

ハイ アベイラビリティ キャンパス リカバリ分析 設計ガイド

Cisco Validated Design

May 21, 2008

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-15550-01-J

【注意】シスコ製品をご使用になる前に、安全上の注意（www.cisco.com/jp/go/safety_warning/）をご確認ください。

本書は、米国シスコシステムズ発行ドキュメントの参考和訳です。
米国サイト掲載ドキュメントとの差異が生じる場合があるため、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。
また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

Cisco Validated Design

Cisco Validated Design Program は、お客様による、より迅速で、信頼性の高い、予測可能な展開を実現するために、設計、テスト、および文書化されたシステムとソリューションから構成されています。詳細については、www.cisco.com/go/validateddesigns を参照してください。

このマニュアルに記載されている設計、仕様、表現、情報、および推奨事項（総称して「設計」）はすべて、現状のままで提供されています。シスコシステムズおよびその代理店は、商品性や特定の目的への準拠性、権利を侵害しないことに関する、または取り扱い、使用、または取引によって発生する、一切の保証の責任を負わないものとします。いかなる場合においても、シスコシステムズおよびその代理店は、設計の使用または設計を使用できないことによって起こる制約、利益の損失、データの損傷など間接的で偶発的に起こる特殊な損害のあらゆる可能性がシスコシステムズまたは代理店に知らされていても、それらに対する責任を一切負いかねます。

設計は予告なしに変更されることがありえます。設計の使用は、すべてユーザ側の責任になります。設計はシスコシステムズおよびその代理店またはパートナーの技術的または専門的なアドバイスを受けたことを意味するものではありません。ユーザは設計を導入する前に、自社のテクニカル アドバイザに相談する必要があります。シスコシステムズによってテストされていない要因により、異なる結果が生まれることがあります。

CCDE, CCENT, Cisco Eos, Cisco StadiumVision, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn is a service mark; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0803R)

ハイ アベイラビリティ キャンパス リカバリ分析設計ガイド
© 2008 Cisco Systems, Inc. All rights reserved.

はじめに　1-1
対象読者　1-1
マニュアルの目的　1-2
概要　1-2
コンバージェンス分析の概要　1-2
テスト時のキャンパス設計　1-3
テストの手順　1-4
テスト ベッドの構成　1-5
テスト トラフィック　1-5
コンバージェンス時間の確認方法　1-7
レイヤ 3 コアのコンバージェンス — 結果および分析　1-7
キャンパス コアについて　1-7
イコール コスト パスのレイヤ 3 キャンパス設計の利点　1-8
レイヤ 3 コアのコンバージェンス結果 — EIGRP および OSPF　1-9
障害の分析　1-9
復旧の分析　1-11
レイヤ 3 ディストリビューションのコンバージェンスを伴うレイヤ 2 アクセス — 結果および分析
1-12
テスト構成の概要　1-12
ディストリビューション ビルディング ブロックの説明　1-14
構成 1 の結果 — HSRP、EIGRP（PVST+ 使用）　1-16
障害の分析　1-16
復旧の分析　1-20
構成 2 の結果 — HSRP、EIGRP（Rapid-PVST+ 使用）　1-23
障害の分析　1-23
復旧の分析　1-24
構成 3 の結果 — HSRP、OSPF（Rapid-PVST+ 使用）　1-26
障害の分析　1-26
復旧の分析　1-28
構成 4 の結果 — GLBP、EIGRP（Rapid-PVST+ 使用）　1-29
障害の分析　1-29
復旧の分析　1-30
構成 5 の結果 — GLBP、EIGRP、Rapid-PVST+（レイヤ 2 ループ使用）　1-32
障害の分析　1-32
復旧の分析　1-33
レイヤ 3 ディストリビューションのコンバージェンスを伴うレイヤ 3 ルーテッド アクセス — 結果およ
び分析　1-35
レイヤ 3 ルーテッド アクセスの概要　1-35
音声 VLAN 102、103、および 149　1-35
EIGRP の結果　1-36
EIGRP 障害結果　1-36
EIGRP の復旧結果　1-38
OSPF の結果　1-39

OSPF の障害結果　1-39
OSPF の復旧結果　1-41
テスト構成　1-43
コア スイッチ構成　1-43
コア スイッチ構成（EIGRP）　1-43
コア スイッチ構成（OSPF）　1-45
レイヤ 2 アクセスおよびディストリビューション ブロックのスイッチ構成　1-46
ディストリビューション 1 ― ルート ブリッジおよび HSRP プライマリ　1-47
ディストリビューション 2 ― セカンダリ ルート ブリッジおよび HSRP スタンバイ　1-51
IOS アクセス スイッチ（4507/SupII+）　1-55
CatOS アクセス スイッチ（6500/Sup2）　1-56
レイヤ 3 アクセスおよびディストリビューション ブロックのスイッチ構成　1-57
ディストリビューション ノード EIGRP　1-57
アクセス ノード EIGRP（冗長スーパーバイザ）　1-60
ディストリビューション ノード OSPF　1-61
アクセス ノード OSPF（冗長スーパーバイザ）　1-63



ハイ アベイラビリティ キャンパス リカバリ分析

はじめに

小規模および大規模エンタープライズ キャンパスで音声、ビデオ、ワイヤレス、およびミッションクリティカル データといったさまざまなアプリケーション向けのビジネス ソリューションをサポートするには、可用性が高くセキュアでインテリジェントなネットワーク インフラストラクチャが必要となります。こうした信頼性のあるネットワーク インフラストラクチャを実現するには、キャンパスを構成するシステム全体で、コンポーネントの障害による中断を最小限にしなければなりません。可用性の高いセキュアなキャンパス ネットワークの設計、アップグレード、および運用のためには、コンポーネントが（事前の計画による、または障害による）停止から復旧するシステムの仕組みを理解し、実際に停止が発生した場合の動作について把握することが重要です。

このマニュアルは、次の URL から入手できる『*Designing a Campus Network for High Availability*』と合わせてご覧ください。

http://www.cisco.com/en/US/docs/solutions/Enterprise/Campus/HA_campus_DG/hacampusdg_book.html

このマニュアルでは、上記の文書で説明されているキャンパス設計での障害復旧について分析しています。具体的な内容は次のとおりです。

- 概要（p.2）
- レイヤ 3 コアのコンバージェンス — 結果および分析（p.7）
- レイヤ 3 ディストリビューションのコンバージェンスを伴うレイヤ 2 アクセス — 結果および分析（p.12）
- レイヤ 3 ディストリビューションのコンバージェンスを伴うレイヤ 3 ルーテッド アクセス — 結果および分析（p.35）
- テスト構成（p.43）

対象読者

このマニュアルは、キャンパス ネットワークの設計を担当するシスコシステムズまたは企業のエンジニアを対象としています。このマニュアルは、システムの運用を担当する方などが既存の実働キャンパス システムで予期されるコンバージェンス動作を理解する場合にも役立ちます。

Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Copyright © 2008 Cisco Systems, Inc. All rights reserved.

マニュアルの目的

このマニュアルでは、推奨される階層型キャンパス設計において、主要コンポーネントに障害が発生した場合のデータ フローの復旧時間を測定し、さらに分析を行っています。このマニュアルの目的は、キャンパス ネットワークを構築したりアップグレードしたりした場合に、その設計の妥当性について参照できる基準を提供することです。

概要

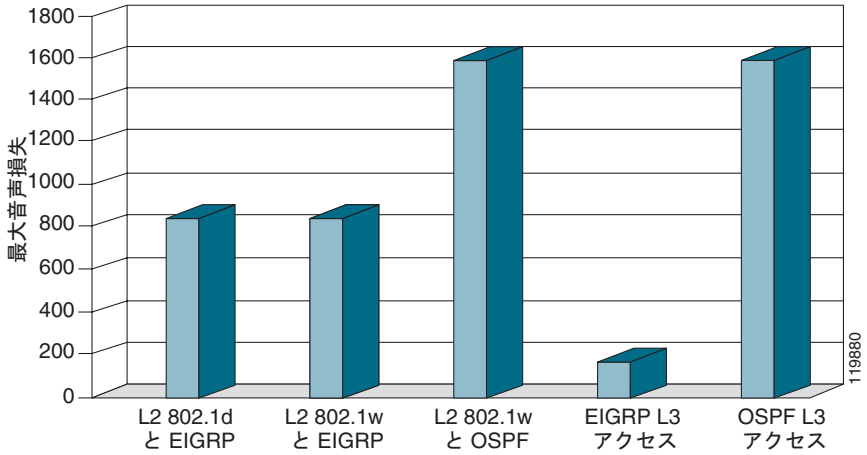
ここでの内容は、次のとおりです。

- コンバージェンス分析の概要（p.2）
- テスト時のキャンパス設計（p.3）
- テストの手順（p.4）
- テスト ベッドの構成（p.5）
- テスト トラフィック（p.5）
- コンバージェンス時間の確認方法（p.7）

コンバージェンス分析の概要

Enhanced Interior Gateway Routing Protocol（EIGRP）を採用したエンドツーエンド レイヤ 3 設計では、単一のコンポーネント、リンク、またはノードに障害が発生した場合、最も効率的に障害を復旧できます。図 1 に、単一コンポーネント障害をテストした際に記録した最長の復旧時間を示します。

