高可用性の概要

Cisco HA（ハイアベイラビリティ）により、ネットワークのどの場所でも発生する障害からの高速回復が可能になり、ネットワーク規模での保護が実現されます。Cisco HA を使用すると、ネットワークのハードウェアおよびソフトウェアが連携し、中断からの高速回復が可能となるため、ユーザおよびネットワーク アプリケーションへの障害の透過性が保証されます。

Cisco Catalyst 8500 シリーズ エッジ プラットフォームの独自のハードウェアおよびソフトウェアアーキテクチャは、あらゆるネットワークイベント時にルータのアップタイムを最大化するように設計されているため、すべてのネットワークシナリオで最大アップタイムと復元力が実現します。

このガイドでは、Cisco 8500 シリーズ Catalyst エッジプラットフォーム独自のハイアベイラビリティの特徴について説明します。このマニュアルには、ハイアベイラビリティに関する総合的な説明は記載されていません。また、Cisco 8500 シリーズ Catalyst エッジプラットフォーム上と同様に設定され、実装されている他の Cisco ルータで使用できるハイアベイラビリティ機能の説明も掲載していません。この章のほかに、Cisco IOS 機能に関する資料およびマニュアルを参照して、複数のシスコのプラットフォームで使用でき、Cisco 8500 シリーズ Catalyst エッジプラットフォーム上でも同様に動作するハイアベイラビリティ機能に関する情報を入手してください。

この章で紹介する機能情報の入手方法

ご使用のソフトウェア リリースで、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェアリリースに対応したリリースノートを参照してください。

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。

目次

ここでは、Cisco 8500 シリーズ Catalyst エッジプラットフォーム上のさまざまなハイアベイラビリティの特徴について説明します。内容は、次のとおりです。

Cisco 8500 シリーズ Catalyst エッジプラットフォームのソフトウェア冗長性

この項では、次のトピックについて取り上げます。

ソフトウェア冗長性の概要

Cisco 8500 シリーズ Catalyst エッジプラットフォームでは、IOS はオペレーティングシステム内の多くのプロセスの 1 つとして実行されます。この点は、Cisco IOS 内ですべてのプロセスが実行されている従来の Cisco IOS とは異なります。Cisco 8500 シリーズ Catalyst エッジプラットフォームのプロセスとしての IOS の詳細については、「IOS as a Process」セクション（2 〜 7 ページ）を参照してください。

このアーキテクチャにより、Cisco IOS ソフトウェアを稼働するその他のプラットフォームでは使用できないソフトウェアの冗長性が実現します。スタンバイ IOS プロセスを、アクティブ IOS プロセスと同じ RP 上で使用することができます。このスタンバイ IOS プロセスは、IOS に障害が発生した場合に切り替えることができます。

Cisco 8500 シリーズ Catalyst エッジプラットフォームでは、2 番目の IOS プロセスはスタンバイルートプロセッサでのみ実行できます。

2 つの Cisco IOS プロセスの設定

Cisco 8500 シリーズ Catalyst エッジプラットフォームでは、Cisco IOS が多くのプロセスの 1 つとして実行されます。このアーキテクチャは、ソフトウェアの冗長性の機会をサポートします。具体的には、スタンバイ Cisco IOS プロセスをアクティブ Cisco IOS プロセスと同じルートプロセッサで使用することができます。Cisco IOS で障害が発生した場合、システムはスタンバイ Cisco IOS プロセスに切り替わります。

手順の概要

1. enable
2. **configure terminal**
3. redundancy

4. mode SSO
5. **exit**
6. reload

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	enable 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	redundancy 例： `Router(config)# redundancy`	冗長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	mode SSO 例： `Router(config)# mode SSO`	SSO を設定します。このコマンドが入力されると、冗長スーパーバイザエンジンがリロードされ、SSO モードで動作を開始します。

ステップ 5	**exit**
	例：
	`Router(config)# exit`
	例：
	`Router #`
		コンフィギュレーションモードを終了して、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	reload 例： `Router # reload`	IOS をリロードします。

例

```
Router# configure terminal
Router(config)# redundancy
Router(config)# mode SSO
Router(config)# exit
Router# reload
```

ステートフル スイッチオーバー

Cisco 8500 シリーズ Catalyst エッジプラットフォームでは、ステートフル スイッチオーバー（SSO）を使用して、2 番目の IOS プロセスを有効にすることができます。

SSO は、NSF と連携すると、さらに威力を発揮します。SSO により、デュアル IOS プロセスは常にステートを維持できます。また、スイッチオーバーが発生すると、ノンストップ フォワーディングによってスイッチオーバーがシームレスに実行されます。

NSF/SSO の詳細については、『Cisco Nonstop Forwarding』マニュアルを参照してください。

SSO 認識プロトコルおよびアプリケーション

SSO によってサポートされるライン プロトコルとアプリケーションは、SSO 認識である必要があります。機能やプロトコルが、RP スイッチオーバーを経ても、一部または全体が問題なく動作し続ける場合、その機能やプロトコルは SSO 認識です。SSO 認識プロトコルおよびアプリケーションのステート情報をアクティブからスタンバイに同期することにより、これらのプロトコルおよびアプリケーションでの SSO が実現されます。

SSO 非認識のプロトコルおよびアプリケーションの場合、ステートをダイナミックに作成しても、スイッチオーバー時に失われるため、スイッチオーバーの際に再初期化と再起動が必要になります。

ルータ上のどのプロトコルが SSO 対応であるかを確認するには、次のコマンドを使用します。**show redundancy client** または **show redundancy history**

IPsec フェールオーバー

IPSec フェールオーバーは、カスタマーの IPsec ネットワークの合計稼働時間（または可用性）を増やす機能です。従来、これは元の（アクティブな）ルータに加えて冗長（スタンバイ）ルータを使用することで実現されています。アクティブ ルータが何らかの理由で使用できなくなると、スタンバイ ルータは、IKE および IPsec の処理を引き継ぎます。IPSec フェールオーバーは、ステートレス フェールオーバーおよびステートフル フェールオーバーの 2 種類のカテゴリに分類されます。

Cisco 8500 シリーズ Catalyst エッジプラットフォームの IPsec は、ステートレス フェールオーバーのみをサポートします。ステートレス フェールオーバーは、ホット スタンバイ ルータ プロトコル（HSRP）のようなプロトコルを使用して、プライマリからセカンダリへのカットオーバーを行い、さらにアクティブおよびスタンバイの VPN ゲートウェイを許可して、共通の仮想 IP アドレスを共有することができます。

双方向フォワーディング検出

双方向フォワーディング検出（BFD）は、すべてのメディアタイプ、カプセル化、トポロジ、およびルーティングプロトコルのために短時間での転送パス障害検出を提供するために設計された検出プロトコルです。高速転送パス障害検出に加えて、BFDはネットワーク管理者に整合性のある障害検出方法を提供します。ネットワーク管理者はBFDを使用することで、さまざまなルーティングプロトコルのHELLOメカニズムにより、変動速度ではなく一定速度で転送パス障害を検出できるため、ネットワークプロファイリングおよびプランニングが容易になります。また、再収束時間の整合性が保たれ、予測可能になります。

Cisco 8500シリーズCatalystエッジプラットフォームでは、IPv4スタティックルート用のBFDとボーダー ゲートウェイ プロトコル（BGP）用のBFDがサポートされます。

BFDの詳細については、『Bidirectional Forwarding Detection』マニュアルを参照してください。

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。