Catalystスイッチネットワークにおける HSRP問題のトラブルシューティング

内容

はじめに

このドキュメントでは、一般的な問題と、ホットスタンバイルータプロトコル(HSRP)の問題のトラブルシューティング方法について説明します。

前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

HSRP について

背景説明

このドキュメントでは、次のような HSRP に関連する最も一般的な問題を取り上げます。

- ルータで重複 HSRP スタンバイ IP アドレスがレポートされる
- HSRP の状態が絶えず変化する（active、standby、speak）
- HSRPピアが存在しない
- HSRP に関連するスイッチのエラー メッセージ
- HSRP 構成への過剰なネットワーク ユニキャストのフラッディング

注：このドキュメントでは、Catalystスイッチ環境でのHSRPのトラブルシューティング方法について詳しく説明しています。このドキュメントには、ソフトウェア バージョンやネットワーク トポロジ設計の参照事項が多数含まれています。しかし、このドキュメントは、専ら、HSRP のトラブルシューティングを行うエンジニアへの手段の提供とガイドを目的としています。このドキュメントは、設計ガイド、ソフトウェア推奨文書、または最適事例文書として意図されたものではありません。

ミッションクリティカルな通信のためにイントラネット サービスおよびインターネット サービスに依存する企業や消費者は、ネットワークとアプリケーションを常時使用できることを求めています。Cisco IOS® ソフトウェアの HSRP を活用すれば、ほぼ 100 % のネットワークアップタイムを実現して、お客様の要求を満たすことができます。HSRP はシスコ プラットフォームに固有のテクノロジーで、これにより、ネットワーク エッジ デバイスやアクセス回線における第 1 ホップでの障害からユーザ トラフィックを即時かつ透過的に復旧させる冗長性が IP ネットワークに提供されます。

IP アドレスと MAC（レイヤ 2（L2））アドレスを共有すれば、複数のルータを 1 つの仮想ルータとして動作させられます。ホスト ワークステーションのデフォルト ゲートウェイの冗長化には、このアドレスが必要です。ほとんどのホスト ワークステーションではルーティング テーブルが保持されておらず、1 つのネクストホップ IP および MAC アドレスだけが使用されます。このアドレスがデフォルト ゲートウェイとして認識されます。HSRP では、仮想ルータ グループのメンバが絶えずステータス メッセージを交換します。いずれかのルータが、予定された理由または予定外の理由で使用不能になった場合は、あるルータが他のルータのルーティングを引き継げます。ホストには 1 つのデフォルト ゲートウェイが設定され、同じ IP および MAC アドレスに IP

パケットが継続的に転送されます。エンド ワークステーションでは、ルーティングを行うデバイスの切り替えは意識されません。

注:Microsoft OSが稼働するホストワークステーションでは、複数のデフォルトゲートウェイを設定できます。ただし、複数のデフォルトゲートウェイは動的ではありません。OS は一度に 1 つのデフォルト ゲートウェイしか使用しません。最初に設定されているデフォルトゲートウェイが Internet Control Management Protocol（ICMP）によって到達不能と判断された場合に、ブート時に予備で設定されているデフォルト ゲートウェイがシステムで選択されるだけです。

基本動作

HSRP を実行する一群のルータが連携して動作し、LAN 上のホストに対してあたかも 1 台のデフォルト ゲートウェイ ルータであるかのような錯覚を与えます。この一群のルータのことを、HSRP グループまたはスタンバイ グループと呼びます。グループから選出された1台のルータが、ホストから仮想ルータに送信されるパケットを転送します。このルータをアクティブ ルータと呼びます。別の 1 台のルータがスタンバイ ルータとして選出されます。アクティブ ルータで障害が発生すると、スタンバイ ルータがパケット転送の役割を担います。HSRPは任意の数のルータで実行できますが、仮想ルータのIPアドレスに送信されたパケットを転送するのはアクティブルータだけです。

ネットワーク トラフィックを最小限に抑えるため、プロトコルによる選出プロセスが完了した後は、アクティブ ルータとスタンバイ ルータだけが、定期的に HSRP メッセージを送信します。HSRP グループ内のそれ以外のルータは Listen 状態のままです。アクティブ ルータで障害が発生すると、スタンバイ ルータがアクティブ ルータの役割を引き継ぎます。スタンバイ ルータで障害が発生するか、またはスタンバイ ルータがアクティブ ルータになると、別のルータがスタンバイルータとして選出されます。

スタンバイ グループはそれぞれ 1 台の仮想ルータ（デフォルト ゲートウェイ）をエミュレートします。グループごとに、周知の MAC および IP アドレスが 1 つ割り当てられます。LAN 上には複数のスタンバイ グループが共存したり、部分的に重複することができ、個々のルータは複数のグループに参加できます。この場合、ルータはグループごとに異なる状態とタイマーを維持します。

HSRP の用語

ターム	定義
アクティブ ルータ	現在、仮想ルータ宛てのパケットを転送しているルータ
スタンバイ ルータ	次に使用されるバックアップ ルータ
スタンバイ グループ	HSRP に参加している一群のルータであり、共同で 1 つの仮想ルータをエミュレートする
Hello タイム	特定のルータから連続した HSRP hello メッセージが送られる間隔
Hold time	hello メッセージを受信してから送信元ルータが故障していると推測するまでの間隔

HSRP アドレッシング

HSRP ルータの通信

HSRP が稼働するルータは、HSRP hello パケットを通じて互いに HSRP 情報をやり取りします。これらのパケットは、User Datagram Protocol（UDP; ユーザ データグラム プロトコル）ポート 1985 の宛先 IP マルチキャスト アドレス 224.0.0.2 に送信されます。IP マルチキャスト アドレス 224.0.0.2 は、すべてのルータと通信を行うための予約済みマルチキャスト アドレスです。アクティブ ルータが、設定されている IP アドレスと HSRP 仮想 MAC アドレスによる hello パケットの送信元となります。スタンバイ ルータは、設定されている IP アドレスとバーンドイン MAC アドレス（BIA）による hello パケットの送信元となります。HSRP ルータが互いを正しく識別するには、この送信元アドレッシングの使用法が必要です。

ほとんどの場合、ルータを HSRP グループの一部として設定する際に、BIA とともにそのグループの HSRP MAC アドレスがルータで受信されます。Cisco 2500、4000、および 4500 ルータに関しては、この動作での唯一の例外となります。これらのルータに搭載されているイーサネット ハードウェアは、1 つの MAC アドレスしか認識しません。したがって、これらのルータではアクティブ ルータとして活動する場合に HSRP MAC アドレスが使用されます。このルータがスタンバイ ルータであるときには BIA が使用されます。

HSRP スタンバイ IP アドレスによる通信（トークン リングを除くすべてのメディア）

ホスト ワークステーションには、デフォルト ゲートウェイとして HSRP スタンバイ IP アドレスが設定されているため、ホストは HSRP スタンバイ IP アドレスに対応付けられた MAC アドレスを使用して通信する必要があります。この MAC アドレスは、0000.0c07.ac** で構成される仮想 MAC アドレスです。ここで ** は、各インターフェイスに基づく 16 進数の HSRP グループ番号です。たとえば、HSRP グループ 1 では、HSRP 仮想 MAC アドレスとして 0000.0c07.ac01 が使用されます。隣接する LAN セグメント上のホストは、通常の Address Resolution Protocol（ARP; アドレス レゾリューション プロトコル）プロセスを使用して、対応する MAC アドレスを解決します。

ICMP リダイレクト

サブネットを保護している HSRP ピア ルータは、ネットワーク内の他のすべてのサブネットへのアクセスを提供できます。これは HSRP の原則です。したがって、どのルータがアクティブ HSRP ルータになるかは関係ありません。Cisco IOS ソフトウェア リリース 12.1(3)T より前の Cisco IOS ソフトウェア リリースでは、あるインターフェイスで HSRP を使用すると、そのインターフェイスでは ICMP リダイレクトが自動的に無効にされます。この設定がないと、ホストが HSRP 仮想 IP アドレスから単一ルータのインターフェイス IP および MAC アドレスへリダイレクトされる可能性があります。つまり、冗長性が失われます。

Cisco IOSソフトウェアでは、HSRPでICMPリダイレクトを許可する方法が導入されています。この方法により、HSRP 経由の発信 ICMP リダイレクト メッセージがフィルタリングされます。ネクスト ホップ IP アドレスが HSRP 仮想アドレスに変更されます。発信 ICMP リダイレクト メッセージ中のゲートウェイ IP アドレスが、そのネットワーク上に存在する HSRP アクティブ ルータのリストと比較されます。ゲートウェイ IP アドレスに対応するルータが HSRP グループの

アクティブ ルータである場合、ゲートウェイ IP アドレスはそのグループの仮想 IP アドレスに置き換えられます。このソリューションにより、ホストがリモート ネットワークへの最適ルートを学習できると同時に、HSRP の提供する障害許容力も維持されます。

HSRP 機能のマトリクス

機能と HSRP をサポートする Cisco IOS ソフトウェア リリースについては、『ホットスタンバイ ルータ プロトコルの特長と機能』の「Cisco IOS のリリースと HSRP 機能のマトリクス」セクションを参照してください。

HSRP の機能

『ホットスタンバイ ルータ プロトコル（HSRP）の特長と機能』に、HSRP のほとんどの機能に関する情報が記載されています。このドキュメントには、次の HSRP 機能に関する情報が含まれています。

- プリエンプション
- インターフェイス トラッキング
- BIA の使用方法
- 複数の HSRP グループ
- 設定可能 MAC アドレス
- Syslog のサポート
- HSRP デバッグ
- 拡張 HSRP デバッグ
- [Authentication]
- IP 冗長性
- SNMP 管理情報ベース（MIB）
- Multiprotocol Label Switching（MPLS; マルチプロトコル ラベル スイッチング）のための HSRP

注：ドキュメント内でこれらのセクションを検索するには、ブラウザの検索機能を使用できます。

パケットのフォーマット

この表は、UDP HSRP フレームのデータ部分のフォーマット示しています。

バージョン	Op コード	都道府県	ハロータイム

ホールドタイム	Priority	Group	Reserved
認証データ			
認証データ			
仮想 IP アドレス			

この表は、HSRP パケットの各フィールドを説明したものです。

パケットのフィールド	説明
Op コード（1 オクテット）	Op コードは、パケットに含まれるメッセージのタイプを示します。可能な値は、0 - hello、1 - coup、および2 - resignです。hello メッセージは、ルータで HSRP を動作していて、アクティブ ルータになる能力があることを示すために送信されます。coup メッセージは、ルータがアクティブ ルータになることを望んでいるときに送信されます。resign メッセージは、ルータがアクティブ ルータであることを放棄したいときに送信されます。
状態（1 オクテット）	スタンバイ グループ内の各ルータには状態マシンが実装されます。状態フィールドには、メッセージを送信するルータの現在の状態が記述されます。個々の状態の詳細は次のとおりです。0 – 初期、1 – 学習、2 – リスニング、4 – スピーク、8 – スタンバイ、16 – アクティブ。
ハロータイム（1 オクテット）	このフィールドは hello メッセージの場合にのみ意味があります。ルータが hello メッセージを送信するおおよその間隔が含まれます。単位は秒です。
ホールドタイム（1 オクテット）	このフィールドは hello メッセージの場合にのみ意味があります。ルータが状態変更を開始する前に hello メッセージを待機する時間の長さが含まれます。
プライオリティ（1 オクテット）	このフィールドはアクティブ ルータとスタンバイ ルータの選出に使用されます。2 台のルータのプライオリティを比較して、大きい値を持つルータがアクティブ ルータになります。プライオリティが同じ場合は、より大きい IP アドレスを持つルータが選出されます。
グループ（1 オクテット）	このフィールドによってスタンバイ グループが識別されます。
認証データ（8 オクテット）	このフィールドには、8 文字のクリア テキスト パスワードが含まれます。
仮想 IP アドレス（4 オクテット）	ルータに仮想 IP アドレスが設定されていない場合は、アクティブ ルータからの hello メッセージからアドレスを学習できます。アドレスが学習されるのは、HSRP スタンバイ IP アドレスが設定されておらず、なおかつ hello メッセージが認証される場合だけです（認証が設定されている場合）。

HSRP 状態

都道府県	定義
Initial	これは最初の状態です。この状態は、HSRP が動作していないことを示します。設定が変更された場合、またはインターフェイスが最初に起動したときにこの状態になります。
Learn	ルータではまだ仮想 IP アドレスが判別されておらず、アクティブ ルータからの認証済み hello パケットも受信されていません。この状態では、ルータはアクティブ ルータからパケットが到達するのを待ち続けます。
Listen	ルータは仮想 IP アドレスを認識していますが、ルータはアクティブ ルータでもスタンバイ ルータでもありません。アクティブ ルータまたはスタンバイ ルータからの hello メッセージをリスニングしています。
Speak	ルータは定期的に hello メッセージを送信し、アクティブ ルータまたはスタンバイ ルータの選出に積極的に参加します。ルータは、仮想 IP アドレスがないと、speak 状態になることはできません。
スタンバイ	ルータは次のアクティブ ルータになる可能性があるため、定期的に hello メッセージを送信している。過渡的な状態を除き、グループ内で最大 1 台のルータが standby 状態になります。
アクティブ	現在、ルータはグループの仮想 MAC アドレスに送信されたパケットを転送している。ルータは、定期的に hello メッセージを送信する。過渡的な状態を除き、グループ内で active 状態のルータは最大 1 台である必要があります。

HSRP タイマー

各ルータは HSRP で 3 つのタイマーのみを使用します。タイマーは、hello メッセージの時間を計ります。障害発生時の HSRP コンバージは、HSRP の hello タイマーと hold タイマーがどのように設定されているかによります。デフォルトでは、これらのタイマーはそれぞれ 3 秒と 10 秒に設定されており、hello パケットは HSRP スタンバイ グループのデバイス間を 3 秒ごとに送信され、スタンバイ デバイスでは、hello パケットが 10 秒間受信されないとアクティブになります。これらのタイマー設定を下げると、フェールオーバーやプリエンプションの速度は上がりますが、CPU使用率の増加と不必要なスタンバイ状態のフラッピングを避けるため、helloタイマーを1秒未満に、またはholdタイマーを4秒未満には設定しないでください。HSRP トラッキング メカニズムを使用していて、トラッキング対象のリンクで障害が発生したら、hello タイマーと hold タイマーの状態にかかわらず、即座にフェールオーバーかプリエンプションが実行される点に注意してください。タイマーが時間切れになると、ルータは、新しい HSRP ステートに移行します。これらのタイマーは、standby [group-number] timers hellotime holdtimeコマンドで変更できます。たとえば、standby 1 timers 5 15 のように指定します。

この表は、これらのタイマーの詳細を示したものです。

タイマー	説明
Active timer	このタイマーは、アクティブ ルータを監視するために使用されます。アクティブ ルータが hello パケットを受信すると、常にこのタイマーが起動します。このタイマーは、HSRP hello メッセージの対応するフィールドに設定されいるホールド タイム値が経過すると時間切れになります。
Standby timer	このタイマーは、スタンバイ ルータを監視するために使用されます。スタンバイ ルータが hello パケットを受信すると、常にこのタイマーが起動します。このタイマーは、各 hello パケットに設定さているホールド タイム値が経過すると時間切れになり

	ます。
ハロー タイマー	このタイマーは、hello パケットのタイミングを計るために使用されます。いずれかの HSRP 状態にあるすべての HSRP ルータでは、このハロー タイマーが時間切れになると hello パケットが生成されます。