図 1　　音声損失の最大期間



テスト結果によると、レイヤ 3 アクセスと EIGRP を実行するキャンパスの場合、いずれの単一コンポーネント障害についても G.711 音声トラフィックの最大損失は 200 ミリ秒 を下回ることが示されました。

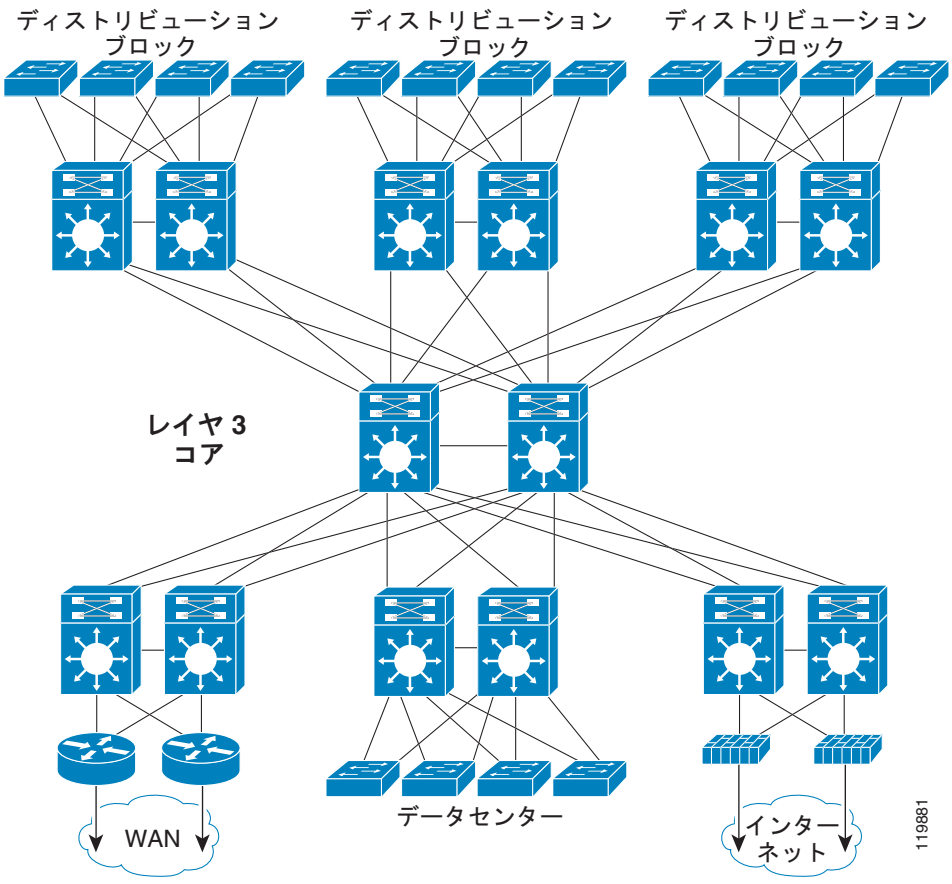
従来のレイヤ 2 アクセス設計で Hot Standby Routing Protocol（HSRP）/Gateway Load Balancing Protocol（GLBP）で Sub-Sec（1 秒未満）のタイマーを使用するケースでは、どのコンポーネント障害の場合でもコンバージェンス時間は 1 秒未満であることが確認されました。この復旧時間は IP テレフォニーの許容範囲内に十分収まっており、エンド ユーザが障害時に認識する音声品質への影響はほとんどありません。

（注） 前述のシナリオでは、スーパーバイザまたはソフトウェアのクラッシュなどによってアクセス スイッチの障害が引き起こされた場合、障害のあるアクセス スイッチに接続されているすべてのデバイスの音声とデータの損失が拡大しました。シスコでは、アクセス スイッチの障害をできる限り発生させないようにするために、各アクセス スイッチに Stateful Switchover（SSO）や Nonstop Forwarding（NSF）/SSO などの冗長スーパーバイザ構成を利用するか、または冗長スタック型構成を導入することをお勧めします。冗長スーパーバイザのコンバージェンス分析の結果は含まれていません。

テスト時のキャンパス設計

テスト用の設計は、『*Designing a Campus Network for High Availability*』で概説されている階層型設計の推奨事項に基づいて決定されました。テスト対象のすべての設計にはレイヤ 3 ルーテッド コア（routed core）が使用され、これに他のアーキテクチャ ビルディング ブロックが接続されています（図 2 を参照）。

図 2　　キャンパス設計



この構造化階層型モデルでは、次の基本的な 4 種類のディストリビューション ビルディング ブロックのテストを行いました。

- レイヤ 2 アクセス（PVST+ を使用）
- レイヤ 2 アクセス（Rapid PVST+ を使用）
- レイヤ 3 アクセス（エンドツーエンド EIGRP）

- レイヤ 3 アクセス（エンドツーエンド OSPF）

これら 4 種類のディストリビューション設計のそれぞれについて、コンポーネント障害テストとコンポーネント復旧テストの両方を実施しました。

このほか、基本 L2 ディストリビューション ブロック設計の違いを比較するためにさらに 2 つのテストを行いました。最初は L2 アクセス（Rapid PVST+ を使用）ディストリビューション ブロック設計を使用し、冗長デフォルト ゲートウェイ プロトコルとして GLBP と HSRP を比較しました。次に Rapid PVST+ ディストリビューション ブロック設計の復旧について、スパニング ツリー ループのある場合とない場合を比較しました。

（注） それぞれの設計の実装に関する詳細については、『*Designing a Campus Network for High Availability*』を参照してください。

測定結果の分析を、次の 3 つの項で説明します。

- レイヤ 3 コアの障害の分析
- レイヤ 2 ディストリビューション ブロック内の障害の分析
- レイヤ 3 を実装したエッジ ディストリビューション ブロックの障害の分析

各テスト ケースはそれぞれ、キャンパス全体を通過するメッシュ型のエンドツーエンド データ フローを使用して行いましたが、各テスト ケースの分析は個別に行っています。階層型設計の大きな利点の 1 つに、障害ドメインの分離（あるドメインで発生した障害が他のドメインに影響を及ぼさないこと）があります。例えばネットワークのコア内でノードまたはリンクの障害が発生した場合、ディストリビューション内の設計がどのようなものであっても、生じるコンバージェンス動作に違いはなく、ビジネス アプリケーションへの影響にも違いがありません。同様に、ディストリビューション ブロック内の障害はコアに影響を及ぼさないので、コアドメインとは切り離して障害調査することができます。

（注） 障害イベントを他のドメインから切り離し、障害の影響を当該ドメイン内に封じ込める機能は、『*Designing a Campus Network for High Availability*』に記載の階層型設計においてのみ当てはまります。

テストの手順

テスト対象のネットワーク、トラフィック、およびシステムの構成は、実際のお客様のトラフィック フローと可用性の要件に可能なかぎり近づけました。本テスト構成は、実稼働環境でのシスコのベスト プラクティスの有効性を実証することを目的に準備されました。

テストの前提条件は次のとおりです。

- キャンパス ネットワークが VoIP およびストリーミング ビデオをサポートしている
- キャンパス ネットワークがマルチキャスト トラフィックをサポートしている
- キャンパスネットワークがワイヤレスをサポートしている
- キャンパス ネットワークがトランザクション アプリケーションおよびバルク データ アプリケーションをサポートしている

テスト ベッドの構成

障害復旧テストで使用したテスト ベッドは、レイヤ 3 ルーテッド コアおよびそれに接続されたディストリビューション ブロックとサーバ ファーム ブロックで構成されています。コア スイッチおよびディストリビューション スイッチには Supervisor 720a エンジン搭載の Cisco Catalyst 6500 を使用しました。アクセス レイヤはディストリビューション レイヤにデュアル接続された 39 台のスイッチで構成しました。テスト時の構成は次のとおりです。

- コア スイッチ — Sup720（Native IOS–12.2(17b)SXA）搭載の 6500 × 2
- サーバ ファーム ディストリビューション — Sup2/MSFC2（Native IOS–12.1(13)E10）搭載の 6500 × 2
- サーバ ファーム アクセス スイッチ — Sup1A（CatOS–8.3(1)）搭載の 6500 × 2
- コア スイッチ — Sup720（Native IOS–12.2(17b)SXA）搭載の 6500 × 2
- アクセス スイッチ
  - 2950（IOS–12.1(19)EA1a）× 1
  - 3550（IOS–12.1(19)EA1）× 1
  - 3750 [IOS–12.1(19)EA1] × 1
  - SupII+（IOS–12.1(20)EW）搭載の 4006 × 1
  - SupIV（IOS–12.1(20)EW）搭載の 4507 × 1
  - Sup1A（CatOS–8.3(1)）搭載の 6500 × 1
  - Sup2/MSFC2（IOS–12.1(13)E10）搭載の 6500 × 1
  - 3550（IOS–12.1(19)EA1）× 32。各アクセス スイッチは次の 3 つの VLAN をループのないトポロジで設定
- 音声専用 VLAN
- データ専用 VLAN
- 固有のネイティブ アップリンク VLAN

テスト トラフィック

テスト中のネットワークのトラフィック負荷の生成と、各障害イベントおよび復旧イベントの影響に関する統計情報の収集には、180 台の Chariot エンドポイント サーバを使用しました。

（注） Chariot の詳細については、http://www.netiq.com/products/chr/default.asp を参照してください。

Chariot エンドポイント サーバは、シスコのお客様の実ネットワークの調査に基づき、エンタープライズ アプリケーションのトラフィック フローの混成を生成するように設定しました。

