルータ、およびリンク層アドレスの変更を検出できるネイバー到達不能検出を実行します。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。