HSRP イベント

この表は、HSRP 有限状態マシンでのイベントを示したものです。

キー	イベント
1	有効なインターフェイスで HSRP が設定された。
2	インターフェイスで HSRP が無効になったか、またはインターフェイスが無効になった。
3	アクティブ タイマーの時間切れ。アクティブ タイマーは、アクティブ ルータから最後の hello メッセージが到達する際にホールド タイムに設定されている。
4	スタンバイ タイマーの時間切れ。スタンバイ タイマーは、スタンバイ ルータから最後の hello メッセージが到達する際にホールド タイムに設定されている。
5	Hello タイマーの時間切れ。hello メッセージ送信用の定期タイマーが時間切れになった。
6	speak 状態のルータからプライオリティの高い hello メッセージが受信された
7	アクティブ ルータからプライオリティの高い hello メッセージが受信された
8	アクティブ ルータからプライオリティの低い hello メッセージが受信された
9	アクティブ ルータから resign メッセージが受信された
10	プライオリティの高いルータから coup メッセージが受信された
11	スタンバイ ルータからプライオリティの高い hello メッセージが受信された
12	スタンバイ ルータからプライオリティの低い hello メッセージが受信された

HSRP アクション

この表は、状態マシンの一部として実行されるアクションを示しています。

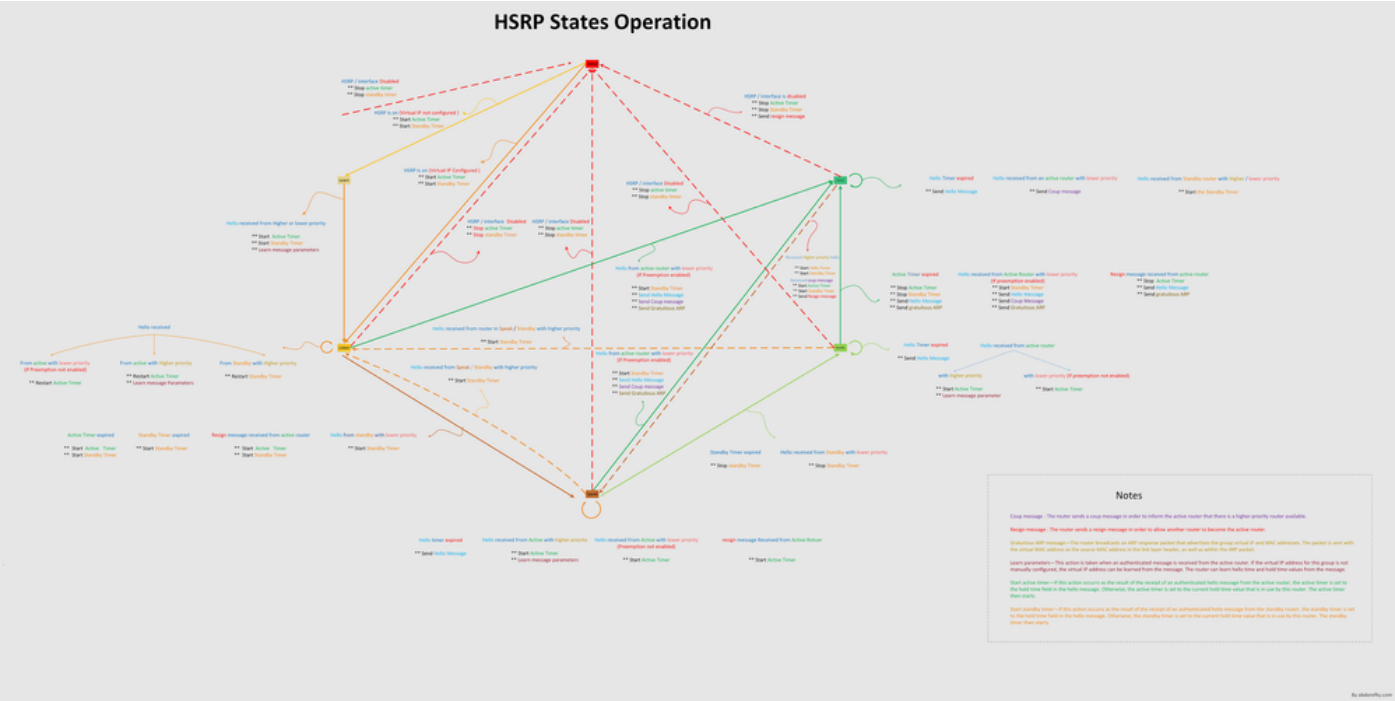
文字	アクション
A	アクティブタイマーの起動：アクティブルータからの認証済みhelloメッセージが受信された結果、このアクションが起こった場合、helloメッセージのホールドタイムフィールドの値がアクティブタイマーに設定されます。それ以外の場合、このルータで使用されている現在のホールド タイム値がアクティブ タイマーに設定されます。続いてアクティブ タイマーが起動します。
B	スタンバイタイマーの起動：スタンバイルータからの認証済みhelloメッセージが受信された結果、このアクションが起こった場合、helloメッセージのホールドタイムフィールドの値がスタンバイタイマーに設定されます。それ以外の場合、このルータで使用されている現在のホールド タイム値がスタンバイ タイマーに設定されます。続いてスタンバイ タイマーが起動します。
C	アクティブ タイマーの停止：アクティブ タイマーが停止します。
D	スタンバイ タイマーの停止：スタンバイ タイマーが停止します。
E	パラメータの学習：このアクションは、アクティブ ルータから認証済みメッセージが受信さ

	れたときに実行されます。このグループの仮想 IP アドレスが手動で設定されていない場合は、メッセージから仮想 IP アドレスを学習できます。ルータは、メッセージからハロー タイムとホールド タイムの値を学習できます。
F	hello メッセージの送信：ルータは、自身の現在の状態、hello タイム、およびホールド タイムを含む hello メッセージを送信します。
G	coup メッセージの送信：ルータは、プライオリティのより高いルータが使用可能であることをアクティブ ルータに通知するために、coup メッセージを送信します。
H	resign メッセージの送信：ルータは、別のルータがアクティブ ルータになれるようにするために、resign メッセージを送信します。
I	gratuitous ARP メッセージの送信：ルータは、グループの仮想 IP アドレスと MAC アドレスをアドバタイズする ARP 応答パケットをブロードキャストします。このパケットの送信時には、リンク層ヘッダーと ARP パケット内部の送信元 MAC アドレスとして仮想 MAC アドレスが使用されます。

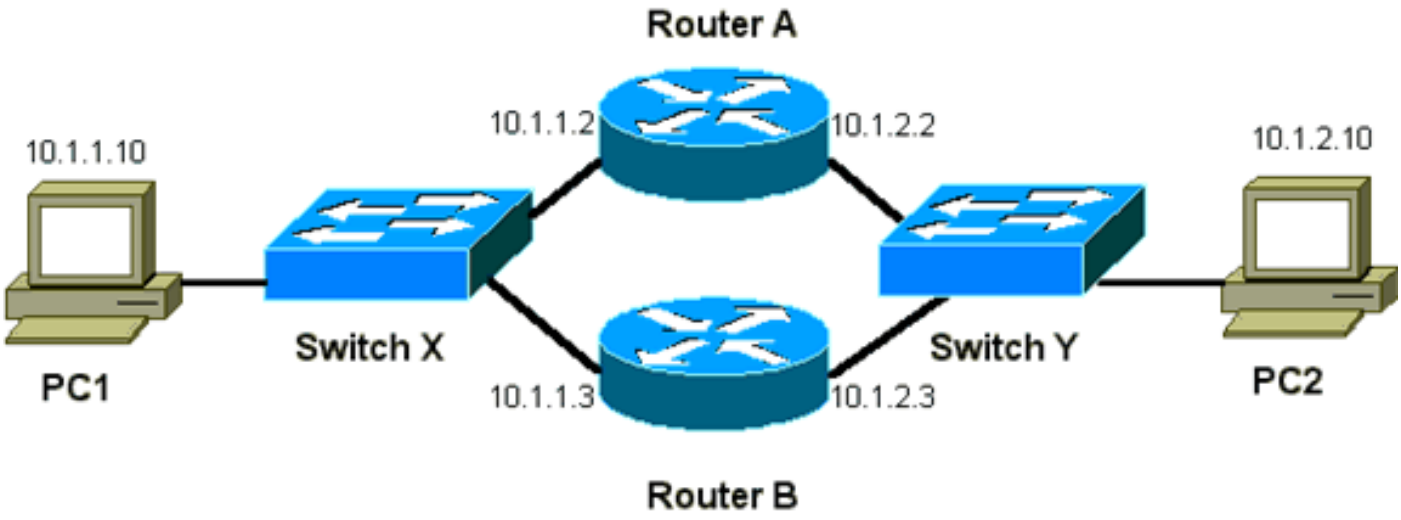
HSRP 状態テーブル

このセクションの図は、HSRP 状態マシンの状態遷移を示しています。イベントが起こるたびに対応するアクションが実行され、ルータが次の HSRP 状態に移行します。図中では番号がイベントを示し、文字が対応するアクションを示します。「HSRP イベント」セクションに番号の定義を示す表があります。また、「HSRP アクション」セクションに文字の定義を示す表があります。この図は参照用としてだけに使用してください。この図は詳細な説明であり、一般的なトラブルシューティングには必要ありません。

図の高解像度画像については、「HSRP 状態 の 動作」を参照してください。



パケット フロー



デバイス	MAC アドレス	IP アドレス	サブネット マスク	[Default Gateway]
PC1	0000.0c00.0001	10.1.1.10	255.255.255.0	10.1.1.1
PC2	0000.0c00.1110	10.1.2.10	255.255.255.0	10.1.2.1

ルータ A の設定 (アクティブ ルータ)

```
interface GigabitEthernet 0/0
 ip address 10.1.1.2 255.255.255.0
 mac-address 4000.0000.0010
 standby 1 ip 10.1.1.1
 standby 1 priority 200

interface GigabitEthernet 0/1
 ip address 10.1.2.2 255.255.255.0
 mac-address 4000.0000.0011
 standby 1 ip 10.1.2.1
 standby 1 priority 200
```

ルータ B の設定 (スタンバイ ルータ)

```
interface GigabitEthernet 0/0
    ip address 10.1.1.3 255.255.225.0
    mac-address 4000.0000.0020
    standby 1 ip 10.1.1.1

interface GigabitEthernet 0/1
     ip address 10.1.2.3 255.255.255.0
     mac-address 4000.0000.0021
     standby 1 ip 10.1.2.1
```

注：これらの例では、説明の目的でのみスタティックMACアドレスを設定しています。必要ない限り、スタティック MAC アドレスは設定しないでください。

HSRP問題のトラブルシューティングを行うためにスニファトレースを取得するときは、パケットフローの背後にある概念を理解する必要があります。ルータ A にはプライオリティ 200 が設定されているため、両方のインターフェイスでアクティブ ルータになります。このセクションの例では、ルータからホスト ワークステーション宛てに送信されるパケットには、送信元 MAC アドレスとしてルータの物理 MAC アドレス (BIA) が含まれます。ホスト マシンから HSRP IP アドレス宛てに送信されるパケットには、宛先 MAC アドレスとして HSRP 仮想 MAC アドレスが含まれます。ルータとホスト間の各フローで MAC アドレスが異なる点に注意が必要です。

この表は、フローごとの各 MAC アドレスと IP アドレスの情報を示しています。この情報は、スイッチ X で取得されるスニファ トレースに基づいています。

パケット フロー	送信元 MAC	宛先 MAC	送信元 IP	宛先 IP
PC1 から PC2 宛てのパケット	PC1 (0000.0c00.0001)	ルータ A のインターフェイス Ethernet 0 の HSRP 仮想 MAC アドレス (0000.0c07.ac01)	10.1.1.10	10.1.2.10
ルータ A を経由して戻ってくる、PC2 から PC1 宛てのパケット	ルータ A の Ethernet 0 の BIA (4000.0000.0010)	PC1 (0000.0c00.0001)	10.1.2.10	10.1.1.10
PC1 から HSRP スタンバイ IP アドレス宛てのパケット (ICMP、Telnet)	PC1 (0000.0c00.0001)	ルータ A のインターフェイス Ethernet 0 の HSRP 仮想 MAC アドレス (0000.0c07.ac01)	10.1.1.10	10.1.1.1
アクティブ ルータの実際の IP アドレス宛てのパケット (ICMP、Telnet)	PC1 (0000.0c00.0001)	ルータ A の Ethernet 0 の BIA (4000.0000.0010)	10.1.1.10	10.1.1.2
スタンバイ ルータの実際の IP アドレス宛てのパケット (ICMP、Telnet)	PC1 (0000.0c00.0001)	ルータ B の Ethernet 0 の BIA (4000.0000.0020)	10.1.1.10	10.1.1.3

HSRP のトラブルシューティング事例

ケーススタディ#1:HSRPスタンバイIPアドレスが重複IPアドレスとしてレポートされる

次のエラー メッセージが表示される可能性があります。

```
Oct 12 13:15:41: %STANDBY-3-DUPADDR: Duplicate address 10.25.0.1
  on Vlan25, sourced by 0000.0c07.ac19
Oct 13 16:25:41: %STANDBY-3-DUPADDR: Duplicate address 10.25.0.1
  on Vlan25, sourced by 0000.0c07.ac19
Oct 15 22:31:02: %STANDBY-3-DUPADDR: Duplicate address 10.25.0.1
  on Vlan25, sourced by 0000.0c07.ac19
Oct 15 22:41:01: %STANDBY-3-DUPADDR: Duplicate address 10.25.0.1
  on Vlan25, sourced by 0000.0c07.ac19
```

これらのエラー メッセージは、必ずしも HSRP の問題を示しているわけではありません。むしろ、これらのエラー メッセージは、Spanning-Tree Protocol（STP; スパンニング ツリー プロトコル）ループが発生しているか、またはルータ/スイッチに設定の問題がある可能性を示しています。エラー メッセージは別の問題の症状に過ぎません。

また、これらのエラー メッセージが発生しても、HSRP の通常の動作が妨げられることはありません。重複した HSRP パケットは無視されます。これらのエラー メッセージの発生頻度は 30 秒間隔に抑えられています。ただし、HSRP アドレスの `STANDBY-3-DUPADDR` エラー メッセージが原因でネットワークが不安定になり、結果的にネットワークのパフォーマンスが低下したり、パケット損失が発生したりする可能性があります。

これらのメッセージを見ると、VLAN 25 の HSRP IP アドレス（MAC アドレス 0000.0c07.ac19）を発信元とするデータ パケットがルータで受信されていることがわかります。HSRP MAC アドレスが 0000.0c07.ac19 であるため、問題のルータが自身のパケットを受信したか、または HSRP グループ内の両方のルータが `active` 状態になっています。ルータは自身のパケットを受信しているため、おそらくルータではなくネットワークに問題があります。この動作の原因にはさまざまな問題が考えられます。エラー メッセージの原因と考えられるネットワークの問題には次のものがあります。

- 瞬間的な STP ループ
- EtherChannel の設定の問題
- フレームの重複

これらのエラーメッセージのトラブルシューティングを行う際には、このドキュメントの「CatalystスイッチのHSRPのトラブルシューティング」セクションでトラブルシューティング手順を参照してください。このセクションには、設定に関するモジュールを含め、すべてのトラブルシューティングモジュールを適用できます。また、スイッチ ログに記録されたエラーに注意し、必要に応じて他の事例も参照してください。

アクティブ ルータが自身のマルチキャスト hello パケットを受信しないようにするため、アクセス リストを使用できます。ただし、これはエラー メッセージの回避策にすぎず、実際には問題の症状を隠すものです。この回避策は、HSRP インターフェイスに拡張着信アクセス リストを適用するものです。アクセス リストは、物理 IP アドレスから発信され全ルータ用のマルチキャスト アドレス 224.0.0.2 へ送信されるすべてのトラフィックを遮断します。

```
access-list 101 deny ip host 172.16.12.3 host 224.0.0.2
```

```
access-list 101 permit ip any any

interface GigabitEthernet 0/0
 ip address 172.16.12.3 255.255.255.0
 standby 1 ip 172.16.12.1
 ip access-group 101 in
```