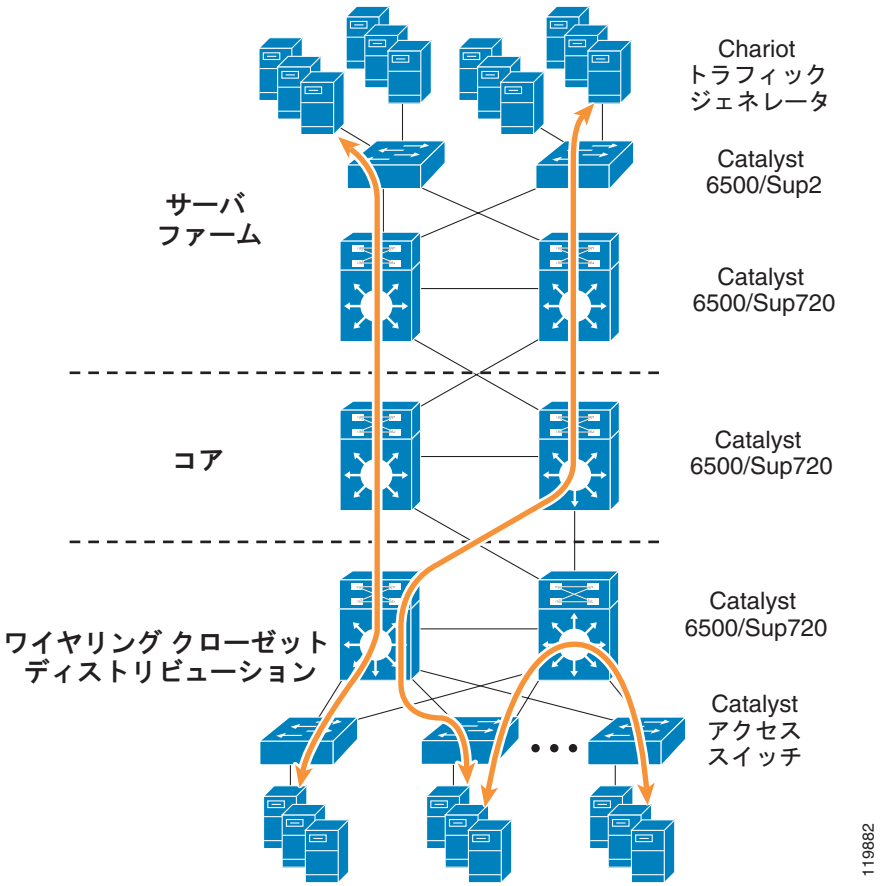
各エンドポイント サーバは 39 台のアクセス スイッチおよびデータセンター スイッチに接続し、次のユニキャスト トラフィックを生成するように設定しました。

- G.711 音声コール — Real-Time Protocol（RTP）ストリーム
- コール制御、バルク データ（FTP）、ミッションクリティカル データ（HTTP、tn3270）、POP3、HTTP、DNS、および WINS をエミュレーションする TCP/UDP データ ストリーム タイプ × 94

すべてのトラフィックは『*Enterprise QoS Solution Reference Network Design Guide*』（http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/QoS_SRND/QoS-SRND-Book.html）の推奨事項に従ってマーキングされ、アップリンクおよびコア インフラストラクチャを輻輳させるのに十分なトラフィック負荷が生成されました。

トラフィック フローについては、トラフィックの大半がネットワーク コアを使用するデータセンターとアクセス レイヤ間を通過するように定義しました。またトラフィックフローのうち VoIP ストリームは、ディストリビューション スイッチを使用するアクセス スイッチ間を通過するように設定されました（図 3 を参照）。

図 3　　テスト ベッド（トラフィック フローを例示）



ユニキャスト トラフィックのほかに、各アクセス スイッチには 40 のマルチキャスト レシーバーを設定し、次の混合マルチキャスト ストリームを受信しました。

- 保留音（Music on Hold, MoH）ストリーム @64 kbps/50 pps（160 バイト ペイロード、RTP = PCMU）
- IPTV ビデオ ストリーム @1451 kbps（1460 バイト ペイロード、RTP = MPEG1）
- IPTV 音声ストリーム @93 kbps（1278 バイト ペイロード、RTP = MPEG2）
- NetMeeting ビデオ ストリーム @64 kbps（522 バイト ペイロード、RTP = H.261）
- NetMeeting 音声ストリーム @12 kbps（44 バイト ペイロード、RTP = G.723）
- NetMeeting 音声ストリーム @80 kbps（351 バイト ペイロード、RTP = G.729）
- Real Media ストリーム @300 kbps（431 バイト ペイロード、RTP = H.261）
- マルチキャスト FTP ストリーム @4000 kbps（4096 バイト ペイロード、RTP = JPEG）

すべてのマルチキャスト MoH は Express Forwarding（EF）としてマーキングされ、他のすべてのマルチキャスト トラフィックは Differentiated Services Code Point（DSCP; DiffServ コード ポイント）14（AF13）としてマーキングされています。

コンバージェンス時間の確認方法

障害イベントが実働ネットワークのアプリケーションと音声トラフィック フローに与える影響を理解するというテストの目的に合わせて、このマニュアルには実際の UDP および TCP テスト フローの測定に基づいたコンバージェンス結果が記載されています。障害ケースごとに記載されているコンバージェンス時間は、各テストの実行時のアクティブなすべての G.711 音声ストリームにおける *ワーストケース* パケット損失に基づいて測定しています。

（注） 標準の G.711 コーデックは、20 ミリ秒 に 1 パケットの一定レートで 1 秒間に 50 パケットを送信します。したがって、連続して「n」パケットを失った場合、（n × 20）ミリ秒の停止を意味します。

記載されているワーストケースの値は、テスト ケースをそれぞれ複数回繰り返して測定されたうちの最大値であり、平均コンバージェンス時間ではなく統計上の外れ値を表しています。ワーストケースの値を使用するのは、実稼働ネットワークにコンバージェンスが与える影響を評価する際によりコンサバティブな値を提供するためです。

各テスト ケースは最低 3 回、反復実施されました。ファイバ障害テストの場合、テスト ケースは次の 3 つです

- リンク両端のファイバの障害
- 1 つのファイバの障害（送信側）
- 1 つのファイバの障害（受信側）

ノード障害を引き起こす障害の場合、テスト ケースは次の 3 つです。

- 電源障害
- ソフトウェア（IOS/CatOS）の擬似クラッシュ
- スーパーバイザの擬似障害

さらに、これらアクセス スイッチにかかわるテスト ケースでは、上述の各 3 つのサブケースを複数回実行しました（アクセス スイッチのタイプごとに 1 回）。テスト対象のすべてのアクセス スイッチについては前述の一覧を参照してください。

音声損失の最大期間のほかに、すべての音声コールの MOS 値、ネットワーク ジッタ、および遅延を記録しました。

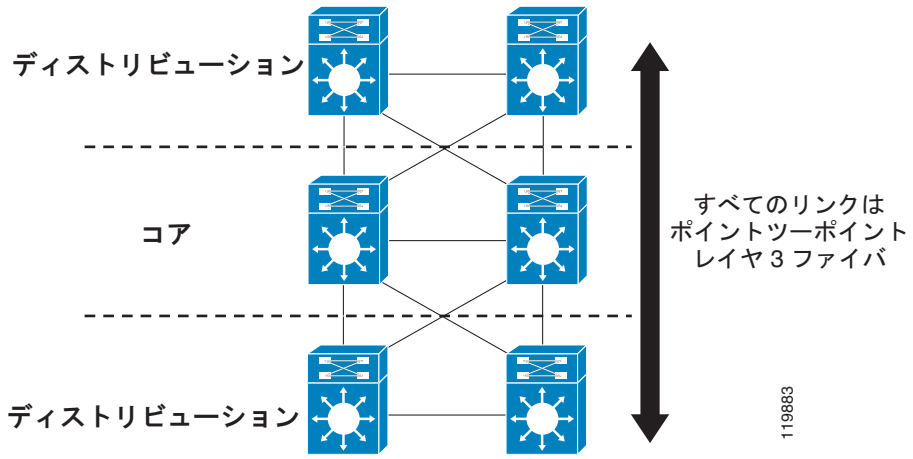
ネットワーク コンバージェンスがアクティブな TCP フローに及ぼす影響についても、テスト データを収集しました。すべてのテスト ケースで中断期間は十分短く、TCP セッションが失われることはありませんでした。ネットワーク コネクティビティ切断の場合は、トラフィック フローのスループット レートに一時的に影響しました。注目点として、「影響時間」つまり TCP フローが通常のスループット レートで通過しなかった時間が G.711 UDP フローの中断期間より長かったことが挙げられます。予測通り、コンバージェンス中のパケット損失によって TCP バックオフ アルゴリズムがトリガーされました。TCP フローが最適なスループットに復旧するための時間は、[パケット損失の期間 + TCP フロー リカバリに必要な時間] で求められます。

レイヤ 3 コアのコンバージェンス — 結果および分析

キャンパス コアについて

キャンパス コアは、他のすべての階層型ビルティング ブロック間に冗長高速接続を提供しています。最適かつ結果が予測可能なコンバージェンス動作を提供するには、ポイントツーポイントのレイヤ 3 ファイバ接続を使用する完全メッシュ型のコア設計が最適です（図 4 を参照）。

図 4　　コア トポロジ



テストが実施されたネットワーク コアは、Supervisor 720 を搭載した Cisco Catalyst 6500 のペアに加えて、各ディストリビューション スイッチとコア スイッチ間を冗長ポイントツーポイント 10 ギガビット イーサネット（10GigE）リンクで接続した構成です。2 つのコア スイッチはポイントツーポイント 10GigE ファイバで相互接続されています。ユニキャストだけの環境の場合、この冗長化リンクは不可欠なものではありませんが、キャンパス設計では依然として推奨される要素です。このリンクは、ある特定の構成でのマルチキャスト トラフィックの復旧に使用します。また、コア ノードがネットワークへのデフォルトまたは集約ルーティング情報の送信元に設定される場合にも必要です。

図 4 に示した、テスト トラフィックを伝送する 2 つのディストリビューション ブロックのほかに、ディストリビューション スイッチとバックエンド ルータのセットをさらにコアに接続し、キャンパスと企業 WAN の擬似的な接続を行いました。テスト ネットワークのこの部分にはテスト トラフィックが転送されないように設定し、キャンパスに新たにルートを追加する用途に限定しました。テストが実施されたキャンパスのルート数の総計は 3572 ルートでした。

```
Core-Switch-2# show ip route summary
IP routing table name is Default-IP-Routing-Table(0)

Route Source  Networks    Subnets     Overhead    Memory (bytes)
connected      1          10          704         1760
static        0           1           64          160
eigrp 100      1          3561        228224      569920
internal      5                                   5900
Total         7           3572        228992      577740
```

イコール コスト パスのレイヤ 3 キャンパス設計の利点

推奨されるキャンパス設計では、ディストリビューションとコア双方におけるすべてのノードは、ローカルに接続されたサブネットの宛先を除いたすべての宛先に対するイコール コスト パスのフォワーディング エントリを持ちます。これらの 2 つのイコール コスト パスは互いに独立しています。これは、リンクまたはノードの単一コンポーネント障害が発生した場合、生き残ったパスが有効なルートを提供できるという意味です。単一コンポーネント障害が発生した場合、この設計内のすべてのスイッチはネクストホップ障害から問題なく復旧し、障害を迂回することができます。

各ノードが 2 つのパスを持ち、リンク障害から復旧可能であり、アップストリーム デバイスは常に有効なパスを保持しているため、ダウンストリーム デバイスはアップストリームの障害に起因するルートの再計算を行う必要がありません。メッシュ型レイヤ 3 設計のアーキテクチャの利点

は、単一コンポーネント障害が発生した場合に、すべてのルート コンバージェンスはスイッチ内で常にローカルで行われ、間接的なリンクまたはノードの障害から復旧やルーティング プロトコルの検出メカニズムにまったく依存しないことです。

レイヤ 3 コア設計では、任意のディストリビューション スイッチ間を通過するトラフィックのコンバージェンス時間は、主としてディストリビューション スイッチにおけるリンク損失の検出に依存します。通常、GigE および 10GigE ファイバ上のリンク損失の検出は 802.3z および 802.3ae のリンク ネゴシエーション プロトコルの一部として実装されるリモート障害検出メカニズムを使用して行われます。

（注） 10GigE および GigE のリモート障害時の動作については、それぞれ IEEE 802.3ae および IEEE 802.3z 規格を参照してください。

ディストリビューション スイッチはリンク損失を検出するとリンク ダウン イベントを処理し、そこで次の 3 段階のプロセスをトリガーします。

1. 障害の発生したリンクに関連するルーティング テーブルのエントリを削除
2. 影響するルートのネクストホップ隣接の損失を反映してソフトウェア Cisco Express Forwarding（CEF）テーブルをアップデート
3. ソフトウェア テーブルに含まれている有効なネクストホップ隣接の変更を反映してハードウェア テーブルをアップデート

イコール コスト パスのコア構成では、スイッチは 2 つのルートおよび対応する 2 つのハードウェア CEF フォワーディング隣接エントリを持っています。リンク障害が発生する前は、トラフィックはこれらの両方のフォワーディング エントリを使用して転送されています。2 つのエントリのいずれかが削除されると、スイッチは残った CEF エントリを使用してすべてのトラフィックの転送を開始します。ネットワーク内のすべてのトラフィック フローの復元に必要な時間は、物理リンク障害を検出し、ソフトウェアおよび関連するハードウェアのフォワーディング エントリをアップデートするのに必要な時間にのみ依存します。

推奨されるイコール コスト パス設計の大きな利点は、ネットワークの復旧動作が高速で結果が予測可能なことです。

イコール コスト パスを使用する際の潜在的な欠点は、特定のトラフィック フローを特定のリンクに振り向ける機能が制限されることです。しかし、この制限を補うだけのものがこの設計にあります。最も複雑性の少ない構成を実現し、安定した最速コンバージェンス時間を提供することにより、ネットワーク全体の可用性がさらに向上します。

（注） イコール コスト パスのレイヤ 3 スイッチド キャンパスでは、特定のトラフィック フローに使用するパスの設定はできませんが、特定のフローが最終的にどこに流れるかを予測することはできます。ハードウェアのフォワーディング アルゴリズムでは、ネットワーク内の同じトラフィック フローは常に同じパスに沿って転送されます。この動作の一貫性は、診断やキャパシティ プランニングの際に役立ち、また冗長パスのトラフィック パターンに関連する問題をある程度緩和できます。

レイヤ 3 コアのコンバージェンス結果 — EIGRP および OSPF

障害の分析

キャンパス コアでは、次の 3 つの基本的なコンポーネント障害について調査しました。

- コア ノードの障害
- コアとディストリビューション間のファイバの障害

- コア間を相互接続するファイバの障害

表 1 に、テスト結果の概要を示します。

表 1　　障害テストの結果

障害ケース	アップストリームの復旧	ダウンストリームの復旧	復旧メカニズム
ノード障害	200 ミリ秒	200 ミリ秒	アップストリーム — L3 イコール コスト パス ダウンストリーム — L3 イコール コスト パス
コアとディストリビューション間のリンクの障害	200 ミリ秒	200 ミリ秒	アップストリーム — L3 イコール コスト パス ダウンストリーム — L3 イコール コスト パス
コア間のリンクの障害	0 ミリ秒	0 ミリ秒	アップストリーム — 転送パスの損失なし ダウンストリーム — 転送パスの損失なし

推奨されるキャンパス コア設計では、すべてのノードが冗長イコール コスト ルートを持ちます。そのため、単一コンポーネント障害の復旧時間は、トラフィック フローを復元するためのルーティング プロトコルの復旧には依存しません。リンク障害が発生した場合、各ノードは単独で残った冗長パスにすべてのトラフィックを転送します。ノード障害が発生した場合、影響を受ける隣接スイッチは、相互接続しているリンクの障害で接続の損失を検出します。これにより、各スイッチは同様に単独で残った冗長パスにすべてのトラフィックを転送します。

3 つの障害ケースのうち 2 つ（コア ノード自体の障害、およびディストリビューション スイッチとコア スイッチ間を接続するファイバの障害）は、イコール コスト パスの復旧に依存します。3 番め（コア間のファイバ リンクの障害）の場合、アクティブなフォワーディング パスは失われていないので、ファイバ リンクが失われたことによるユニキャスト トラフィック フローへの影響はありません。3 つの障害ケースすべてにおいて、ネットワークはルーティング プロトコルによるトポロジのアップデートと再計算を待たなくてもすべてのユニキャスト トラフィック フローを復元できます。

コア スイッチ間でファイバの障害が発生しても、ユニキャスト トラフィック フローに対する直接の影響は通常ありません。コア ネットワークは完全メッシュ型の設計なので、このリンクは二重障害の場合にユニキャスト トラフィックにだけ使用されます。ユニキャストだけの環境の場合、このリンクは冗長性に不可欠なものではありませんが、キャンパス設計では依然として推奨される要素です。このリンクは、ある特定の構成でのマルチキャスト トラフィックの復旧に使用します。また、コア ノードがネットワークへのデフォルトまたは集約ルーティング情報の送信元に設定される場合にも必要です。

コンポーネント障害に起因したトラフィック フローを復元するためのネットワークの機能は、使用するルーティング プロトコルに無関係ですが、それでもルーティング プロトコルのコンバージェンスは起こります。EIGRP はトポロジ アップデートを生成し、OSPF は Link-State Advertisements（LSA; リンクステートアドバタイズメント）をフラッディングさせ Dijkstra 計算を行います。これらのイベントがネットワークに及ぼす影響を最小限にするために、シスコはキャンパス設計の際にルーティング プロトコルの適切な設計ガイドラインに従うことを推奨します。詳細については、ハイ アベイラビリティ キャンパスおよびレイヤ 3 アクセスの設計ガイドを参照してください。

イコール コスト パスの復旧につながるイベントの復旧に要する時間は、次の時間に依存します。

- 物理リンクの障害の検出に要する時間

- ソフトウェアおよび対応するハードウェア フォワーディング テーブルのアップデートに要する時間

前述のコンバージェンス時間の実現に必要なリンク損失の高速検出を可能にするには、すべてのポイントツーポイント リンクで 802.3z または 802.3ae のリンク ネゴシエーションをイネーブルにしておく必要があります。CatOS および Cisco IOS ともに、リンク ネゴシエーションはデフォルトでイネーブルになっています。リンク ネゴシエーションをディセーブルにすると、アップストリーム フローとダウンストリーム フローともにコンバージェンス時間が増加します。