ケーススタディ#2:HSRP状態が継続的に変化する（アクティブ、スタンバイ、スピーク）か、%HSRP-6-STATECHANGE

次のエラー メッセージが表示される可能性があります。

```
Jan 9 08:00:42.623: %STANDBY-6-STATECHANGE: Standby: 49:
  Vlan149 state Standby -> Active
Jan 9 08:00:56.011: %STANDBY-6-STATECHANGE: Standby: 49:
  Vlan149 state Active -> Speak
Jan 9 08:01:03.011: %STANDBY-6-STATECHANGE: Standby: 49:
  Vlan149 state Speak -> Standby
Jan 9 08:01:29.427: %STANDBY-6-STATECHANGE: Standby: 49:
  Vlan149 state Standby -> Active
Jan 9 08:01:36.808: %STANDBY-6-STATECHANGE: Standby: 49:
  Vlan149 state Active -> Speak
Jan 9 08:01:43.808: %STANDBY-6-STATECHANGE: Standby: 49:
  Vlan149 state Speak -> Standby
```

```
Jul 29 14:03:19.441: %HSRP-5-STATECHANGE: Vlan10 Grp 110 state Standby -> Active
Jul 29 16:27:04.133: %HSRP-5-STATECHANGE: Vlan10 Grp 110 state Active -> Speak
Jul 29 16:31:49.035: %HSRP-5-STATECHANGE: Vlan10 Grp 110 state Speak -> Standby
```

これらのエラー メッセージは、スタンバイ HSRP ルータで HSRP ピアからの HSRP hello パケットが 3 回連続して受信されなかった状態を示します。出力は、スタンバイ ルータが `standby` 状態から `active` 状態に移行し、そのすぐ後に、`standby` 状態に戻ったことを示しています。初期インストール時に発生する場合を除き、HSRP 問題がこのエラー メッセージの原因になることはおそらくありません。このエラー メッセージはピア間で HSRP hello パケットが失われていることを示しています。この問題のトラブルシューティングを行う際は、HSRP ピア間の通信を確認する必要があります。これらのメッセージを引き起こす最も一般的な問題は、ピア間のデータ通信におけるランダムで瞬間的な損失です。HSRP 状態の変化は、高 CPU 使用率によるものであることがよくあります。エラー メッセージが高 CPU 使用率によるものである場合は、ネットワークにスニファを置いて、高 CPU 使用率の原因となっているシステムをトレースします。

ピア間で HSRP パケットが失われる原因にはさまざまなものがあります。最も一般的な問題は、物理層の問題、スパニング ツリーの問題による過剰なネットワーク トラフィック、または各 VLAN による過剰なトラフィックです。事例1と同様に、HSRP状態の変化を解決するためすべてのトラブルシューティングモジュールを適用できますが、特にレイヤ3 HSRPデバッグが有効です。

ピア間での HSRP パケット損失が、前述の各 VLAN による過剰なトラフィックが原因である場合は、Selective Packet Discard（SPD; 選択的パケット廃棄）と保留キューのサイズを調整するか増やして、入力キューの廃棄の問題を解決できます。

Selective Packet Discard（SPD；選択パケット廃棄）のサイズを大きくするには、コンフィギュレーションモードに移行して、Cat6500スイッチで次のコマンドを実行します。

```
(config)#ip spd queue max-threshold 600

!--- Hidden Command

(config)#ip spd queue min-threshold 500

!--- Hidden Command
```

保留キューのサイズを増やすには、VLAN インターフェイスモードに入り、次のコマンドを実行します。

```
(config-if)#hold-queue 500 in
```

SPDと保留キューのサイズを増やした後、**clear counter interface**コマンドを実行するとインターフェイスカウンタをクリアできます。

ケーススタディ#3:HSRPでピアが認識されない

このセクションのルータ出力には、ルータで HSRP が設定されているにもかかわらず、HSRP ピアが認識されていないことが示されています。これが発生している場合、ルータでは隣接ルータからの HSRP hello の受信が失敗します。この問題のトラブルシューティングを行う際は、このドキュメントの「物理層の接続性の確認」セクションおよび「HSRP ルータ設定の確認」セクションを参照してください。物理層の接続に問題がない場合は、VTP モードのミスマッチを調べます。

```
Vlan8 - Group 8
Local state is Active, priority 110, may preempt
Hellotime 3 holdtime 10
Next hello sent in 00:00:01.168
Hot standby IP address is 10.1.2.2 configured
Active router is local
Standby router is unknown expired
Standby virtual mac address is 0000.0c07.ac08
5 state changes, last state change 00:05:03
```

ケーススタディ#4:HSRP状態が変化し、スイッチのsyslogにSYS-4-P2_WARN: 1/Host <mac_address> Is Flapping Between Port <port_1> and Port <port_2>がレポートされる

次のエラー メッセージが表示される可能性があります。

```
2001 Jan 03 14:18:43 %SYS-4-P2_WARN: 1/Host 00:00:0c:14:9d:08
  is flapping between port 2/4 and port 2/3
```

Feb 4 07:17:44 AST: %SW_MATM-4-MACFLAP_NOTIF: Host 0050.56a9.1f28 in vlan 1027 is flapping between port Te1/0/7 and port Te2/0/2

Catalystスイッチでは、ホストのMACアドレスが15秒以内に2回移動すると、スイッチからホストのMACアドレスの移動が報告されます。原因としては、STPループが考えられます。スイッチは、STP ループの影響を最小限に抑えるため、このホストからのパケットをおよそ 15 秒間廃棄します。2 つのポートの間で移動しているとレポートされている MAC アドレスが HSRP 仮想 MAC アドレスの場合、この問題はおそらく両方の HSRP ルータが active 状態になる問題です。

レポートされている MAC アドレスが HSRP 仮想 MAC アドレスでない場合、この問題はネットワーク内でのループ、重複、またはパケットのリフレクションを示している可能性があります。この種の状況が、HSRP 問題の原因となる可能性があります。MAC アドレスの移動を引き起こす最も一般的な原因は、スパニング ツリーの問題または物理層の問題です。

このエラー メッセージのトラブルシューティングを行うには、次の手順を行います。

注：このドキュメントの「CatalystスイッチのHSRPのトラブルシューティング」セクションにある手順も実施してください。

---

1. ホスト MAC アドレスの正確な発信元（ポート）を特定します。
2. ホストのMACアドレスの発信元にはなれないポートの接続を解除します。
3. VLAN ごとに STP トポロジを明確にして、STP 障害がないかをチェックします。
4. ポート チャネリング設定を確認します。
    1. ポート チャネル設定が誤っていると、ホスト MAC アドレスによるエラー メッセージのフラップが発生することがあります。これは、ポート チャネリングのロード バランシング特性が原因です。

ケーススタディ#5：非対称ルーティングとHSRP（HSRPを実行するルータを使用したネットワークでのユニキャストトラフィックの過剰なフラッディング）

非対称ルーティングでは、送信パケットと受信パケットは、ホストと通信相手のピア間で異なるパスを使用します。このパケットフローは、HSRPプライオリティに基づいてHSRPルータ間にロードバランシングを設定し、HSRPをアクティブまたはスタンバイに設定した結果です。スイッチング環境でこの種のパケット フローにより、不明なユニキャストのフラッディングが過剰に発生する場合があります。また、Multilayer Switching（MLS; マルチレイヤ スイッチング）エントリが欠落する場合もあります。不明なユニキャストのフラッディングは、スイッチがすべてのポートからユニキャスト パケットをフラッディングした場合に起こります。スイッチは、宛先 MAC アドレスのエントリがないためにパケットをフラッディングします。それでもパケットは転送されるため、この動作によって接続が断絶することはありません。しかし、この動作によってホスト ポートによけいなパケットがフラッディングされます。この事例では、非対称ルーティングの動作と、ユニキャスト フラッディングが起こる理由について検討します。

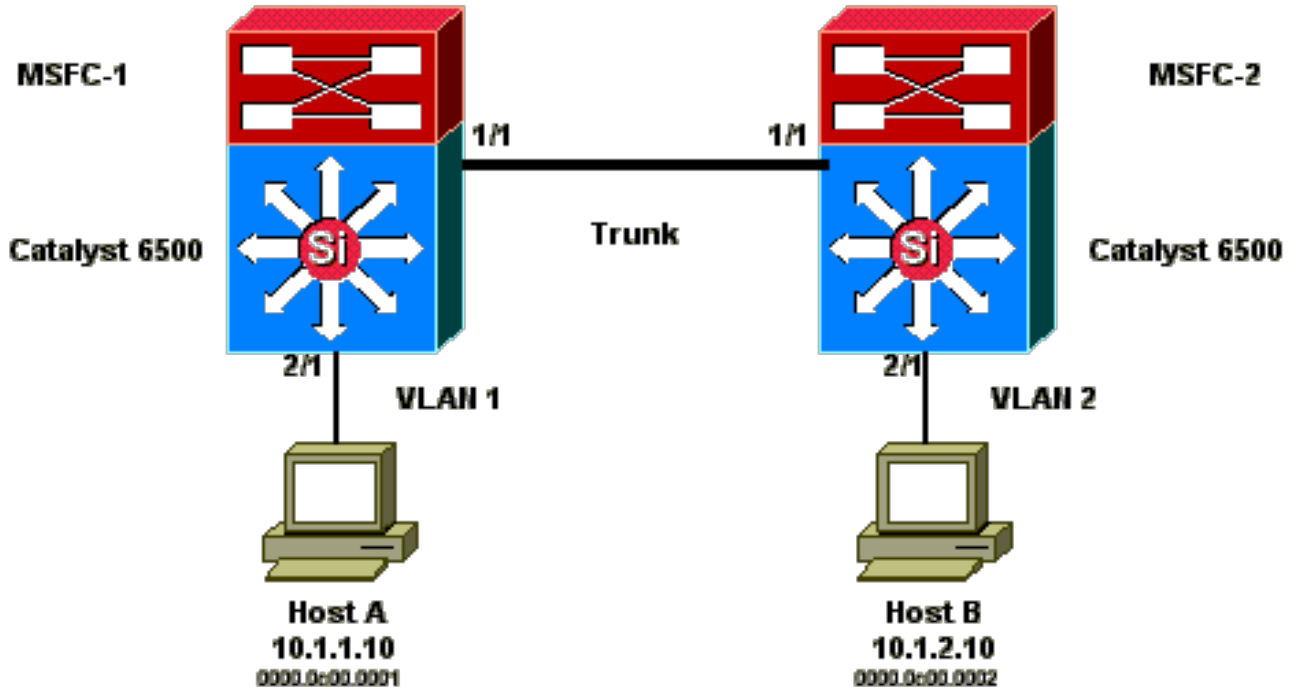
非対称ルーティングの症状には次のものがあります。

- ユニキャスト パケットの過剰なフラッディング
- フローで使用される MLS エントリの欠落
- ホスト ポート上のパケットがホスト宛てでないことを示すスニファ トレース
- サーバ ロード バランサ、Web キャッシュ デバイス、ネットワーク アプライアンスなど、L2 ベースのパケット リライト エンジンを使用した場合の、ネットワーク遅延の増加

  （例：Cisco LocalDirector、Cisco Cache Engine）
- ユニキャスト フラッディング トラフィックの負荷の増加を処理できない接続先ホストおよびワークステーションでの、パケットの廃棄

注：ルータでのARPキャッシュのデフォルトのエージングタイムは4時間です。スイッチの content-addressable memory（CAM; 連想メモリ）エントリのデフォルトのエージング タイムは 5 分です。ここでは、ホスト ワークステーションの ARP のエージング タイムは重要ではありませんが、例では ARP のエージング タイムは 4 時間に設定されています。

次の図に、この問題を示します。このトポロジ例のスイッチはどちらも、Multilayer Switch Feature Card（MSFC; マルチレイヤ スイッチ フィーチャ カード）を搭載した Catalyst 6500 です。この例では MSFC を使用していますが、MSFC の代わりに任意のルータを使用することもできます。たとえば、使用できるルータには Route Switch Module（RSM; ルート スイッチ モジュール）、Gigabit Switch Router（GSR; ギガビット スイッチ ルータ）、および Cisco 7500 があります。ホストはスイッチのポートに直接接続されています。スイッチは、VLAN 1 と VLAN 2 のトラフィックを伝送するトランクを通じて相互接続されています。



この出力は、各 MSF の show standby コマンド コンフィギュレーションから抜粋したものです。

MSFC1

```
interface Vlan 1
 mac-address 0003.6bf1.2a01
 ip address 10.1.1.2 255.255.255.0
 no ip redirects
 standby 1 ip 10.1.1.1
 standby 1 priority 110

interface Vlan 2
 mac-address 0003.6bf1.2a01
 ip address 10.1.2.2 255.255.255.0
 no ip redirects
 standby 2 ip 10.1.2.1

MSFC1#show standby
Vlan1 - Group 1
Local state is Active, priority 110
Hellotime 3 holdtime 10
Next hello sent in 00:00:00.696
Hot standby IP address is 10.1.1.1 configured
Active router is local
Standby router is 10.1.1.3 expires in 00:00:07
Standby virtual mac address is 0000.0c07.ac01
2 state changes, last state change 00:20:40
Vlan2 - Group 2
Local state is Standby, priority 100
Hellotime 3 holdtime 10
Next hello sent in 00:00:00.776
Hot standby IP address is 10.1.2.1 configured
Active router is 10.1.2.3 expires in 00:00:09, priority 110
Standby router is local
```

```
4 state changes, last state change 00:00:51
MSFC1#exit
Console> (enable)
```

MSFC2

```
interface Vlan 1
 mac-address 0003.6bf1.2a02
 ip address 10.1.1.3 255.255.255.0
 no ip redirects
 standby 1 ip 10.1.1.1

interface Vlan 2
 mac-address 0003.6bf1.2a02
 ip address 10.1.2.3 255.255.255.0
 no ip redirects
 standby 2 ip 10.1.2.1
 standby 2 priority 110

MSFC2#show standby
Vlan1 - Group 1
Local state is Standby, priority 100
Hellotime 3 holdtime 10
Next hello sent in 00:00:01.242
Hot standby IP address is 10.1.1.1 configured
Active router is 10.1.1.2 expires in 00:00:09, priority 110
Standby router is local
7 state changes, last state change 00:01:17
Vlan2 - Group 2
Local state is Active, priority 110
Hellotime 3 holdtime 10
Next hello sent in 00:00:00.924
Hot standby IP address is 10.1.2.1 configured
Active router is local
Standby router is 10.1.2.2 expires in 00:00:09
Standby virtual mac address is 0000.0c07.ac02
2 state changes, last state change 00:40:08
MSFC2#exit
```

注:MSFC1では、VLAN 1はHSRP active状態で、VLAN 2はHSRP standby状態です。MSFC2では、VLAN 2 は HSRP active 状態で、VLAN 1 は HSRP standby 状態です。各ホストのデフォルト ゲートウェイはそれぞれのスタンバイ IP アドレスです。

---

1. 最初はどのキャッシュにも何も入っていません。ホスト A はデフォルト ゲートウェイとして MSFC1 を使用します。ホスト B は MSFC2 を使用します。

   ARP および MAC アドレス テーブル：ping を発行する前

ホスト A の ARP テーブル	スイッチ 1 の MAC アドレス テーブル MAC VLAN ポート	MSFC1 ARP テーブル	MSFC2 ARP テーブル	スイッチ 2 の MAC アドレス テーブル MAC VLAN ポート	ホスト B の ARP テーブル

	0003.6bf1.2a01 1 15/1			0003.6bf1.2a02 1 15/1	
	0003.6bf1.2a01 2 15/1			0003.6bf1.2a02 2 15/1	
	0000.0c07.ac01 1 15/1			0000.0c07.ac01 1 1/1	
	0000.0c07.ac02 2 1/1			0000.0c07.ac02 2 15/1	
	0003.6bf1.2a02 1 1/1			0003.6bf1.2a01 1 1/1	
	0003.6bf1.2a02 2 1/1			0003.6bf1.2a01 2 1/1	

注：簡略化するため、スイッチ1のルータHSRP用MACアドレスとMACアドレスは、このセクションに記載されている他の表には含まれていません。

2. ホスト A はホスト B に ping を行います。つまりホスト A は ICMP エコー パケットを送信します。ホストはそれぞれ別の VLAN にあるため、ホスト A はホスト B 宛てのパケットをデフォルト ゲートウェイに転送します。このプロセスが行われるためには、ホスト A はデフォルト ゲートウェイの MAC アドレス、10.1.1.1 を解決するため ARP を送信する必要があります。

   ARP および MAC アドレス テーブル：ホスト A がデフォルト ゲートウェイに ARP を送信した後

ホスト A の ARP テーブル	スイッチ 1 の MAC アドレス テーブル MAC VLAN ポート	MSFC1 ARP テーブル	MSFC2 ARP テーブル	スイッチ 2 の MAC アドレス テーブル MAC VLAN ポート	ホスト B の ARP テーブル
10.1.1.1 : 0000.0c07.ac01	0000.0c00.0001 1 2/1	10.1.1.10 : 0000.0c00.0001			

3. MSFC1はパケットを受信し、パケットを書き換えて、ホストBに転送します。パケットを書き換えるために、MSFC1はホストBに対するARP要求を送信します。これは、ホストBが、直接接続されたインターフェイス上にないためです。このフローで、MSFC2 はまだパケットを 1 つも受信していません。MSFC1 がホスト B からの ARP 応答を受信すると、どちらのスイッチもホスト B に関連づけられているソース ポートを学習します。

   ARP および MAC アドレス テーブル：ホスト A がデフォルト ゲートウェイにパケットを送信し、MSFC1 がホスト B に対する ARP を送信した後

ホスト A の ARP テーブル	スイッチ 1 の MAC アドレス テーブル MAC VLAN ポート	MSFC1 ARP テーブル	MSFC2 ARP テーブル	スイッチ 2 の MAC アドレス テーブル MAC VLAN ポート	ホスト B の ARP テーブル
10.1.1.1 : 0000.0c07.ac01	0000.0c00.0001 1 2/1	10.1.1.10 : 0000.0c00.0001		0000.0c00.0002 2 2/1	10.1.2.2 : 0003.6bf1.2a0
	0000.0c00.0002 2 1/1	10.1.2.10:0000.0c00.0002			

4. ホスト B は、MSFC1 を通じてホスト A からのエコー パケットを受信します。ホスト B はホスト A に対してエコー応答を送信する必要があります。ホスト A は異なる VLAN 上に存

在するため、ホスト B はデフォルト ゲートウェイ MSFC2 を通じて応答を転送します。MSFC2 を通じてパケットを転送するために、ホスト B はデフォルト ゲートウェイの IP アドレス、10.1.2.1 の ARP を送信する必要があります。

ARP および MAC アドレス テーブル：ホスト B がそのデフォルト ゲートウェイに ARP を送信した後

ホスト A の ARP テーブル	スイッチ 1 の MAC アドレス テーブル MAC VLAN ポート	MSFC1 ARP テーブル	MSFC2 ARP テーブル	スイッチ 2 の MAC アドレス テーブル MAC VLAN ポート	ホス
10.1.1.1 : 0000.0c07.ac01	0000.0c00.0001 1 2/1	10.1.1.10 : 0000.0c00.0001	10.1.2.10 0000.0c00.0002	0000.0c00.0002 2 2/1	10.1.2
	0000.0c00.0002 2 1/1	10.1.2.10:0000.0c00.0001			10.1.2

5. ホスト B はここで MSFC2 にエコー応答パケットを転送します。MSFC2 は、ホスト A が VLAN 1 に直接接続されているため、ホスト A に対する ARP 要求を送信します。スイッチ 2 の MAC アドレス テーブルには、ホスト B の MAC アドレスが格納されます。

ARP および MAC アドレス テーブル：ホスト A でエコー パケットが受信された後

ホスト A の ARP テーブル	スイッチ 1 の MAC アドレス テーブル MAC VLAN ポート	MSFC1 ARP テーブル	MSFC2 ARP テーブル	スイッチ 2 の MAC アドレス テーブル MAC VLAN ポート	ホス
10.1.1.1 : 0000.0c07.ac01	0000.0c00.0001 1 2/1	10.1.1.10 : 0000.0c00.0001	10.1.2.10 0000.0c00.0002	0000.0c00.0002 2 2/1	10.1.
10.1.1.3 : 0003.6bf1.2a0	0000.0c00.0002 2 1/1	10.1.2.10:0000.0c00.0001	10.1.1.10 0000.0c00.0001	0000.0c00.00001 1 1/1	10.1.

6. エコー応答がホスト A に到達し、フローが完了します。

非対称ルーティングの結果

ホスト A がホスト B に対して連続的に ping を発行する場合について考えます。ホスト A はエコー パケットを MSFC1 に送信し、ホスト B はエコー応答を MSFC2 に送信することを考えると、これは非対称ルーティングの状態です。スイッチ 1 がホスト B の送信元 MAC を学習できるのは、ホスト B が MSFC1 からの ARP 要求に応答するときだけです。これは、ホスト B が MSFC2 をデフォルト ゲートウェイとして使用しており、パケットを MSFC1 へ (結果的にスイッチ 1 へ) 送信していないためです。ARP タイムアウトはデフォルトでは 4 時間なので、スイッチ 1 はデフォルトで 5 分後にホスト B の MAC アドレスをエージングします。スイッチ2は5分後にホストAをエージングします。その結果、スイッチ 1 はホスト B の MAC 宛てのパケットをすべて不明のユニキャストとして処理する必要があります。スイッチ 1 は、ホスト A からホスト B 宛てに送信されるパケットを、すべてのポートからフラッディングします。また、スイッチ 1 にホスト B の MAC アドレス エントリがないため、同様に MLS エントリもありません。

ARP および MAC アドレス テーブル：ホスト A がホスト B に対し連続的に ping を発行し始めて

から 5 分後

ホスト A の ARP テーブル	スイッチ 1 の MAC アドレス テーブル MAC VLAN ポート	MSFC1 ARP テーブル	MSFC2 ARP テーブル	スイッチ 2 の MAC アドレス テーブル MAC VLAN ポート	ホスト B ARP テーブ
10.1.1.1 : 0000.0c07.ac01	0000.0c00.0001 1 2/1	10.1.1.10 : 0000.0c00.0001	10.1.2.10 0000.0c00.0002	0000.0c00.0002 2 2/1	10.1.2.2 : 0003.6bf1.2
10.1.1.3 : 0003.6bf1.2a0		10.1.2.10:0000.0c00.0001	10.1.1.10 0000.0c00.0001		10.1.2.1 : 0000.0c07.a

ホスト B から送信されるエコー応答パケットは、スイッチ 2 でホスト A の MAC アドレス エントリがエージングした後、同じ問題に遭遇します。ホスト B はエコー応答を MSFC2 に転送し、MSFC2 はこのパケットをルーティングして VLAN 1 上に送出します。スイッチの MAC アドレス テーブルにはホスト A のエントリがないため、VLAN 1 上のすべてのポートからパケットがフラッディングされます。

非対称ルーティングの問題によって接続が失われることはありません。しかし、非対称ルーティングが行われると過剰なユニキャスト フラッディングが発生し、MLS エントリが欠落する場合があります。この状況に対処するには、次の 3 通りの設定変更が考えられます。

- 各スイッチの MAC エージング タイムを 14,400 秒（4 時間）以上に調整する。
- ルータの ARP タイムアウトを 5 分（300 秒）に変更する。
- MAC エージング タイムと ARP タイムアウトを同じタイムアウト値に変更する。

最適な方法は、MAC エージング タイムを 14,400 秒に変更することです。設定のガイドラインを次に示します。

- Cisco IOS ソフトウェア：

  mac address-table aging-time <seconds> vlan <vlan_id>

ケーススタディ#6:HSRP仮想IPアドレスが異なるIPアドレスとしてレポートされる

スイッチでのブリッジング ループが原因で VLAN 間漏出があると、STANDBY-3-DIFFVIP1 エラー メッセージが表示されます。

このメッセージが表示されて、スイッチ内にブリッジング ループによる VLAN 間漏出がある場合、次の手順でエラーを解決します。

1. エンドノード間でパケットが辿るパスを特定します。

   そのパス上にルータがある場合は、次の手順を実行します。

   a. 最初のスイッチからルータまでのパスのトラブルシューティングを行う。

   b. ルータから 2 番目のスイッチまでのパスのトラブルシューティングを行う。

2. パス上の各スイッチを接続して、エンド ノード間のパスで使用されているポートの状態を調べる。

ケーススタディ#7：セキュアポートでHSRPによりMAC違反が発生する

HSRP が有効になっているルータに接続されたスイッチ ポートにポート セキュリティが設定されている場合、複数のインターフェイスに同じセキュア MAC アドレスを付けることはできないため、MAC 違反になります。次のいずれかの場合に、セキュア ポートでセキュリティ違反が発生します。

- アドレス テーブルにはセキュア MAC アドレスが最大数入っている状態で、MAC アドレスがアドレス テーブルに登録されていないステーションがインターフェイスにアクセスしようとした。
- あるセキュア インターフェイスで学習または設定されたアドレスが、同じ VLAN 内の別のセキュア インターフェイスで検出された場合。

デフォルトでは、ポート セキュリティ違反により、スイッチのインターフェイスは error-disable の状態になり、即座にシャットダウンされます。これにより、ルータ間の HSRP 状態のメッセージはブロックされます。

回避策

- ルータで、standby use-bia コマンドを発行します。これにより、ルータでは、仮想 MAC アドレスではなく、HSRP 用のバーンドイン アドレスが使用されるようになります。
- HSRP が有効にされているルータに接続されたスイッチのポートで、ポート セキュリティを無効にします。

ケーススタディ#9: %Interfaceハードウェアは複数のグループをサポートできません

インターフェイスに複数の HSRP グループが作成されている場合は、次のエラー メッセージが表示されます。

```
%Interface hardware cannot support multiple groups
```

このエラー メッセージが表示される理由は、一部のルータやスイッチでのハードウェアの制限です。ソフトウェアでこの制限を克服することはできません。インターフェイスで各 HSRP グループが 1 つの追加 MAC アドレスを使用しているため、イーサネット MAC チップでは、複数の HSRP グループを有効にするために複数のプログラマブル MAC アドレスをサポートする必要があることが、問題点です。

standby use-bia インターフェイス コンフィギュレーション コマンドの使用が解決策で、その場合、事前に割り当てられた MAC アドレスではなく、仮想 MAC アドレスとしてのインターフェイ

スのバーンドイン アドレス (BIA) が使用されます。

CatalystスイッチにおけるHSRPのトラブルシューティング

A. HSRPルータ設定の確認

1. ルータ インターフェイスの一意の IP アドレス確認

各 HSRP ルータで、サブネットごとに一意の IP アドレスが設定されていることをインターフェイス単位で確認します。また、各インターフェイスの回線プロトコルが up であることも確認します。各インターフェイスの現在の状態を簡単に確認するには、show ip interface brief コマンドを発行します。ランダム データの例は次のとおりです。

```
Router_1#show ip interface brief
Interface          IP-Address      OK? Method Status            Protocol
Vlan1              192.168.1.1     YES manual up                up
Vlan10             192.168.10.1    YES manual up                up
Vlan11             192.168.11.1    YES manual up                up

Router_2#show ip interface brief
Interface          IP-Address      OK? Method Status            Protocol
Vlan1              192.168.1.2     YES manual up                up
Vlan10             192.168.10.2    YES manual up                up
Vlan11             192.168.11.2    YES manual up    up
```

2. スタンバイ (HSRP) IP アドレスとスタンバイ グループ番号の確認

設定されているスタンバイ (HSRP) IP アドレスとスタンバイ グループ番号が、HSRP に参加する各ルータ間で一致していることを確認します。スタンバイ グループまたは HSRP スタンバイ アドレスが一致していないと、HSRP に問題が生じるおそれがあります。各インターフェイスのスタンバイ グループとスタンバイ IP アドレスの設定の詳細を表示するには、show standby コマンドを発行します。ランダム データの例は次のとおりです。

```
Router_1#show standby
Vlan10 - Group 110
  State is Active
    2 state changes, last state change 00:01:34
  Virtual IP address is 192.168.10.100
  Active virtual MAC address is 0000.0c07.ac6e (MAC In Use)
    Local virtual MAC address is 0000.0c07.ac6e (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 0.144 secs
  Preemption enabled
  Active router is local
  Standby router is 192.168.10.2, priority 109 (expires in 10.784 sec)
  Priority 110 (configured 110)
  Group name is "hsrp-Vl10-110" (default)
```

```
  FLAGS: 0/1
Vlan11 - Group 111
  State is Active
    2 state changes, last state change 00:00:27
  Virtual IP address is 192.168.11.100
  Active virtual MAC address is 0000.0c07.ac6f (MAC In Use)
    Local virtual MAC address is 0000.0c07.ac6f (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 2.096 secs
  Preemption enabled
  Active router is local
  Standby router is 192.168.11.2, priority 109 (expires in 8.944 sec)
  Priority 110 (configured 110)
  Group name is "hsrp-Vl11-111" (default)
  FLAGS: 0/1

Router_2#show standby
Vlan10 - Group 110
  State is Standby
    1 state change, last state change 00:03:15
  Virtual IP address is 192.168.10.100
  Active virtual MAC address is 0000.0c07.ac6e (MAC Not In Use)
    Local virtual MAC address is 0000.0c07.ac6e (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 1.088 secs
  Preemption disabled
  Active router is 192.168.10.1, priority 110 (expires in 11.584 sec)
  Standby router is local
  Priority 109 (configured 109)
  Group name is "hsrp-Vl10-110" (default)
  FLAGS: 0/1
Vlan11 - Group 111
  State is Standby
    1 state change, last state change 00:02:53
  Virtual IP address is 192.168.11.100
  Active virtual MAC address is 0000.0c07.ac6f (MAC Not In Use)
    Local virtual MAC address is 0000.0c07.ac6f (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 2.352 secs
  Preemption disabled
  Active router is 192.168.11.1, priority 110 (expires in 9.120 sec)
  Standby router is local
  Priority 109 (configured 109)
  Group name is "hsrp-Vl11-111" (default)
  FLAGS: 0/1
```

3. スタンバイ（HSRP）IP アドレスがインターフェイスごとに異なることを確認

スタンバイ（HSRP）IP アドレスが、インターフェイス単位で設定されている IP アドレスで一意であることを確認します。この情報を簡単に表示するには、show standby コマンドを発行します。ランダム データの例は次のとおりです。

```
Router_1#show standby
```

```
Vlan10 - Group 110
  State is Active
    2 state changes, last state change 00:01:34
  Virtual IP address is 192.168.10.100
  Active virtual MAC address is 0000.0c07.ac6e (MAC In Use)
    Local virtual MAC address is 0000.0c07.ac6e (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 0.144 secs
  Preemption enabled
  Active router is local
  Standby router is 192.168.10.2, priority 109 (expires in 10.784 sec)
  Priority 110 (configured 110)
  Group name is "hsrp-Vl10-110" (default)
  FLAGS: 0/1
Vlan11 - Group 111
  State is Active
    2 state changes, last state change 00:00:27
  Virtual IP address is 192.168.11.100
  Active virtual MAC address is 0000.0c07.ac6f (MAC In Use)
    Local virtual MAC address is 0000.0c07.ac6f (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 2.096 secs
  Preemption enabled
  Active router is local
  Standby router is 192.168.11.2, priority 109 (expires in 8.944 sec)
  Priority 110 (configured 110)
  Group name is "hsrp-Vl11-111" (default)
  FLAGS: 0/1

Router_2#show standby
Vlan10 - Group 110
  State is Standby
    1 state change, last state change 00:03:15
  Virtual IP address is 192.168.10.100
  Active virtual MAC address is 0000.0c07.ac6e (MAC Not In Use)
    Local virtual MAC address is 0000.0c07.ac6e (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 1.088 secs
  Preemption disabled
  Active router is 192.168.10.1, priority 110 (expires in 11.584 sec)
  Standby router is local
  Priority 109 (configured 109)
  Group name is "hsrp-Vl10-110" (default)
  FLAGS: 0/1
Vlan11 - Group 111
  State is Standby
    1 state change, last state change 00:02:53
  Virtual IP address is 192.168.11.100
  Active virtual MAC address is 0000.0c07.ac6f (MAC Not In Use)
    Local virtual MAC address is 0000.0c07.ac6f (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 2.352 secs
  Preemption disabled
  Active router is 192.168.11.1, priority 110 (expires in 9.120 sec)
  Standby router is local
  Priority 109 (configured 109)
  Group name is "hsrp-Vl11-111" (default)
  FLAGS: 0/1
```