CatOS：

```
set port negotiation [mod/port] enable
show port negotiation [mod[/port]]
```

Cisco IOS：

```
int gig [mod/port]
 [no] speed nonegotiate
```

復旧の分析

リンクおよびデバイスの復旧のためのコンバージェンスは、次のような障害シナリオのコンバージェンスと同じです。

- コア ノードの復旧
- コアとディストリビューション間のファイバの復旧
- コア間を相互接続するファイバの復旧

表 2 に、テスト結果の概要を示します。

表 2　　復旧テストの結果

障害ケース	アップストリームの復旧	ダウンストリームの復旧	復旧メカニズム
ノードの復旧	0 ミリ秒	0 ミリ秒	アクティブ データ パスの損失なし
コアとディストリビューション間のリンクの復旧	0 ミリ秒	0 ミリ秒	アクティブ データ パスの損失なし
コア間のリンクの復旧	0 ミリ秒	0 ミリ秒	アクティブ データ パスの損失なし

表 2 の結果が示すように、レイヤ 3 キャンパスのリンクとノードの復旧は、既存および新規のデータ フローにほとんど影響しません。レイヤ 3 のフォワーディング パスのアクティブ化または再アクティブ化にもこの同じ利点があります。スイッチはネイバーからトラフィックの転送が可能なことを通知されるまで、アップストリーム ネイバーにもダウンストリーム ネイバーにもトラフィックをまったく転送しません。有効なルートの存在が確認できるまでトラフィックは転送されないので、スイッチは継続して既存の冗長パスを使用しながら新しいパスをアクティブ化できます。

新しくリンクをアクティブにするアクティブ化のときに、各スイッチは EIGRP/OSPF のネイバー ディスカバリ（近隣探索）とトポロジ交換を実行します。各スイッチは新しいルートを学習すると、ルーティング テーブルと CEF フォワーディング テーブルに 2 つめのイコール コスト エントリを作成します。冗長設計では、現存のエントリを無効にしないでこの 2 つめのイコール コスト フォワーディング エントリが追加されます。ルーティング プロトコルのアップデート処理中、スイッチは既存のハードウェア フォワーディング エントリを継続して使用するので、新しいルートの挿入が原因でデータを失うことはありません。

ルートの削除がルーティング プロトコルのコンバージェンスとは無関係な前述のコンポーネント障害の場合とは異なり、各キャンパス スイッチは新しいリンクまたはノードのアクティブ化のときに新しいルートを挿入します。このため、ルーティング プロトコルに直接依存します。ネットワークはこれらの新しいルートが挿入される速度に左右されないので、EIGRP および OSPF により新しいルートが伝播、挿入される速度はそれほど重要ではありません。ただし、この障害ケースのように、推奨される設計上のガイドラインに従って、ルート コンバージェンス プロセスがネットワーク全体に与える影響を最小限に抑えることが必要です。

ほとんどの環境では、冗長レイヤ 3 キャンパス設計でリンクまたはスイッチがアクティブ化されても影響はありません。ただし、大規模なオーバーサブスクライブ型ネットワークの場合、新しいルート（より適切なパス ルートまたは 2 つめのイコール コスト ルート）を挿入する際の移行期間に、新しいアクティブ パス上で送信された既存のフローのパケットが古いパス上で先に送信されたパケットより早く到着し、到着順序が前後することがあります。これは、元のパスの高負荷によって重大な輻輳が発生し、そのために伝送遅延が生じる場合にのみ発生します。

大規模なオーバーサブスクライブ型（ワーストケース）負荷を使用したテスト時に、アクティブな音声フローの 0.003 パーセントに満たない割合で、再順序付けに起因する音声ストリームのパケット損失が発生したことが測定されました。2 つめのリンクのアクティブ化により生じた、この非常に低いレベルのパケット損失とそれに関連する低いレベルのジッタによる影響および音声ストリームのフォワーディング パスのダイナミックな変更による影響は、テスト ストリームの MOS スコアの記録には表れませんでした。冗長レイヤ 3 キャンパス設計では、既存のトラフィック フローに動作上の影響を及ぼすことなく新しいリンクまたはノードをアクティブ化することができます。

レイヤ 3 ディストリビューションのコンバージェンスを伴うレイヤ 2 アクセス — 結果および分析

ここでの内容は、次のとおりです。

- テスト構成の概要（p.12）
- ディストリビューション ビルディング ブロックの説明（p.14）
- 構成 1 の結果 — HSRP、EIGRP（PVST+ 使用）（p.16）
- 構成 2 の結果 — HSRP、EIGRP（Rapid-PVST+ 使用）（p.23）
- 構成 3 の結果 — HSRP、OSPF（Rapid-PVST+ 使用）（p.26）
- 構成 4 の結果 — GLBP、EIGRP（Rapid-PVST+ 使用）（p.29）
- 構成 5 の結果 — GLBP、EIGRP、Rapid-PVST+（レイヤ 2 ループ使用）（p.32）

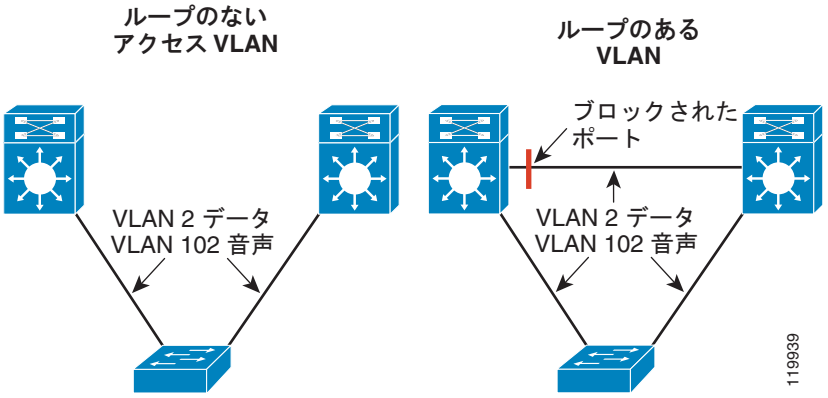
テスト構成の概要

ディストリビューション レイヤを構成する一連のスイッチとそれに接続するすべてのアクセス スイッチを、ディストリビューション ブロックと呼びます。階層型の設計モデルにおいて、ディストリビューション ブロック設計は、アクセス スイッチに接続されたデバイス間を流れるすべてのトラフィックに対する復元力を備えると同時に、キャンパスのコアに冗長接続を提供することで、キャンパスのこの部分を出入りするすべてのトラフィックに復元力を提供します。

標準のディストリビューション ブロック設計には次の 2 つの構成が存在します。

- レイヤ 2 ループのある構成の VLAN
- ループのないトポロジ構成の VLAN

図 5　標準のディストリビューション ビルディング ブロック（レイヤ 2 ループのある場合とない場合）



使用できるデフォルト ゲートウェイ、スパニング ツリー バージョン、およびルーティング プロトコルにはさまざまなものがあるので、この 2 つの基本構成に基づきさらに複数の構成を検討することができます。ここでは、各構成の違いを示すために、調査対象のテスト構成を 5 つ選択しました（表 3 を参照）。

表 3　5 つのテスト構成

テスト構成	デフォルト ゲートウェイ プロトコル	スパニング ツリー バージョン	ルーティング プロトコル
構成 1	HSRP	PVST+（ループなし）	EIGRP
構成 2	HSRP	Rapid PVST+（ループなし）	EIGRP
構成 3	HSRP	Rapid PVST+（ループなし）	OSPF
構成 4	GLBP	Rapid PVST+（ループなし）	EIGRP
構成 5	GLBP	Rapid-PVST+（ループ型トポロジ）	EIGRP

5 つのテスト構成それぞれについて、次の 5 つの基本的な障害テストを実行しました。

1. アクセス スイッチからアクティブ デフォルト ゲートウェイ（HSRP/GLBP）ディストリビューション スイッチ間のアップリンク ファイバの障害
2. アクセス スイッチからスタンバイ デフォルト ゲートウェイ（HSRP/GLBP）ディストリビューション スイッチ間のアップリンク ファイバの障害
3. アクティブ デフォルト ゲートウェイ ディストリビューション スイッチの障害
4. スタンバイ デフォルト ゲートウェイ ディストリビューション スイッチの障害
5. ディストリビューション スイッチ間のファイバ接続の障害

テスト ケース 1 および 2 は、アクセス スイッチのタイプごとに複数回実行し、次の 3 つの障害シナリオを使用しました。

- リンク両端のファイバの障害
- 1 つのファイバの障害（送信側）

- 1 つのファイバの障害（受信側）

障害テストごとに、補完的にスイッチの再起動またはリンクのアクティブ化 テストを実施し、障害コンポーネントのリブートまたは交換を行う操作の影響を調べました。

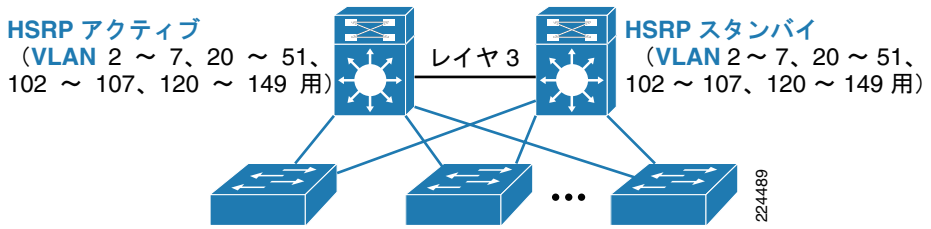
下記に記載されている結果は、テストを複数回繰り返したときに測定されたワーストケースの値です。最初の 4 つのテスト ケースでは、各テストを通し物理トポロジ、VLAN、および他のすべての構成に変更はありません。5 番めのテスト ケースでは、音声およびデータ VLAN が 2 つのディストリビューション スイッチを接続するトランクを通過するよう設定しました。ディストリビューション スイッチおよびアクセス スイッチの説明および構成については、下記を参照してください。