4. standy use-bia コマンドを使用するケース

トークン リング インターフェイスで HSRP が設定されている場合を除き、standby use-bia コマンドを使用するのは、特別な状況でだけです。このコマンドはルータに対して、HSRP グループの仮想 HSRP MAC アドレスではなくルータの BIA を使用するように指示します。トークン リング ネットワークでは、ソースルート ブリッジング（SRB）を使用している場合、standby use-bia コマンドにより、新しいアクティブ ルータで gratuitous ARP を使用してホストのルーティング情報フィールド（RIF）のキャッシュを更新できます。ただし、すべてのホストの実装で gratuitous ARP が正しく処理されるとは限りません。standby use-bia コマンドに関するもう 1 つの注意はプロキシ ARP に関係するものです。スタンバイ ルータは、故障したアクティブ ルータのプロキシ ARP データベースが失われた場合、それを補うことができません。

5. アクセス リスト設定の確認

すべての HSRP ピアに設定されているアクセス リストにより、各ピアのインターフェイスに設定されているどの HSRP アドレスもフィルタリングされていないことを確認します。特に、サブネット上のすべてのルータにトラフィックを送信するためのマルチキャスト アドレス（224.0.0.2）を確認してください。さらに、HSRP ポート 1985 宛ての UDP トラフィックがフィルタリングされていないことも確認します。HSRP では、このアドレスとポートを使用して、ピア間で hello パケットを送信します。ルータで設定されているアクセス リストを簡単に参照するには、show access-lists コマンドを発行します。ランダム データの例は次のとおりです。

```
Router_1#show access-lists
Standard IP access list 77
    deny 10.19.0.0, wildcard bits 0.0.255.255
    permit any
Extended IP access list 144
    deny pim 238.0.10.0 0.0.0.255 any
    permit ip any any (58 matches)
```

B. Catalyst の Fast EtherChannel 設定とトランキング設定の確認

1. トランキング設定の確認

HSRP ルータの接続にトランクを使用している場合は、ルータとスイッチのトランキング設定を確認します。設定可能なトランキング モードは 5 種類あります。

- on
- 望ましい
- 自動

- オフ
- nonegotiate

設定されているトランキング モードによって、必要なトランキング方式が提供されることを確認します。

HSRP 問題のトラブルシューティングを行う際、スイッチ間の接続では desirable 設定を使用してください。このように設定すると、スイッチ ポートで正常にトランクを確立できない問題を切り分けることができます。ルータとスイッチ間の設定では、ほとんどの Cisco IOS ルータがトランクのネゴシエートをサポートしていないため nonegotiate に設定します。

IEEE 802.1Q(dot1q)トランキングモードの場合は、トランクの両側が同じネイティブVLANとカプセル化を使用するように設定されていることを確認します。シスコ製品はデフォルトではネイティブ VLAN にタグ付けしないため、ネイティブ VLAN 設定が一致していないと、それらの VLAN 上で接続できません。最後に、ルータで設定されている VLAN を伝送するようにトランクが設定されていることと、その VLAN がプルーニングされておらず、ルータ接続ポートで STP 状態にあることを確認します。この情報を簡単に参照するには、show interfaces <interface> trunkコマンドを発行します。ランダム データの例は次のとおりです。

```
L2Switch_1#show interfaces gigabitEthernet1/0/13 trunk Port Mode Encapsulation Status Native vlan Gi1/0/13 on 802.1q trunking 1 Port Vlans allowed o
Router_1#show interfaces gigabitEthernet1/0/1 trunk Port Mode Encapsulation Status Native vlan Gi1/0/1 on 802.1q trunking 1 Port Vlans allowed on trun
```

2. Fast EtherChannel（ポート チャネリング）設定の確認

HSRP ルータの接続にポート チャネルを使用している場合は、ルータとスイッチ両方の EtherChannel 設定を確認します。スイッチ間のポート チャネルでは、少なくとも一方を desirable に設定します。もう一方は、次のモードのいずれかに設定できます。

- on
- 望ましい
- 自動

ただし、この例では、インターフェイスはポートチャネルのメンバではありません。

```
Router_1#show etherchannel summary
Flags:  D - down        P - bundled in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator

        M - not in use, minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
```

```
        d - default port

        A - formed by Auto LAG


Number of channel-groups in use: 0
Number of aggregators:           0

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------

Router_1#

Router_2#show etherchannel summary
Flags:  D - down        P - bundled in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator

        M - not in use, minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port

        A - formed by Auto LAG


Number of channel-groups in use: 0
Number of aggregators:           0

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------

Router_2#
```

3. スイッチの MAC アドレス転送テーブルの確認

HSRP ルータのスイッチの MAC アドレス テーブルに、HSRP の仮想 MAC アドレスおよび物理 BIA のエントリが存在することを確認します。ルータ上で show standby コマンドを発行すると仮想 MAC アドレスが表示されます。show interface コマンドを発行すると物理 BIA が表示されます。次に出力例を示します。

```
Router_1#show standby
Vlan10 - Group 110
  State is Active
    2 state changes, last state change 00:37:03
  Virtual IP address is 192.168.10.100
  Active virtual MAC address is 0000.0c07.ac6e (MAC In Use)
    Local virtual MAC address is 0000.0c07.ac6e (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 0.768 secs
  Preemption enabled
```

```
  Active router is local
  Standby router is 192.168.10.2, priority 109 (expires in 10.368 sec)
  Priority 110 (configured 110)
  Group name is "hsrp-Vl10-110" (default)
  FLAGS: 0/1
Vlan11 - Group 111
  State is Active
    2 state changes, last state change 00:35:56
  Virtual IP address is 192.168.11.100
  Active virtual MAC address is 0000.0c07.ac6f (MAC In Use)
    Local virtual MAC address is 0000.0c07.ac6f (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 1.472 secs
  Preemption enabled
  Active router is local
  Standby router is 192.168.11.2, priority 109 (expires in 8.336 sec)
  Priority 110 (configured 110)
  Group name is "hsrp-Vl11-111" (default)
  FLAGS: 0/1

Router_1#show interfaces vlan 10
Vlan10 is up, line protocol is up , Autostate Enabled
  Hardware is Ethernet SVI, address is d4e8.801f.4846 (bia d4e8.801f.4846)
  Internet address is 192.168.10.1/24
  MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive not supported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:00, output 00:00:01, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/375/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     9258 packets input, 803066 bytes, 0 no buffer
     Received 0 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     3034 packets output, 368908 bytes, 0 underruns
     Output 0 broadcasts (0 IP multicasts)
     0 output errors, 2 interface resets
     0 unknown protocol drops
     0 output buffer failures, 0 output buffers swapped out

L2Switch_1#show mac address-table address 0000.0c07.ac6e
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
  10    0000.0c07.ac6e    DYNAMIC     Gi1/0/13
Total Mac Addresses for this criterion: 1

L2Switch_1#show mac address-table address 0000.0c07.ac6f
          Mac Address Table
-------------------------------------------
```

```
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
  11    0000.0c07.ac6f    DYNAMIC     Gi1/0/13
Total Mac Addresses for this criterion: 1
```

エントリがどれくらいの時間でエージングされるかを確認するために、CAM エージング タイムをチェックしてください。この時間が、STP 転送遅延に設定されている値、つまりデフォルトで 15 秒と同じである場合は、ネットワーク内に STP ループが発生している可能性が高くなります。コマンド出力例を挙げます。

```
L2Switch_1#show mac address-table aging-time  vlan 10
Global Aging Time:  300
Vlan    Aging Time
----    ----------
  10     300

L2Switch_1#show mac address-table aging-time  vlan 11
Global Aging Time:  300
Vlan    Aging Time
----    ----------
  11     300
```

C. 物理層の接続性の確認

HSRP グループ内で複数のルータがアクティブになった場合、これらのルータでは他の HSRP ピアからの hello パケットを定常的には受信しなくなります。物理層の問題によって、ピア間のトラフィックの定常的なパスが妨げられ、このシナリオが発生する場合があります。HSRP のトラブルシューティングを行う際には、HSRP ピア間の物理的な接続性と IP の接続性を確認してください。接続性を確認するには、show standby コマンドを発行します。ランダム データの例は次のとおりです。

```
Router_1#show standby
Vlan10 - Group 110
  State is Active
    2 state changes, last state change 00:54:03
  Virtual IP address is 192.168.10.100
  Active virtual MAC address is 0000.0c07.ac6e (MAC In Use)
    Local virtual MAC address is 0000.0c07.ac6e (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 0.848 secs
  Preemption enabled
  Active router is local
  Standby router is unknown
  Priority 110 (configured 110)
  Group name is "hsrp-Vl10-110" (default)
  FLAGS: 0/1
Vlan11 - Group 111
  State is Active
```

```
    2 state changes, last state change 00:52:56
  Virtual IP address is 192.168.11.100
  Active virtual MAC address is 0000.0c07.ac6f (MAC In Use)
    Local virtual MAC address is 0000.0c07.ac6f (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 0.512 secs
  Preemption enabled
  Active router is local
  Standby router is unknown
  Priority 110 (configured 110)
  Group name is "hsrp-Vl11-111" (default)
  FLAGS: 0/1

Router_2#show standby
Vlan10 - Group 110
  State is Init (interface down)
    2 state changes, last state change 00:00:42
  Virtual IP address is 192.168.10.100
  Active virtual MAC address is unknown (MAC Not In Use)
    Local virtual MAC address is 0000.0c07.ac6e (v1 default)
  Hello time 3 sec, hold time 10 sec
  Preemption disabled
  Active router is unknown
  Standby router is unknown
  Priority 109 (configured 109)
  Group name is "hsrp-Vl10-110" (default)
  FLAGS: 0/1
Vlan11 - Group 111
  State is Init (interface down)
    2 state changes, last state change 00:00:36
  Virtual IP address is 192.168.11.100
  Active virtual MAC address is unknown (MAC Not In Use)
    Local virtual MAC address is 0000.0c07.ac6f (v1 default)
  Hello time 3 sec, hold time 10 sec
  Preemption disabled
  Active router is unknown
  Standby router is unknown
  Priority 109 (configured 109)
  Group name is "hsrp-Vl11-111" (default)
  FLAGS: 0/1
```

1. インターフェイスのステータスのチェック

インターフェイスを確認します。次の例のように、HSRP が設定されているインターフェイスがすべて up/up であることを確認します。

```
Router_1#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
Vlan1                  192.168.1.1     YES manual up                    up
Vlan10                 192.168.10.1    YES manual up                    up
Vlan11                 192.168.11.1    YES manual up                    up

Router_2#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
```

```
Vlan1              192.168.1.2     YES manual up                    up
Vlan10             192.168.10.2    YES manual administratively down down
Vlan11             192.168.11.2    YES manual administratively down down
```

インターフェイスのいずれかが管理上 down/down となっている場合は、そのルータで設定モードに入り、インターフェイス固有のコマンド no shutdown を発行します。ランダム データの例は次のとおりです。

```
Router_2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router_2(config)#interface vlan 10
Router_2(config-if)#no shutdown
Router_2(config-if)#end

Router_2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router_2(config)#interface vlan 11
Router_2(config-if)#no shutdown
Router_2(config-if)#end

Router_2#show ip interface brief
Interface          IP-Address      OK? Method Status                Protocol
Vlan1              192.168.1.2     YES manual up                    up
Vlan10             192.168.10.2    YES manual up                    down
Vlan11             192.168.11.2    YES manual up                    up
```

インターフェイスのいずれかが down/down または up/down の場合は、何らかのインターフェイス変更通知を示すログを確認します。Cisco IOS ソフトウェア ベースのスイッチでは、リンクが up/down 状態になると次のメッセージが表示されます。

```
%LINK-3-UPDOWN: Interface "interface", changed state to up
%LINK-3-UPDOWN: Interface "interface", changed state to down

Router_1#show log
3d04h: %STANDBY-6-STATECHANGE: Standby: 0: Vlan10 state Active-> Speak
3d04h: %LINK-5-CHANGED: Interface Vlan10, changed state to down
3d04h: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan10, changed state to down
```

HSRP ピア間にある、ポート、ケーブル、トランシーバやその他のデバイスを検査します。取り外されていたり、接続が緩んだりしているものはないか。繰り返しリンクが失われるインターフェイスはないか。適切なタイプのケーブルが使用されているか。この例のように、インターフェイスにエラーがないかチェックします。

```
Router_2#show interface vlan 10
Vlan10 is down, line protocol is down , Autostate Enabled
  Hardware is Ethernet SVI, address is 1880.90d8.5946 (bia 1880.90d8.5946)
```

```
  Internet address is 192.168.10.2/24
  MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive not supported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:10, output 00:00:08, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/375/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     1243 packets input, 87214 bytes, 0 no buffer
     Received 0 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     23 packets output, 1628 bytes, 0 underruns
     Output 0 broadcasts (0 IP multicasts)
     0 output errors, 2 interface resets
     0 unknown protocol drops
     0 output buffer failures, 0 output buffers swapped out
```

2. リンク変更およびポート エラー

スイッチ ポートでのリンク変更やその他のエラーが発生していないかをチェックします。次のコマンドを発行し、出力を確認します。

- show logging
- show interfaces <インターフェイス> counters
- show interfaces <interface>ステータス

これらのコマンドは、スイッチと他のデバイスの間の接続性に問題がないかを確認するのに役立ちます。

リンクが up/down 状態では、次のメッセージは正常です。

```
L2Switch_1#show logging
Syslog logging: enabled (0 messages dropped, 5 messages rate-limited, 0 flushes, 0 overruns, xml disabled, filtering disabled)

No Active Message Discriminator.



No Inactive Message Discriminator.



    Console logging: level informational, 319 messages logged, xml disabled,
                     filtering disabled
    Monitor logging: level debugging, 0 messages logged, xml disabled,
```

```
                filtering disabled
  Buffer logging:  level debugging, 467 messages logged, xml disabled,
                filtering disabled
  Exception Logging: size (4096 bytes)
  Count and timestamp logging messages: disabled
  File logging: disabled
  Persistent logging: disabled

No active filter modules.

  Trap logging: level informational, 327 message lines logged
    Logging Source-Interface:       VRF Name:

Log Buffer (10000 bytes):
*Jul 26 17:52:07.526: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/13, changed state to up
*Jul 26 17:52:09.747: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/13, changed state to down
*Jul 26 17:57:11.716: %SPANTREE-7-RECV_1Q_NON_TRUNK: Received 802.1Q BPDU on non trunk GigabitEthernet1/0/16 VLAN307.
*Jul 26 17:57:11.716: %SPANTREE-7-BLOCK_PORT_TYPE: Blocking GigabitEthernet1/0/16 on VLAN0307. Inconsistent port type.
*Jul 26 17:57:13.583: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/16, changed state to up
*Jul 26 17:57:16.237: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/16, changed state to down
*Jul 26 18:02:16.481: %SPANTREE-7-RECV_1Q_NON_TRUNK: Received 802.1Q BPDU on non trunk GigabitEthernet1/0/16 VLAN307.
*Jul 26 18:02:16.481: %SPANTREE-7-BLOCK_PORT_TYPE: Blocking GigabitEthernet1/0/16 on VLAN0307. Inconsistent port type.
*Jul 26 18:02:18.367: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/16, changed state to up
*Jul 26 18:02:20.561: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/16, changed state to down
```

ポートの一般的な健全性を確認するには、show interfaces <interface> statusコマンドを発行します。ランダム データの例は次のとおりです。

```
L2Switch_1#show interfaces gigabitEthernet 1/0/13 status

Port      Name               Status       Vlan       Duplex  Speed Type
Gi1/0/13                     connected    trunk      a-full a-1000 10/100/1000BaseTX
```

インターフェイスのステータスが`connected`、`notconnect`、または`errdisable`のいずれであるかを確認します。状態が `notconnect` の場合、両側でケーブルが差し込まれていることを確認します。適切なケーブルが使用されているか確認します。状態が `errdisable` の場合は、カウントが過度のエラーを示していないかを確認します。詳細は、『Cisco IOSプラットフォームでのerrdisableポート状態の回復』を参照してください。

ポートがどの VLAN に設定されているか調べます。接続されている相手側も同じ VLAN に設定されていることを確認します。リンクがトランクになるように設定されている場合は、トランクの両端で同じ VLAN に伝送されるようになっているかを確認します。

速度と二重モードの設定を調べます。設定が a- で始まっている場合、そのポートは速度と二重モードをオートネゴシエートする設定になっています。それ以外の場合、ネットワーク管理者によって設定が事前に定義されています。リンクの速度と二重モードを設定する場合には、リンクの両端で設定を一致させる必要があります。一方のスイッチ ポートがオートネゴシエーションに設定されている場合、リンクのもう一方もオートネゴシエーションに設定する必要があります。一方の側が特定の速度と二重モードにハードコードされている場合は、もう一方の側も同様にハー

ドコードされている必要があります。一方の側をハードコードし、もう一方の側をオートネゴシエートのままにしておくと、オートネゴシエーション プロセスは中止されます。

<#root>

L2Switch_1#show interfaces gi1/0/13 counters errors Port Align-Err FCS-Err Xmit-Err Rcv-Err UnderSize OutDiscards Gi1/0/13

0 0 0 0 0 0

Port Single-Col Multi-Col Late-Col Excess-Col Carri-Sen Runts Gi1/0/13

0 0 0 0 0 0

Align-Err、FCS-Err、または Runts が大量に発生していないかを調べます。これらは、ポートと接続先デバイスとの間で速度と二重モードが一致していないことを示します。このエラーの解消に、問題のポートの速度と二重モードの設定を変更してください。

ポートがトラフィックの受け渡しを行っていることを確認するには、show mac コマンドを発行します。In列とOut列は、特定のポートで送受信されたユニキャスト、マルチキャスト、およびブロードキャストパケットの数を示しています。最後の行のカウンタは、廃棄されたパケットと失われたパケットの数、およびそれらのパケットが着信トラフィックと発信トラフィックのいずれの一部であったかが示されています。Lrn-Discrd、In-Lost、および Out-Lost は、バッファ不足が原因で誤って転送または廃棄されたパケットの数をカウントします。

L2Switch_1#show interfaces gi1/0/13 counters

Port	InOctets	InUcastPkts	InMcastPkts	InBcastPkts
Gi1/0/13	304933333	1180453	1082538	14978

Port	OutOctets	OutUcastPkts	OutMcastPkts	OutBcastPkts
Gi1/0/13	282752538	276716	824562	588960

3. IP 接続性の確認

IP 接続性を確認します。関連付けられたルータからリモートHSRPデバイスにIP pingを発行します。瞬間的な接続性の喪失があれば、これによって明らかになります。拡張 ping が使用できるのは enable モードでだけです。コマンド出力例を挙げます。

Router_1#show run interface vlan 10
Building configuration...

Current configuration : 141 bytes
!
interface Vlan10
 ip address 192.168.10.1 255.255.255.0
 standby 110 ip 192.168.10.100

```
 standby 110 priority 110
 standby 110 preempt
end

Router_2#show run interface vlan 10
Building configuration...

Current configuration : 120 bytes
!
interface Vlan10
 ip address 192.168.10.2 255.255.255.0
 standby 110 ip 192.168.10.100
 standby 110 priority 109
end

Router_1#ping 192.168.10.2 repeat 1500
Type escape sequence to abort.
Sending 1500, 100-byte ICMP Echos to 192.168.10.2, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (1500/1500), round-trip min/avg/max = 1/2/9 ms
```

各 HSRP ルータからピアに対して ping を発行し、接続性の障害のある箇所を特定します。

4. 単方向リンクのチェック

スイッチに HSRP ピアとの間の単方向リンクがないかをチェックします。単方向リンクが発生するのは、ローカル デバイスがリンクを通じて送信したトラフィックは隣接デバイスで受信されるにもかかわらず、隣接デバイスが送信したトラフィックがそのローカル デバイスでは受信されない場合です。この機能は、UniDirectional Link Detection（UDLD; 単方向リンク検出）アグレッシブ モードと呼ばれています。UDLD が可能なのは、接続の両端でこの機能がサポートされている場合だけです。UDLD アグレッシブ モードは L2 で動作し、リンクが正常に接続されているかどうか、およびトラフィックが適切な隣接デバイス間で双方向に流れているかを判断します。次に

コマンド出力例を示します。

注：次のリンクに移動して、UDLD機能の理解と設定を行います。これは、使用されているプラットフォームによって異なります。

UDLDが使用できない場合に単方向リンクの確認に役立つもう1つのオプションは、Cisco Discovery Protocol(CDP)を使用する方法です。CDP を有効にすることでも、単方向リンクの存在を検出できます。リンクの片側だけで隣接デバイスを認識できる場合は、デバイスを接続しているケーブルを交換し、インターフェイスが故障していないかをチェックします。

```
Router_1#show cdp
Global CDP information:
    Sending CDP packets every 60 seconds
    Sending a holdtime value of 180 seconds
    Sending CDPv2 advertisements is  enabled

Router_1#show cdp neighbors gi1/0/1 detail
-------------------------
Device ID: L2Switch_1.cisco.com
Entry address(es):
  IP address: 192.168.70.1
  IPv6 address: 2001:420:140E:2101::1  (global unicast)
  IPv6 address: FE80::2FE:C8FF:FED3:86C7  (link-local)
Platform: cisco WS-C3650-12X48UR,  Capabilities: Router Switch IGMP
Interface: GigabitEthernet1/0/1,  Port ID (outgoing port): GigabitEthernet1/0/13
Holdtime : 173 sec

Version :
Cisco IOS Software [Denali], Catalyst L3 Switch Software (CAT3K_CAA-UNIVERSALK9-M), Version 16.3.8, RELEASE SOFTWARE (fc3)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2019 by Cisco Systems, Inc.
Compiled Wed 13-Feb-19 03:00 by mcpre

advertisement version: 2
VTP Management Domain: 'CALOnet'
Native VLAN: 1
Duplex: full
Management address(es):
  IP address: 192.168.70.1
Spare Pair PoE: Yes, Spare Pair Detection Required: No
Spare Pair PD Config: Disable, Spare Pair PSE Operational: No


Total cdp entries displayed : 1
```

5. 物理層のトラブルシューティングに関するその他のリファレンス

次のドキュメントを参照してください。

- イーサネット 10/100/1000 Mbps 半二重/全二重自動ネゴシエーションの設定とトラブルシ

ューティング

- Cisco IOS プラットフォームでの Errdisable ポート状態の回復
- 「Troubleshooting Cisco Catalyst Switches to NIC Compatibility Issues（Cisco Catalyst スイッチと NIC との互換性に関する問題のトラブルシューティング）」
- Cisco Catalyst スイッチと NIC との互換性に関する問題のトラブルシューティングの「データ リンク エラーについて」セクション
- トラブルシューティング：スイッチ ポートおよびインターフェイスの問題

D. レイヤ 3 HSRP デバッグ

HSRP状態の変化が頻繁に起こる場合は、ルータでHSRP debugコマンド（イネーブルモード）を使用して、HSRPのアクティビティを監視します。この情報は、どのような HSRP パケットがルータで送受信されているかを確認する上で役立ちます。シスコ テクニカル サポートでサービスリクエストを作成する場合は、この情報を収集します。デバッグ出力には、HSRP 状態に関する情報とともに、詳細な HSRP hello パケットのアカウントも表示されます。

1. 標準 HSRP デバッグ

Cisco IOSでは、debug standbyコマンドを使用して、HSRPデバッグ機能を有効にします。この情報は、問題が断続的で、影響が少数のインターフェイスだけに及ぶような場合に役立ちます。このデバッグによって、問題の HSRP ルータが一定の間隔で HSRP hello パケットを送受信しているかどうかがわかります。ルータが hello パケットが受信しない場合は、ピアが hello パケットを送信していないか、またはネットワークがパケットを廃棄しているかのどちらかが推測されます。

コマンド	目的
debug standby	HSRP デバッグを有効にする

コマンド出力例を挙げます。

```
Router_1#debug standby
HSRP debugging is on
Jul 29 16:12:16.889: HSRP: Vl10 Grp 110 Hello  out 192.168.10.1 Active  pri 110 vIP 192.168.10.100
Jul 29 16:12:16.996: HSRP: Vl11 Grp 111 Hello  in  192.168.11.2 Standby pri 109 vIP 192.168.11.100
Jul 29 16:12:17.183: HSRP: Vl10 Grp 110 Hello  in  192.168.10.2 Standby pri 109 vIP 192.168.10.100
Jul 29 16:12:17.366: HSRP: Vl11 Grp 111 Hello  out 192.168.11.1 Active  pri 110 vIP 192.168.11.100
Jul 29 16:12:18.736: HSRP: Vl10 Interface adv in, Passive, active 0, passive 1, from 192.168.10.2
Jul 29 16:12:19.622: HSRP: Vl10 Grp 110 Hello  out 192.168.10.1 Active  pri 110 vIP 192.168.10.100
```

2. 条件付き HSRP デバッグ（スタンバイ グループや VLAN に基づく出力の制限）

Cisco IOS ソフトウェア リリース 12.0(3) ではデバッグ条件が導入されたため、インターフェイ

スとグループ番号に基づいて、debug standby コマンドの出力にフィルタをかけることができます。コマンドは、Cisco IOS ソフトウェア リリース 12.0 で導入されたデバッグ条件のパラダイムを利用します。

コマンド	目的
デバッグ条件standby <インターフェイス> <グループ>	グループ (0 ~ 255) に対する HSRP 条件付きデバッグをイネーブルにする

interface は、HSRP をサポートできる有効なインターフェイスである必要があります。group には、0 から 255 の任意のグループを指定できます。存在しないグループにデバッグ条件を設定することもできます。これにより、新しいグループの初期化中のデバッグを取得することが可能です。デバッグ出力を生成するためには、debug standby を有効にしておく必要があります。スタンバイ デバッグ条件が存在しない場合は、すべてのインターフェイス上にあるすべてのグループについてデバッグ出力が生成されます。スタンバイ デバッグ条件が 1 つ以上存在する場合は、すべてのスタンバイ デバッグ条件に従って、スタンバイ デバッグの出力がフィルタリングされます。コマンド出力例を挙げます。

```
Router_1#debug condition standby vlan 10 110
Condition 1 set
Router_1#
Jul 29 16:16:20.284: Vl10 HSRP110 Debug: Condition 1, hsrp Vl10 HSRP110 triggered, count 1
Router_1#debug standby
HSRP debugging is on
Router_1#
Jul 29 16:16:44.797: HSRP: Vl10 Grp 110 Hello out 192.168.10.1 Active pri 110 vIP 192.168.10.100
Jul 29 16:16:45.381: HSRP: Vl10 Grp 110 Hello in 192.168.10.2 Standby pri 109 vIP 192.168.10.100
Jul 29 16:16:47.231: HSRP: Vl10 Grp 110 Hello out 192.168.10.1 Active pri 110 vIP 192.168.10.100
Jul 29 16:16:48.248: HSRP: Vl10 Grp 110 Hello in 192.168.10.2 Standby pri 109 vIP 192.168.10.100
```

3. 拡張 HSRP デバッグ

Cisco IOS ソフトウェア リリース 12.1(1) では、拡張 HSRP デバッグが導入されました。有用な情報を見つけ出せるよう、拡張 HSRP デバッグでは定期的な hello メッセージのノイズが制限されるほか、状態に関する情報が追加されます。この情報は、サービス リクエストを作成する場合、シスコ テクニカル サポートのエンジニアと共同作業を行う際に特に役立ちます。

コマンド	目的
debug standby	HSRP のエラー、イベント、およびパケットをすべて表示する
debug standby errors	HSRP エラーを表示する
debug standby events [[all] | [hsrp | redundancy | track]] [detail]	HSRP イベントを表示する
debug standby packets [[all | terse] | [advertise | coup | hello | resign]] [detail]	HSRP パケットを表示する
debug standby terse	HSRPエラー、イベント、およびパケットの範囲が限られている

コマンド出力例を挙げます。

```
Router_2#debug standby terse
HSRP:
  HSRP Errors debugging is on
  HSRP Events debugging is on
    (protocol, neighbor, redundancy, track, ha, arp, interface)
  HSRP Packets debugging is on
    (Coup, Resign)
Router_2#
*Jul 29 16:49:35.416: HSRP: Vl10 Grp 110 Resign in  192.168.10.1 Active  pri 110 vIP 192.168.10.100
*Jul 29 16:49:35.416: HSRP: Vl10 Grp 110 Standby: i/Resign rcvd (110/192.168.10.1)
*Jul 29 16:49:35.416: HSRP: Vl10 Grp 110 Active router is local, was 192.168.10.1
*Jul 29 16:49:35.416: HSRP: Vl10 Nbr 192.168.10.1 no longer active for group 110 (Standby)
*Jul 29 16:49:35.417: HSRP: Vl10 Nbr 192.168.10.1 Was active or standby - start passive holddown
*Jul 29 16:49:35.417: HSRP: Vl10 Grp 110 Standby router is unknown, was local
*Jul 29 16:49:35.417: HSRP: Vl10 Grp 110 Standby -> Active
*Jul 29 16:49:35.418: %HSRP-5-STATECHANGE: Vlan10 Grp 110 state Standby -> Active
*Jul 29 16:49:35.418: HSRP: Peer not present
*Jul 29 16:49:35.418: HSRP: Vl10 Grp 110 Redundancy "hsrp-Vl10-110" state Standby -> Active
*Jul 29 16:49:35.419: HSRP: Vl10 Grp 110 Added 192.168.10.100 to ARP (0000.0c07.ac6e)
*Jul 29 16:49:35.420: HSRP: Vl10 IP Redundancy "hsrp-Vl10-110" standby, local -> unknown
*Jul 29 16:49:35.421: HSRP: Vl10 IP Redundancy "hsrp-Vl10-110" update, Standby -> Active
*Jul 29 16:49:38.422: HSRP: Vl10 IP Redundancy "hsrp-Vl10-110" update, Active -> Active
```

このデバッグ出力をフィルタリングするため、インターフェイスや HSRP グループによる条件付きデバッグを使用できます。

コマンド	目的
debug condition interface interface	インターフェイスの条件付きデバッグを有効にする
デバッグ条件standby <インターフェイス> <グループ>	HSRP の条件付きデバッグを有効にする