（注） 下記のテスト結果および分析の項では、最初の構成についてのみ障害テストの結果および復旧テストの結果を詳しく説明します。他の 4 つの構成については、分析の項で、構成の変更がネットワークの復旧に及ぼした影響についてのみ説明します。

ディストリビューション ビルディング ブロックの説明

図 6 に示すように、標準のディストリビューション ビルディング ブロックは、ディストリビューション スイッチのペアと、その 2 つのディストリビューション スイッチにアップリンク接続される複数のアクセス スイッチで構成されています。

図 6　レイヤ 2 ループなしの標準のディストリビューション ビルディング ブロック（テスト構成 1 ～ 4）



基本物理トポロジの範囲内で、ディストリビューション ビルディング ブロックの構成の細部は徐々に発展してきています。最初の 4 つのテスト ネットワーク構成には、次の設計オプションを採用しました。

- 各アクセス スイッチに固有の音声 VLAN およびデータ VLAN を設定
- アクセス スイッチおよびディストリビューション スイッチ間のアップリンクには、レイヤ 2 トランクを使用してネイティブ、データ、および音声 VLAN を伝送。3 つめの固有のネイティブ VLAN は、VLAN ホッピング攻撃を防止するために使用。詳細については、『*Designing a Campus Network for High Availability*』を参照してください。
  http://www.cisco.com/en/US/docs/solutions/Enterprise/Campus/HA_campus_DG/hacampusdg.html
- ディストリビューション スイッチ間のリンクには、レイヤ 3 ポイントツーポイントを使用

音声およびデータ VLAN はアクセス スイッチごとに固有で、アクセス スイッチとディストリビューション スイッチの間でトランキングされていますが、ディストリビューション スイッチ間ではトランキングされていません。ディストリビューション スイッチ間のリンクはレイヤ 3 ポイントツーポイントとして設定しました。シスコのベスト プラクティス設計では、複数のアクセス スイッチをまたがる VLAN がないことを推奨しています。これまで、ワイヤレス デバイスがアクセス ポイント（AP）間をシームレスにローミングできるようにするメカニズムの 1 つとして、複数のアクセス スイッチ間をブリッジする共通ワイヤレス VLAN の使用が推奨されてきました。Wireless LAN Switching Module（WLSM）を導入すると、AP 用の共通レイヤ 2 VLAN がなくても高速ローミングができるスケーラブルなアーキテクチャが提供されます。

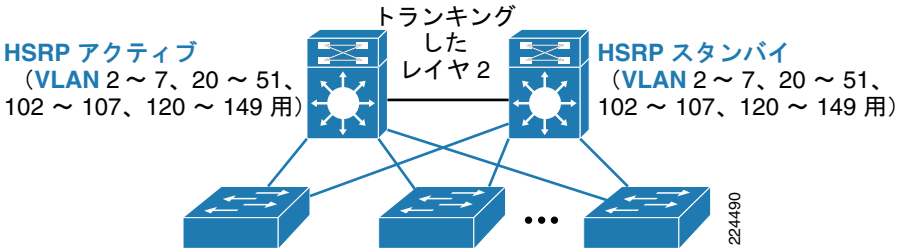
スパニング ツリー ルートと HSRP プライマリ ゲートウェイは、すべての VLAN を対象にディストリビューション スイッチ 1 に割り当てられます。

固有のアクセス データ VLAN と音声 VLAN ごとにデフォルト ゲートウェイ プロトコル（HSRP または GLBP）が設定されました。テスト ネットワークでは、すべてのアクティブ HSRP ゲートウェイと各 VLAN の関連ルート ブリッジがディストリビューション スイッチ 1 に設定されました。

デフォルト ゲートウェイの場所を割り当てる場合、通常 2 つの異なる設計方法を使用します。1 つは、アップストリーム トラフィックをロード シェアリングするメカニズムとして、音声 VLAN とデータ VLAN か、または奇数番と偶数番の VLAN に対応させて 2 つのディストリビューション スイッチ間で HSRP ゲートウェイを交互に使用する方法です。もう 1 つは、設定および運用動作に一貫性を持たせる手段として、すべての VLAN を対象にアクティブ ゲートウェイとしてディストリビューション スイッチの 1 つを割り当てる方法です。ロード バランシング要件のある環境では、アップストリーム トラフィックを効率的にロード バランシングできることから、シスコは HSRP グループを交互に使用する方法でなく、GLBP の使用を推奨しています。より予測可能な方法を必要とする環境では、シスコはすべての HSRP グループを 1 つのディストリビューション スイッチに割り当てる方法を推奨します。

5 番めのテスト ケースではネットワーク構成が変更されました（図 7 を参照）。

図 7　　レイヤ 2 ループのあるディストリビューション ビルディング ブロック（テスト構成 5）



5 番めのネットワーク構成において前述の構成から変更になった点は、すべての音声およびデータ VLAN が 2 つのディストリビューション スイッチ間の 10GigE ファイバ上でトランキングされたことです。各アクセス スイッチには専用の音声およびデータ VLAN が引き続き設定され、ディストリビューション スイッチ 1 にはすべての VLAN を対象にルート ブリッジと HSRP アクティブ ノードが設定されました。

GLBP により提供されるデフォルト ゲートウェイのダイナミック ロード バランシング メカニズムの使用効率を最大化するため、スパニング ツリーをディストリビューション間のリンクに接続するポートでブロックするよう設定しました。すべての VLAN を対象にアクセスおよびディストリビューション間の 2 つのリンクをこのリンクで強制的にブロックすることで、ネットワークの通常動作時のアップストリームとダウンストリーム両方向のトラフィックをロード シェアリングすることができました。この構成例を次に示します。

```
Distribution-Switch-2#sh run int ten 4/3

interface TenGigabitEthernet4/3

 description 10GigE trunk to Distribution 1 (trunk to root bridge)

 no ip address

 load-interval 30

 mls qos trust dscp

 switchport
```

```
switchport trunk encapsulation dot1q
 switchport trunk native vlan 900
 switchport trunk allowed vlan 2-7,20-51,102-107,120-149
 spanning-tree cost 2000 << Increase port cost on trunk to root bridge
```

（注） 図 7 に示すレイヤ 2 ループを使用する構成は、推奨されるベスト プラクティスではありません。Loop Guard、Unidirectional Link Detection; UDLD）、BPDU Guard など、正しく使用すればループ型レイヤ 2 トポロジを使用する場合のリスクが大幅に軽減される機能もありますが、レイヤ 2 サブネットの拡張を必要とするアプリケーションやビジネス要件がない場合、シスコはハイ アベイラビリティ キャンパス設計ではレイヤ 2 ループ構成を推奨しません。このテスト項目は、比較分析の目的でのみ提供されています。

これらのテストで使用された設計上の推奨事項に関する詳細については、『*Designing a Campus Network for High Availability*』を参照して下さい。

構成 1 の結果 — HSRP、EIGRP（PVST+ 使用）

障害の分析

構成 1 の特性は次のとおりです。

- デフォルト ゲートウェイ プロトコル — HSRP
- スパニング ツリー バージョン — PVST+（per VLAN 802.1d）
- IGP — EIGRP

表 4 に、テスト結果の概要を示します。

表 4　　構成 1 の障害テスト結果

障害ケース	アップストリームの復旧	ダウンストリームの復旧	復旧メカニズム
アクティブ HSRP へのアップリンク ファイバの障害	900 ミリ秒	700 ～ 1100 ミリ秒の間で変動	アップストリーム — HSRP ダウンストリーム — EIGRP
スタンバイ HSRP へのアップリンク ファイバの障害	0 ミリ秒	700 ～ 1100 ミリ秒の間で変動	アップストリーム — 損失なし ダウンストリーム — EIGRP
アクティブ HSRP ディストリビューション スイッチの障害	800 ミリ秒	200 ミリ秒	アップストリーム — HSRP ダウンストリーム — L3 インコール コスト パス

表 4　構成 1 の障害テスト結果（続き）

スタンバイ HSRP ディストリビューション スイッチの障害	0 ミリ秒	200 ミリ秒	アップストリーム — 損失なし ダウンストリーム — L3 イコール コスト パス
ディストリビューション スイッチ間のファイバの障害	0 ミリ秒	0 ミリ秒	アクティブ データ パスの損失なし