この例では、ルータが既存の HSRP グループに参加しています。

```
Rotuer_2#debug condition standby vlan 10 110
Condition 1 set
Router_2#debug condition interface gigabitEthernet 1/0/1 vlan-id 10
Condition 2 set
Router_2#debug standby
HSRP debugging is on
Router_2#
*Jul 29 16:54:12.496: HSRP: Vl10 Grp 110 Hello  out 192.168.10.2 Active  pri 109 vIP 192.168.10.100
*Jul 29 16:54:15.122: HSRP: Vl10 Grp 110 Hello  out 192.168.10.2 Active  pri 109 vIP 192.168.10.100
*Jul 29 16:54:17.737: HSRP: Vl10 Grp 110 Hello  out 192.168.10.2 Active  pri 109 vIP 192.168.10.100
*Jul 29 16:54:18.880: HSRP: Vl10 Nbr 192.168.10.1 is passive
*Jul 29 16:54:20.316: HSRP: Vl10 Grp 110 Hello  out 192.168.10.2 Active  pri 109 vIP 192.168.10.100
*Jul 29 16:54:20.322: HSRP: Vl10 Grp 110 Coup   in  192.168.10.1 Listen  pri 110 vIP 192.168.10.100
*Jul 29 16:54:20.323: HSRP: Vl10 Grp 110 Active: j/Coup rcvd from higher pri router (110/192.168.10.1)
```

```
*Jul 29 16:54:20.323: HSRP: Vl10 Grp 110 Active router is 192.168.10.1, was local
*Jul 29 16:54:20.323: HSRP: Vl10 Nbr 192.168.10.1 is no longer passive
*Jul 29 16:54:20.324: HSRP: Vl10 Nbr 192.168.10.1 active for group 110
*Jul 29 16:54:20.324: HSRP: Vl10 Grp 110 Active -> Speak
*Jul 29 16:54:20.325: %HSRP-5-STATECHANGE: Vlan10 Grp 110 state Active -> Speak
*Jul 29 16:54:20.325: HSRP: Peer not present
*Jul 29 16:54:20.325: HSRP: Vl10 Grp 110 Redundancy "hsrp-Vl10-110" state Active -> Speak
*Jul 29 16:54:20.326: HSRP: Vl10 Grp 110 Removed 192.168.10.100 from ARP
*Jul 29 16:54:20.326: HSRP: Vl10 Grp 110 Deactivating MAC 0000.0c07.ac6e
*Jul 29 16:54:20.327: HSRP: Vl10 Grp 110 Removing 0000.0c07.ac6e from MAC address filter
*Jul 29 16:54:20.328: HSRP: Vl10 Grp 110 Hello  out 192.168.10.2 Speak   pri 109 vIP 192.168.10.100
*Jul 29 16:54:20.328: HSRP: Vl10 Grp 110 Hello  in  192.168.10.1 Active  pri 110 vIP 192.168.10.100
*Jul 29 16:54:23.104: HSRP: Vl10 Grp 110 Hello  out 192.168.10.2 Speak   pri 109 vIP 192.168.10.100
*Jul 29 16:54:23.226: HSRP: Vl10 Grp 110 Hello  in  192.168.10.1 Active  pri 110 vIP 192.168.10.100
*Jul 29 16:54:25.825: HSRP: Vl10 Grp 110 Hello  in  192.168.10.1 Active  pri 110 vIP 192.168.10.100
*Jul 29 16:54:25.952: HSRP: Vl10 Grp 110 Hello  out 192.168.10.2 Speak   pri 109 vIP 192.168.10.100
*Jul 29 16:54:28.427: HSRP: Vl10 Grp 110 Hello  in  192.168.10.1 Active  pri 110 vIP 192.168.10.100
*Jul 29 16:54:28.772: HSRP: Vl10 Grp 110 Hello  out 192.168.10.2 Speak   pri 109 vIP 192.168.10.100
*Jul 29 16:54:30.727: HSRP: Vl10 Grp 110 Speak: d/Standby timer expired (unknown)
*Jul 29 16:54:30.727: HSRP: Vl10 Grp 110 Standby router is local
*Jul 29 16:54:30.727: HSRP: Vl10 Grp 110 Speak -> Standby
*Jul 29 16:54:30.727: %HSRP-5-STATECHANGE: Vlan10 Grp 110 state Speak -> Standby
*Jul 29 16:54:30.728: HSRP: Peer not present
*Jul 29 16:54:30.728: HSRP: Vl10 Grp 110 Redundancy "hsrp-Vl10-110" state Speak -> Standby
*Jul 29 16:54:30.728: HSRP: Vl10 Grp 110 Hello  out 192.168.10.2 Standby pri 109 vIP 192.168.10.100
*Jul 29 16:54:31.082: HSRP: Vl10 Grp 110 Hello  in  192.168.10.1 Active  pri 110 vIP 192.168.10.100
*Jul 29 16:54:33.459: HSRP: Vl10 Grp 110 Hello  out 192.168.10.2 Standby pri 109 vIP 192.168.10.100
*Jul 29 16:54:33.811: HSRP: Vl10 Grp 110 Hello  in  192.168.10.1 Active  pri 110 vIP 192.168.10.100
*Jul 29 16:54:36.344: HSRP: Vl10 Grp 110 Hello  out 192.168.10.2 Standby pri 109 vIP 192.168.10.100
*Jul 29 16:54:36.378: HSRP: Vl10 Grp 110 Hello  in  192.168.10.1 Active  pri 110 vIP 192.168.10.100
*Jul 29 16:54:38.856: HSRP: Vl10 Grp 110 Hello  in  192.168.10.1 Active  pri 110 vIP 192.168.10.100
*Jul 29 16:54:38.876: HSRP: Vl10 Grp 110 Hello  out 192.168.10.2 Standby pri 109 vIP 192.168.10.100
*Jul 29 16:54:41.688: HSRP: Vl10 Grp 110 Hello  out 192.168.10.2 Standby pri 109 vIP 192.168.10.100
*Jul 29 16:54:41.717: HSRP: Vl10 Grp 110 Hello  in  192.168.10.1 Active  pri 110 vIP 192.168.10.100
```

E. スパニング ツリーのトラブルシューティング

ネットワーク内での STP のループ状態や不安定さにより、HSRP ピアの適切な通信が妨げられる場合があります。この不適切な通信が原因で、それぞれのピアがアクティブルータになります。STP ループにより、ブロードキャスト ストーム、フレームの重複、および MAC テーブルの矛盾が引き起こされる可能性があります。これらの問題はすべてネットワーク全体、とりわけ HSRP に影響を及ぼします。STP 問題の最初の徴候が HSRP エラー メッセージであることもあります。

STP のトラブルシューティングを行う際には、ネットワークの STP トポロジを VLAN ごとに理解する必要があります。どのスイッチがルート ブリッジであり、スイッチ上のどのポートがブロッキング状態で、どのポートがフォワーディング状態かを特定する必要があります。各 VLAN にはそれぞれ固有の STP トポロジがあるため、この情報は VLAN ごとに非常に重要です。

1. スパニング ツリー設定の確認

ネットワーク内にあるすべてのスイッチとブリッジング デバイスで STP が設定されていること

を確認します。各スイッチが、ルートブリッジをどこにあると認識しているかに注意します。また、次のタイマーの値にも注意します。

- Root Max Age
- Helloタイム
- 転送遅延

この情報すべてを参照するにはshow spanning-treeコマンドを発行します。デフォルトでは、このコマンドはすべてのVLANに関する情報を表示します。ただし、コマンドを使用してVLAN番号を指定すると、他のVLAN情報をフィルタリングすることもできます。この情報は、STP 問題のトラブルシューティングを行う際に非常に役に立ちます。

show spanning-treeの出力に表示される、これらの3つのタイマーは、ルートブリッジから学習されます。これらのタイマーは、特定のブリッジに設定されているタイマーと一致する必要はありません。しかし、このスイッチがある時点でルート ブリッジになるような場合は、これらのタイマーがルート ブリッジと一致していることを確認してください。タイマーがルート ブリッジと一致していると、一貫性が維持され管理が容易になります。また、誤ったタイマーを持つスイッチによってネットワークが損なわれることが防止されます。

注：ネットワーク内に冗長リンクがあるかどうかに関係なく、常にすべてのVLANでSTPを有効にしてください。非冗長ネットワークで STP を有効にすると、障害が防止されます。スイッチどうしやスイッチとハブをブリッジし、誤って物理ループが作成された場合に障害が発生する場合があります。STP は特定の問題を切り分けるためにも非常に役立ちます。STP を有効にした結果、ネットワーク内のなんらかの動作に影響が生じた場合は、切り分けが必要な既存の問題がある可能性があります。

---

show spanning-treeコマンドの出力例を次に示します。

```
L2Switch_1#show spanning-tree vlan 10

VLAN0010
  Spanning tree enabled protocol rstp
  Root ID    Priority    32778
             Address     00fe.c8d3.8680
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32778  (priority 32768 sys-id-ext 10)
             Address     00fe.c8d3.8680
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  300 sec

Interface          Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Gi1/0/3            Desg FWD 4         128.3    P2p
Gi1/0/10           Desg FWD 4         128.10   P2p Edge
Gi1/0/11           Desg FWD 4         128.11   P2p
Gi1/0/13           Desg FWD 4         128.13   P2p
```

```
Gi1/0/14         Desg FWD 4        128.14   P2p
Gi1/0/15         Desg FWD 4        128.15   P2p
Gi1/0/16         Desg FWD 4        128.16   P2p
Gi1/0/35         Desg FWD 4        128.35   P2p


L2Switch_1#show spanning-tree vlan 11

VLAN0011
  Spanning tree enabled protocol rstp
  Root ID    Priority    32779
             Address     00fe.c8d3.8680
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32779  (priority 32768 sys-id-ext 11)
             Address     00fe.c8d3.8680
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  300 sec

Interface          Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Gi1/0/3            Desg FWD 4         128.3    P2p
Gi1/0/10           Desg FWD 4         128.10   P2p Edge
Gi1/0/11           Desg FWD 4         128.11   P2p
Gi1/0/13           Desg FWD 4         128.13   P2p
Gi1/0/14           Desg FWD 4         128.14   P2p
Gi1/0/15           Desg FWD 4         128.15   P2p
Gi1/0/16           Desg FWD 4         128.16   P2p
Gi1/0/35           Desg FWD 4         128.35   P2p
```

スイッチL2Switch_1はVLAN 10とVLAN 11のルートです。

2. スパニング ツリー ループ状態

STP ループが発生する場合、ネットワーク内に L2 の物理的冗長性があるはずです。物理ループの状態になる可能性がない場合、STP ループは発生しません。STP ループ状態の症状には次のものがあります。

- ネットワーク全体の停止
- 接続の消失
- ネットワーク機器によりプロセスやシステムの高い使用率がレポートされる

STP ループ状態の VLAN が 1 つでもあれば、リンクの輻輳が起こり、他の VLAN が帯域幅不足に陥る可能性があります。show interfaces <interface> controllerコマンドにより、過剰な数のパケットを送受信しているポートが特定されます。ブロードキャストとマルチキャストが過剰なポートは、STP ループを構成している可能性があります。基本的には、マルチキャストまたはブロードキャストがユニキャスト パケットの数を上回っている場合は、リンクが STP ループ状態に陥っていることを常に疑います。

注：スイッチでは、マルチキャストフレームとして送受信されるSTPブリッジプロトコルデータユニット(BPDU)もカウントされます。ポートでは、STP ブロッキング状態になっても、引き続き STP BPDU は送受信されます。

```
Router_2#show interfaces gi1/0/1 controller
GigabitEthernet1/0/1 is up, line protocol is up (connected)
  Hardware is Gigabit Ethernet, address is 1880.90d8.5901 (bia 1880.90d8.5901)
  Description: PNP STARTUP VLAN
  MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 1000Mb/s, media type is 10/100/1000BaseTX
  input flow-control is on, output flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:00, output 00:00:04, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/2000/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 33000 bits/sec, 31 packets/sec
  5 minute output rate 116000 bits/sec, 33 packets/sec
     9641686 packets input, 1477317083 bytes, 0 no buffer
     Received 1913802 broadcasts (1151766 multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 1151766 multicast, 0 pause input
     0 input packets with dribble condition detected
     10702696 packets output, 4241534645 bytes, 0 underruns
     Output 3432 broadcasts (0 multicasts)
     0 output errors, 0 collisions, 2 interface resets
     9582 unknown protocol drops
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier, 0 pause output
     0 output buffer failures, 0 output buffers swapped out
Transmit                GigabitEthernet1/0/1          Receive
   4241534645 Total bytes                1477317083 Total bytes
     10562003 Unicast frames                7727884 Unicast frames
   4229489212 Unicast bytes              1291270617 Unicast bytes
      137261 Multicast frames              1151766 Multicast frames
     11812065 Multicast bytes              91096867 Multicast bytes
        3432 Broadcast frames              762036 Broadcast frames
      233368 Broadcast bytes              94949599 Broadcast bytes
           0 System FCS error frames             0 IpgViolation frames
           0 MacUnderrun frames                  0 MacOverrun frames
           0 Pause frames                  0 Pause frames
           0 Cos 0 Pause frames                  0 Cos 0 Pause frames
           0 Cos 1 Pause frames                  0 Cos 1 Pause frames
           0 Cos 2 Pause frames                  0 Cos 2 Pause frames
           0 Cos 3 Pause frames                  0 Cos 3 Pause frames
           0 Cos 4 Pause frames                  0 Cos 4 Pause frames
           0 Cos 5 Pause frames                  0 Cos 5 Pause frames
           0 Cos 6 Pause frames                  0 Cos 6 Pause frames
           0 Cos 7 Pause frames                  0 Cos 7 Pause frames
           0 Oam frames                  0 OamProcessed frames
```

0 Oam frames	0 OamDropped frames
38144 Minimum size frames	4165201 Minimum size frames
4910833 65 to 127 byte frames	3126489 65 to 127 byte frames
1237675 128 to 255 byte frames	750243 128 to 255 byte frames
1029126 256 to 511 byte frames	1279281 256 to 511 byte frames
2205966 512 to 1023 byte frames	103668 512 to 1023 byte frames
1280952 1024 to 1518 byte frames	205229 1024 to 1518 byte frames
0 1519 to 2047 byte frames	11575 1519 to 2047 byte frames
0 2048 to 4095 byte frames	0 2048 to 4095 byte frames
0 4096 to 8191 byte frames	0 4096 to 8191 byte frames
0 8192 to 16383 byte frames	0 8192 to 16383 byte frames
0 16384 to 32767 byte frame	0 16384 to 32767 byte frame
0 > 32768 byte frames	0 > 32768 byte frames
0 Late collision frames	0 SymbolErr frames
0 Excess Defer frames	0 Collision fragments
0 Good (1 coll) frames	0 ValidUnderSize frames
0 Good (>1 coll) frames	0 InvalidOverSize frames
0 Deferred frames	0 ValidOverSize frames
0 Gold frames dropped	0 FcsErr frames
0 Gold frames truncated	
0 Gold frames successful	
0 1 collision frames	
0 2 collision frames	
0 3 collision frames	
0 4 collision frames	
0 5 collision frames	
0 6 collision frames	
0 7 collision frames	
0 8 collision frames	
0 9 collision frames	
0 10 collision frames	
0 11 collision frames	
0 12 collision frames	
0 13 collision frames	
0 14 collision frames	
0 15 collision frames	
0 Excess collision frames	