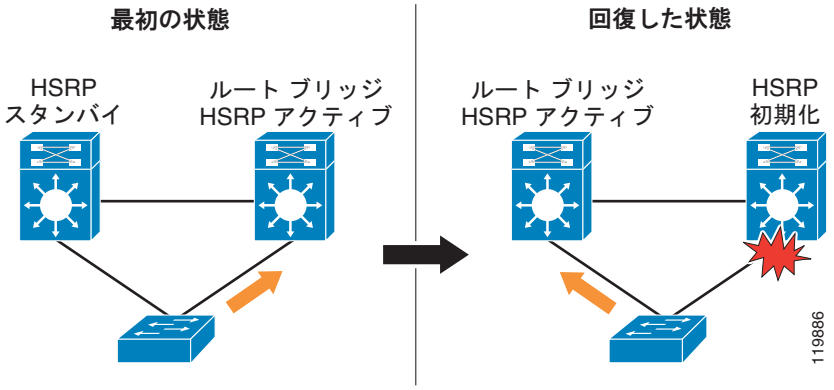
アクティブ HSRP ディストリビューション スイッチへのアップリンク ファイバの障害

アップストリームのコンバージェンス

アップストリーム トラフィック フローの復旧時間は、主に HSRP タイマーの設定により決まります。通常の状態では、端末を発信元とするすべてのトラフィックは、HSRP ピアに送られる仮想 HSRP MAC アドレス向けのアクティブ ブリッジド アップストリームです。アクティブ HSRP ピアへのアップリンクに障害が発生すると、アクセス スイッチはフォワーディング テーブルからそのリンクに関連付けられているすべての CAM エントリを、仮想 HSRP MAC を含めて削除します。

同時に、スタンバイ HSRP ピアはアクティブ ピアから HELLO を受信しなくなるので、設定されているデッド タイマーをカウント ダウンします。スタンバイ ピアは 3 つの HELLO を失うとアクティブ ステートに移行し、gratuitous ARP を送信してアクセス スイッチの CAM テーブルに仮想 HSRP MAC アドレスの新しいロケーションを入力したあと、仮想 HSRP MAC アドレスに送信されるパケットを受け入れ、転送を開始します（図 8 を参照）。

図 8　アクティブ HSRP ディストリビューション スイッチへのアップリンク ファイバの障害 — アップストリームのコンバージェンス



記載されているこれらの特定のテスト ケースの復旧時間は、250 ミリ秒の HELLO タイマーおよび 800 ミリ秒のデッド インターバル HSRP タイマーを使用して得られた値です。900 ミリ秒のアップストリーム損失は、特定の障害シナリオでのみで発生するワーストケースの値です。2 つのスイッチ間のファイバ損失には、ペア内の 1 つのファイバを損失する場合とペア内の両方のファイバを同時に損失する場合があります。アクティブ ディストリビューション スイッチの受信ポートに接続されたファイバだけに障害が発生した場合、スイッチが HSRP HELLO フレームを送信することができても、インバウンド トラフィックを受信できず、リモート障害検出機能によりインターフェイスがシャットダウンされる前にわずかな時間が存在します。

アクティブ スイッチの送信ファイバの損失の場合には、これと反対の現象が起こります。HSRP HELLO は送信されませんが、コアに送信されるデータは引き続き受信され、結果として損失の時間が短くなります。単一ファイバ障害と HSRP アップデートの送信の同期化でワーストケースのコンバージェンスは増加することがありますが、テスト結果の 900 ミリ秒は全体の平均コンバージェンス時間の 780 ミリ秒からわずかにずれた外れ値です。

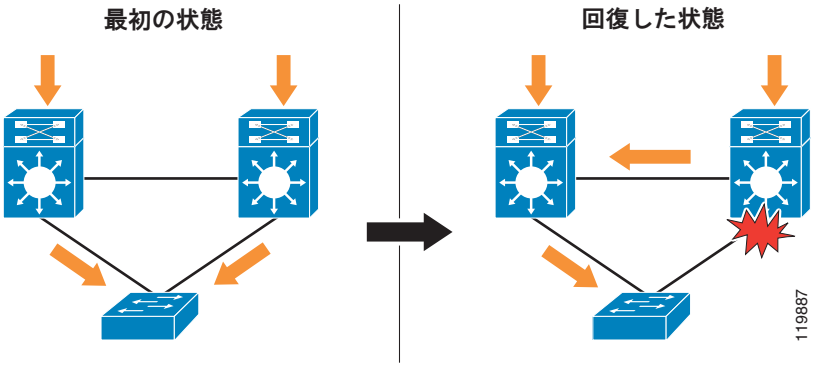
アクティブ HSRP ピアの損失は、スパニング ツリーのルート ブリッジの損失も意味しますが、これがトラフィックの損失につながることはありません。設定されているスパニング ツリー トポロジはループがなく、どのポートもブロッキング ステートから移行させる必要がありません。アクティブ ルート ブリッジの損失により新しいルート ブリッジの選択が開始されますが、802.1d 実装ではそれによりアクティブ ポートの転送が影響を受けることはありません。

設計のヒント — HSRP HELLO とデッド インターバルの値を小さくすることで音声またはデータ トラフィック フローのアップストリーム部分の復旧時間を短くできますが、シスコは HSRP デッド時間を同じフローのダウンストリーム部分の復旧時間と一致させることを推奨します。これらのテスト ケースは 800 ミリ秒のデッド時間を使用して行われ、この時間は音声 VLAN で測定された EIGRP ダウンストリームの復旧時間に対応しています。HSRP タイマーの値を小さくしすぎると、ディストリビューション スイッチの負荷が非常に高くなった場合にネットワークが不安定になることがあります。この参照用のテスト トポロジでは、250/800 ミリ秒の設定にした場合に CPU 負荷が 99% の状態で正常に動作することが検証されました。

ダウンストリームのコンバージェンス

ループのない構成におけるダウンストリーム トラフィック フローの復旧時間は、主としてルーティング プロトコルのコンバージェンスにより決まります（図 9 を参照）。

図 9　アクティブ HSRP ディストリビューション スイッチへのアップリンク ファイバの障害 — ダウンストリームのコンバージェンス



ファイバの障害を検出すると、スイッチは次の一連のイベントを処理して接続を復元します。

1. 影響を受けたインターフェイスのライン プロトコルをダウンにマーキングします。
2. 対応する VLAN スパニング ツリー ポートをディセーブル（ダウン）にマーキングします。
3. autostate プロセスによりトリガーされて、各スパニング ツリー インスタンスに関連付けられている VLAN インターフェイスもダウンとマーキングします。
4. フォワーディング テーブルから、障害 VLAN に関連付けられている CEF の Glean エントリを削除します（ローカルに接続されているホストのエントリ）。
5. VLAN インターフェイスが失われたことを Cisco IOS が EIGRP プロセスに通知します。
6. EIGRP は失われたサブネット ルートを削除し、すべてのアクティブ ネイバーにそのルートに関するクエリーを送信します。
7. 転送テーブルから、失われたルートに関連付けられている CEF エントリを削除します。
8. すべてのクエリーを受信すると、EIGRP は最適なネクストホップ ルートを決定し、新しいルートをルーティング テーブルに挿入します。

9. 新しいルートと一致する CEF エントリをフォワーディング テーブルに挿入します。
10. トラフィック フローを復元します。

ディストリビューション スイッチにはイコール コスト パスがなく、障害のあったネットワークのフィジブル サクセサもないので、EIGRP がルーティング コンバージェンスを開始してトラフィック フローを復元させる必要があります。

(注) *設計のヒント* — 最適なコンバージェンスが得られるように、シスコは各ディストリビューション ビルディング ブロック内のすべてのルートを各ディストリビューション スイッチのアップストリームからコアに集約することを推奨します。コア上に集約ルートが存在するとコア ノードはネットワークの他の部分にクエリーを伝播しないので、クエリーの抑制とコンバージェンス時間の抑制に役立ちます。集約した設定を使用した場合、どの接続ルートが失われても EIGRP クエリーの生成、応答、およびルートの挿入に要する時間は 100 ミリ秒を下回ることが測定されました。

クエリー処理を迅速に完了する能力は、送信元スイッチと宛先スイッチの EIGRP クエリーを処理する能力にも左右されます。コンバージェンス時間を確実に予測するには、スイッチに高い CPU 負荷をもたらすワーム、DDoS 攻撃、スパニング ツリー ループなどの異常なイベントからネットワークを確実に保護することも必要です。

(注) *設計のヒント* — 音声トラフィックの最適なコンバージェンスが得られるように、シスコでは VLAN 番号を割り当てる際に、表 5 に示すとおり音声など最も影響を受け易いアプリケーションに各物理インターフェイスの最も小さい VLAN 番号を割り当てることを推奨します。

表 5　VLAN 割り当ての推奨事項

VLAN 機能	VLAN インターフェイス
Wired_Voice_VLAN	7
Wireless_Voice_VLAN	57
Wired_Data_VLAN	107
Wireless_Multicast_VLAN	157

特定のインターフェイス上でトランキングしたすべての VLAN が同時にコンバージェンスするわけではありません。Cisco IOS は、ルーティング プロセス（EIGRP/OSPF）への VLAN 損失の通知を 100 ミリ秒に 1 つのレートに制限します。たとえば、アクセス スイッチあたり 6 つの VLAN を設定すると、アップリンクの障害が発生した場合 6 番めの VLAN は最初の VLAN から 500 ミリ秒後にコンバージェンスします。

スタンバイ HSRP ディストリビューション スイッチへのアップリンク ファイバの障害

アップストリームのコンバージェンス

スタンバイ HSRP ディストリビューション スイッチの障害が発生した場合、すべてのトラフィックがアクティブ スイッチで処理されているのでアップストリーム トラフィックへの影響はありません。