LAST UPDATE 2384 msecs AGO

3. トポロジ変更通知

STP問題の診断に重要なもう1つのコマンドが、show spanning-tree detailコマンドです。このコマンドは、Topology Change Notification（TCN; トポロジ変更通知）メッセージを発信者までたどって追跡します。TCN メッセージは、特別な BPDU としてスイッチ間で送信され、スイッチ上でトポロジの変更があったことを示します。トポロジの変更があったスイッチは、自身のルート ポートから TCN を送出します。TCN は上流方向にルート ブリッジまで移動します。ルート ブリッジは、Topology Change Acknowledgement（TCA; トポロジ変更確認応答）というもう 1 つの特別な BPDU をすべてのポートから送出します。ルート ブリッジはコンフィギュレーション BPDU に TCN ビットを設定します。これにより、すべての非ルート ブリッジは自身の MAC アドレス テーブルのエージング タイマーをコンフィギュレーション STP 転送遅延に設定します。

この問題を切り分けるには、各VLANのルートブリッジにアクセスし、スイッチが接続されたポートに対してshow spanning-tree <interface> detailコマンドを発行します。`last change occurred`エントリに、最後のTCNが受信された時刻が表示されます。この状況では、TCN を受信してから時間が経過し過ぎているため、どのデバイスが STP ループの原因となる TCN を発行したかはわかりません。`Number of topology changes`エントリから、発生したTCNの数を推測できます。STP ループの間、このカウンタは 1 分ごとに増分される可能性があります。詳細は、「Spanning Tree Protocol Problems and Related Design Considerations（スパニングツリー プロトコルのトラブルシューティングと設計上の考慮事項）」を参照してください。

そのほか、次のような役立つ情報があります。

- 前回の TCN のポート
- 前回の TCN の時刻
- 現在の TCN の数

コマンド出力例を挙げます。

```
L2Switch_1#show spanning-tree vlan 10 detail

 VLAN0010 is executing the rstp compatible Spanning Tree protocol
  Bridge Identifier has priority 32768, sysid 10, address 00fe.c8d3.8680
  Configured hello time 2, max age 20, forward delay 15, transmit hold-count 6
  We are the root of the spanning tree
  Topology change flag not set, detected flag not set
  Number of topology changes 8 last change occurred 03:21:48 ago
        from GigabitEthernet1/0/35
  Times:  hold 1, topology change 35, notification 2
        hello 2, max age 20, forward delay 15
  Timers: hello 0, topology change 0, notification 0, aging 300

 Port 3 (GigabitEthernet1/0/3) of VLAN0010 is designated forwarding
   Port path cost 4, Port priority 128, Port Identifier 128.3.
   Designated root has priority 32778, address 00fe.c8d3.8680
   Designated bridge has priority 32778, address 00fe.c8d3.8680
   Designated port id is 128.3, designated path cost 0
   Timers: message age 0, forward delay 0, hold 0
   Number of transitions to forwarding state: 1
   Link type is point-to-point by default
   BPDU: sent 6066, received 0

 Port 10 (GigabitEthernet1/0/10) of VLAN0010 is designated forwarding
   Port path cost 4, Port priority 128, Port Identifier 128.10.
   Designated root has priority 32778, address 00fe.c8d3.8680
   Designated bridge has priority 32778, address 00fe.c8d3.8680
   Designated port id is 128.10, designated path cost 0
   Timers: message age 0, forward delay 0, hold 0
   Number of transitions to forwarding state: 1
   The port is in the portfast mode by portfast trunk configuration
   Link type is point-to-point by default
   BPDU: sent 6063, received 0

 Port 11 (GigabitEthernet1/0/11) of VLAN0010 is designated forwarding
```

Port path cost 4, Port priority 128, Port Identifier 128.11.
Designated root has priority 32778, address 00fe.c8d3.8680
Designated bridge has priority 32778, address 00fe.c8d3.8680
Designated port id is 128.11, designated path cost 0
Timers: message age 0, forward delay 0, hold 0
Number of transitions to forwarding state: 1
Link type is point-to-point by default
BPDU: sent 6066, received 0

Port 13 (GigabitEthernet1/0/13) of VLAN0010 is designated forwarding
Port path cost 4, Port priority 128, Port Identifier 128.13.
Designated root has priority 32778, address 00fe.c8d3.8680
Designated bridge has priority 32778, address 00fe.c8d3.8680
Designated port id is 128.13, designated path cost 0
Timers: message age 0, forward delay 0, hold 0
Number of transitions to forwarding state: 1
Link type is point-to-point by default
BPDU: sent 6066, received 3

Port 14 (GigabitEthernet1/0/14) of VLAN0010 is designated forwarding
Port path cost 4, Port priority 128, Port Identifier 128.14.
Designated root has priority 32778, address 00fe.c8d3.8680
Designated bridge has priority 32778, address 00fe.c8d3.8680
Designated port id is 128.14, designated path cost 0
Timers: message age 0, forward delay 0, hold 0
Number of transitions to forwarding state: 1
Link type is point-to-point by default
BPDU: sent 6066, received 3

Port 15 (GigabitEthernet1/0/15) of VLAN0010 is designated forwarding
Port path cost 4, Port priority 128, Port Identifier 128.15.
Designated root has priority 32778, address 00fe.c8d3.8680
Designated bridge has priority 32778, address 00fe.c8d3.8680
Designated port id is 128.15, designated path cost 0
Timers: message age 0, forward delay 0, hold 0
Number of transitions to forwarding state: 1
Link type is point-to-point by default
BPDU: sent 6067, received 0

Port 16 (GigabitEthernet1/0/16) of VLAN0010 is designated forwarding
Port path cost 4, Port priority 128, Port Identifier 128.16.
Designated root has priority 32778, address 00fe.c8d3.8680
Designated bridge has priority 32778, address 00fe.c8d3.8680
Designated port id is 128.16, designated path cost 0
Timers: message age 0, forward delay 0, hold 0
Number of transitions to forwarding state: 1
Link type is point-to-point by default
BPDU: sent 6067, received 0

Port 35 (GigabitEthernet1/0/35) of VLAN0010 is designated forwarding
Port path cost 4, Port priority 128, Port Identifier 128.35.
Designated root has priority 32778, address 00fe.c8d3.8680
Designated bridge has priority 32778, address 00fe.c8d3.8680
Designated port id is 128.35, designated path cost 0
Timers: message age 0, forward delay 0, hold 0
Number of transitions to forwarding state: 1
Link type is point-to-point by default
BPDU: sent 6067, received 0

この出力は、インターフェイスGigabitEthernet1/0/35に接続されたデバイスから最後のトポロジ変更が発生したことを示しています。次に、このデバイスから同じshow spanning-tree detailコマンドを発行して、問題の追跡を試みます。TCNを生成するこのスイッチがPCまたはエンドポイントだけに接続されている場合は、これらのポートでSTP PortFastが有効になっていることを確認します。STP PortFast が有効であれば、ポートの状態が遷移したときに STP TCN が抑制されます。

STP の情報と、ネットワーク インターフェイス カード（NIC）に関連するリンク遷移のトラブルシューティングを行う方法については、次のドキュメントを参照してください。

- PortFast と他のコマンドを使用したワークステーションの接続始動遅延の修復
- 高速スパニングツリープロトコル（802.1w）について
- STP の問題点と関連設計の考慮事項

4. ブロックされたポートの切断

Fast EtherChannel（FEC）（ポートチャネリング）のロード バランシング特性が原因で、FEC 問題が HSRP と STP 両方の問題の一因になる場合があります。STPまたはHSRPのトラブルシューティングを行う際、FEC接続の設定を削除できます。設定の変更を行った後、両方のスイッチでshow spanning-tree blockedportsコマンドを発行します。少なくとも一方のポートが、接続の片側でブロッキングを開始するようにします。

Fast EtherChannel については、次のドキュメントを参照してください。

- CatalystスイッチでのEtherChannelのロードバランシングと冗長性について
- EtherChannel の設定

5. ブロードキャストの抑制

ブロードキャスト ストームの影響が軽減されるようにするには、ブロードキャストの抑制を有効にします。ブロードキャスト ストームは、STP ループの主な副作用の 1 つです。コマンド出力例を挙げます。

```
L2Switch_1#show run interface TenGigabitEthernet1/1/5
Building configuration...

Current configuration : 279 bytes
!
interface TenGigabitEthernet1/1/5
 switchport trunk allowed vlan 300-309
 switchport mode trunk
 storm-control broadcast level 30.00
 storm-control multicast level 30.00
 storm-control unicast level 30.00
 spanning-tree guard root
end
```

```
L2Switch_1#show storm-control broadcast
Key: U - Unicast, B - Broadcast, M - Multicast
Interface  Filter State   Upper       Lower       Current     Action     Type
---------  -------------  ----------  ----------  ----------  ---------  ----
Te1/1/5    Forwarding        30.00%      30.00%       0.00%  None       B
Te1/1/7    Link Down         30.00%      30.00%       0.00%  None       B
Te1/1/8    Forwarding        10.00%      10.00%       0.00%  None       B

L2Switch_1#show storm-control multicast
Key: U - Unicast, B - Broadcast, M - Multicast
Interface  Filter State   Upper       Lower       Current     Action     Type
---------  -------------  ----------  ----------  ----------  ---------  ----
Te1/1/5    Forwarding        30.00%      30.00%       0.00%  None       M
Te1/1/7    Link Down         30.00%      30.00%       0.00%  None       M
```

6. コンソールおよび Telnet アクセス

スイッチへのコンソール トラフィックまたは Telnet トラフィックが停滞し、STP ループの発生時に問題のデバイスを適切に追跡できない場合があります。ネットワークを強制的に即時復旧するには、冗長物理リンクをすべて削除します。新しい非冗長トポロジで STP が再コンバージされるようになってから、一度に 1 つずつ冗長リンクを再接続します。特定のセグメントを追加した後で STP ループが再び発生すれば、問題のデバイスがどれであるかがわかります。

7. スパニングツリーの機能：Portfast、UplinkFast、およびBackboneFast

PortFast、UplinkFast、および BackboneFast が適切に設定されていることを確認します。STP 問題のトラブルシューティングを行う際には、拡張 STP (UplinkFast と BackboneFast) をすべて無効にします。さらに、STP PortFast が有効になっているのは、非ブリッジング ホストに直接接続されているポートだけであることを確認します。非ブリッジング ホストには、ユーザ ワークステーションやブリッジ グループを持たないルータがあります。ハブや他のスイッチに接続されているポートでは、PortFast を有効にしないでください。これらの機能の理解と設定に役立つドキュメントを次に示します。

スパニングツリーPortFast、BPDUガード、BPDUフィルタ、UplinkFast、BackboneFast、およびループガードの設定

UplinkFast機能の理解と設定

8. BPDU ガード

PortFast の BPDU ガードを有効にすると、PortFast 対応の非トランキング ポートで BPDU が受信されたときに、そのポートが errdisable 状態に移行します。この機能は、PortFast が正しく設定されていないポートを検出するのに役立ちます。また、デバイスがパケットを反映する場所、またはネットワークにSTP BPDUを挿入する場所も検出します。STP問題のトラブルシューティングを行う際に、この機能を有効にすると、STPの問題を切り分けるのに役立ちます。

```
L2Switch_1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
L2Switch_1(config)#spanning-tree portfast bpduguard
L2Switch_1(config)#end
```

9. VTP プルーニング

ネットワークで VTP プルーニングが有効にされていると、HSRP グループのデバイスがアクティブになる場合があります。これにより、ゲートウェイで IP 競合が発生し、トラフィックの問題となります。いずれかの HSRP グループの VLAN が、ネットワーク内で VTP によりプルーニングされていないことを確認してください。

F.分割攻略方式

HSRP 問題を切り分けたり解決したりする試みがすべて失敗した場合は、次のアプローチとして「分割統治」法を利用します。この方法を使用すると、ネットワークと、ネットワークを構成するコンポーネントを切り離すことができます。分割統治には、次に列挙するようなガイドラインがあります。

注：このリストには、このドキュメントの他のセクションで説明したガイドラインが含まれています。

- HSRP 用テスト VLAN と、HSRP ルータを使用してスイッチングする隔離された VLAN を作成します。
- すべての冗長ポートの接続を解除します。
- FEC ポートを単一接続ポートに分割します。
- HSRP グループのメンバを削減して 2 メンバだけにします。
- トランク ポートをプルーニングして、それらのポートから必要な VLAN だけが伝搬されるようにします。
- 問題がなくなるまで、ネットワーク内で接続されているスイッチの接続を解除します。

既知の問題

Cisco 2620/2621、ファストイーサネットを搭載したCisco 3600使用時のHSRP状態のフラッピング/不安定性

この問題は、ネットワーク接続の途絶、または優先度の高い HSRP ルータのネットワークへの追加により、ファスト イーサネット インターフェイスで発生する可能性があります。HSRP 状態がアクティブからスピークに変わると、ルータはインターフェイスの MAC アドレス フィルタから HSRP MAC アドレスを削除するために、そのインターフェイスをリセットします。この問題

が発生するのは、Cisco 2600、3600、および 7500 のファスト イーサネット インターフェイスで使用される特定のハードウェアに限られます。ルータ インターフェイスがリセットされるとファスト イーサネット インターフェイスのリンク状態が変わり、スイッチがその変更を検出します。スイッチで STP が動作している場合、その変更により STP の移行が発生します。STP がポートを forwarding 状態に遷移させるには 30 秒かかります。この時間はデフォルトの転送遅延時間である 15 秒の 2 倍です。同時に、HSRP ホールド タイムの 10 秒が経過すると、スピーク状態のルータが standby 状態に遷移します。STP はまだフォワーディング状態でないため、アクティブ ルータからの HSRP hello メッセージは受信されません。そのため、およそ 10 秒後にスタンバイ ルータがアクティブになります。この時点で両方のルータが active になっています。STP ポートがフォワーディング状態になると、プライオリティの低い方のルータがアクティブからスピークに変わり、プロセス全体が繰り返されます。

Platform	説明	Cisco Bug ID	修正	回避策
Cisco 2620/2621	HSRP を設定したときやケーブルが抜けたときに、ファースト イーサネット インターフェイスがフラップし始める。		ソフトウェア アップグレード。リビジョンの詳細は不具合情報を参照してください。	接続スイッチ ポートでスパニング ツリー PortFast を有効にする。
Cisco 2620/2621	2600 のファスト イーサネットで HSRP 状態のフラッピングが発生している。		Cisco IOS ソフトウェア リリース 12.1.3	接続スイッチ ポートでスパニング ツリー PortFast を有効にする。
NM-1FE-TX[1] を搭載した Cisco 3600	2600 および 3600 のファースト イーサネットで HSRP 状態のフラッピングが発生しています。		Cisco IOS ソフトウェア リリース 12.1.3	接続スイッチ ポートでスパニング ツリー PortFast を有効にする。
ファスト イーサネット インターフェイスを搭載した Cisco 4500	4500 のファスト イーサネットで HSRP 状態のフラッピングが発生している。	Cisco Bug ID CSCds16055	Cisco IOS ソフトウェア リリース 12.1.5	接続スイッチ ポートでスパニング ツリー PortFast を有効にする。

1NM-1FE-TX は、1 ポートのファスト イーサネット (10/100BASE-TX インターフェイス) ネットワーク モジュールです。

STP 転送遅延がデフォルトの HSRP ホールド タイムの半分よりも短くなるように HSRP タイマーを調整するという、別の回避策もあります。デフォルトでは、STP 転送遅延は 15 秒、HSRP ホールド タイムは 10 秒になっています。

HSRP プロセスで track コマンドを使用する場合、HSRP フラップを回避するために特定のデクリメント値を使用することをお勧めします。

track コマンドを使用する場合の、HSRP アクティブ ルータの設定例を次に示します。

```
standby 1 ip 10.0.0.1
standby 1 priority 105
standby 1 preempt delay minimum 60
standby 1 name TEST
standby 1 track <object> decrement 15
```

ここで、15はオブジェクトがフラップしたときの減少値です。trackコマンドの詳細については、『HSRPv2の設定例』のドキュメント「trackオプション」に移動してください。

関連情報

- キャンパスLAN Catalystスイッチ – アクセス
- LAN スイッチング
- テクニカル サポートとドキュメント - Cisco Systems

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。