ダウンストリームのコンバージェンス

ダウンストリーム トラフィックへの影響は、アクティブ ディストリビューション スイッチへのアップリンクの障害の場合と同じです。コア スイッチは継続して両方のディストリビューション スイッチにトラフィックを転送し、ダウンストリーム データ パスの復旧はディストリビューション スイッチ間のルート変更に依存します。

アクティブ HSRP ディストリビューション スイッチの障害

アップストリームのコンバージェンス

ディストリビューション スイッチの障害後のアップストリーム トラフィックの復旧メカニズムは、ファイバの障害ケースとまったく同じです。スイッチの障害が発生した場合、複数の HSRP アドレスを同時に復旧するため、スタンバイ スイッチに加わる復旧処理の負荷が増加します。ただし、テスト ケースの範囲内では、このオーバーヘッド処理の増加による復旧時間への影響は測定されませんでした。

ダウンストリームのコンバージェンス

ディストリビューション スイッチの障害後のダウンストリーム トラフィックの復旧は、コア スイッチ内のレイヤ 3 イコール コスト復旧機能を使用して行います。前述のレイヤ 3 コア設計のテスト結果の項で説明されているように、両方のコア スイッチには 2 つのディストリビューション スイッチを使用したすべてのアクセス サブネットへの冗長ルートがあります。ディストリビューション スイッチのいずれかに障害が発生した場合、コア ノードは残ったディストリビューション スイッチを経由してすべてのダウンストリーム トラフィックの転送を開始します。測定では 200 ミリ秒を下回る損失時間でした。

スタンバイ HSRP ディストリビューション スイッチの障害

スタンバイ HSRP ディストリビューション スイッチに障害が発生した場合、アップストリーム トラフィック フローへの影響はありません。ダウンストリーム フローの障害は、前述のアクティブ HSRP スイッチで説明した障害の場合と同じです。

ディストリビューション スイッチ間のファイバの障害

ディストリビューション スイッチ間のレイヤ 3 接続に障害が発生した場合、アップストリームとダウンストリーム トラフィック フローへの影響はありません。このリンクは、アップリンクの障害時にディストリビューション ブロック内のトラフィックを復旧するためにだけ使用されます。このリンクのサブネットはディストリビューション ブロックの集約アドレス範囲に含まれているので、コアに EIGRP トポロジ アップデートが送信されることはありません。

復旧の分析

構成 1 の特性は次のとおりです。

- デフォルト ゲートウェイ プロトコル — HSRP
- スパニング ツリー バージョン — PVST+（per VLAN 802.1d）
- IGP — EIGRP

表 6 に、テスト結果の概要を示します。

表 6　　構成 1 の復旧テスト結果

復旧ケース	アップストリームの復旧	ダウンストリーム復旧	復旧メカニズム
アクティブ HSRP へのアップリンク ファイバの復旧	0 秒	0 秒	アップストリーム — 損失なし ダウンストリーム — 損失なし

表 6　構成 1 の復旧テスト結果（続き）

スタンバイ HSRP へのアップリンク ファイバの復旧	0 秒	0 秒	アップストリーム — 損失なし ダウンストリーム — 損失なし
アクティブ HSRP ディストリビューション スイッチの復旧	0 秒	0 ～ 6 秒の間で変動	アップストリーム — 損失なし ダウンストリーム — L3 イコール コスト パスおよび ARP
スタンバイ HSRP ディストリビューション スイッチの復旧	0 秒	0 ～ 6 秒の間で変動	アップストリーム — 損失なし ダウンストリーム — L3 イコール コスト パスおよび ARP
ディストリビューション スイッチ間のファイバの復旧	0 秒	0 秒	損失なし

アクティブ HSRP へのアップリンク ファイバの復旧

アクセス スイッチとディストリビューション スイッチ間のファイバ接続をアクティブ化した場合、データの損失は通常は発生しません。リンクがアクティブ化されると、プライマリ ディストリビューション スイッチはルート ブリッジの再選択をトリガーし、ルートとしてのアクティブ ロールを引き継ぎます。この処理によりスパニング ツリーの論理的なコンバージェンスが発生しますが、既存のポートのフォワーディング ステータスは変化せず、フォワーディング パスの損失もありません。

スパニング ツリーのコンバージェンスに加えて、HSRP プリエンプト遅延タイマーが期限切れになるとプライマリ HSRP ピアはデフォルト ゲートウェイの引き継ぎを開始します。この処理はディストリビューション スイッチ間で同期しているのでパケット損失は通常発生しません。音声およびデータ VLAN のスパニング ツリー ステートの移行により、接続ルートがルーティング テーブルに挿入されます。接続ルートが挿入されると、スイッチはローカル サブネット上にパケットのフォワーディングを開始します。

スタンバイ HSRP へのアップリンク ファイバの復旧

プライマリ ディストリビューション スイッチの場合と同じように、スタンバイ ディストリビューション スイッチへのアップリンク ファイバをアクティブ化しても既存の音声またはデータ フローに影響しません。この場合、ルート ブリッジと HSRP ゲートウェイの復旧のいずれも発生しません。スイッチは音声およびデータ VLAN の接続ルートを挿入し、トラフィックのフォワーディングを開始します。前述のように、この動作によるアクティブ データ フローへの影響は通常ありません。

アクティブ HSRP ディストリビューション スイッチの復旧

ディストリビューション スイッチをアクティブ化した場合、アクティブな音声フローのアップストリームとダウンストリームの両方のコンポーネントに大きな影響が生じる可能性があります。HSRP がアクティブ ゲートウェイの役割を引き継ぐように設定されている場合、プライマリ ディストリビューション スイッチ、ルート ブリッジ、および HSRP 高次プライオリティがアクティブ化されたとき、スイッチがデフォルト ゲートウェイの役割を引き継いでいるにもかかわらずコ

アとの EIGRP ネイバーが確立されていない時間が存在することがあります。スイッチはアクセス サブネットから受信したトラフィックを転送することができないため、一時的なルーティング ブラック ホールが発生します。

この問題を回避する方法はいくつかあります。推奨事項の 1 つとして、スイッチ上のすべてのラインカードとインターフェイスがアクティブであること、およびすべてのルーティング隣接がアクティブになったことを確実視できるだけの十分に大きな HSRP プリエンプト遅延タイマーを設定します。このようにした設定例を次に示します。

```
interface Vlan20
 description Voice VLAN for 3550
 ip address 10.120.20.2 255.255.255.0
 ip verify unicast source reachable-via any
 ip helper-address 10.121.0.5
 no ip redirects
 ip pim query-interval 250 msec
 ip pim sparse-mode
 load-interval 30
 standby 1 ip 10.120.20.1
 standby 1 timers msec 250 msec 800
 standby 1 priority 150
standby 1 preempt delay minimum 180  << Configure 3 minute delay
 standby 1 authentication ese
```

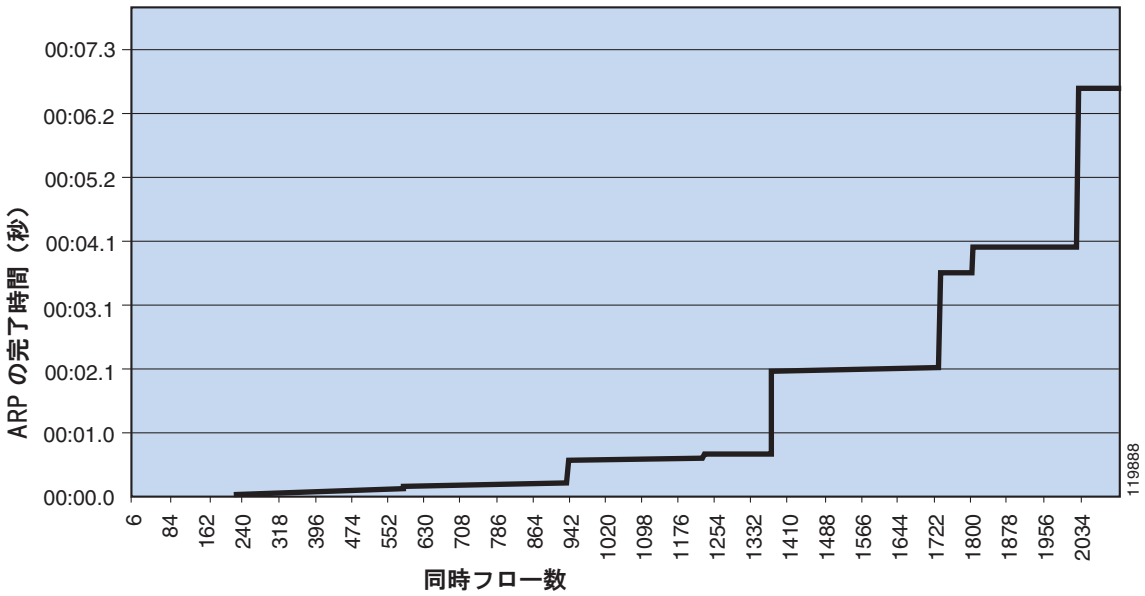
アップストリームの損失の問題は HSRP をチューニングすることで回避できますが、負荷の高い環境でディストリビューション ノードがアクティブ化されると、ダウンストリーム トラフィックの損失が発生することもあります。ディストリビューション ノードはディストリビューション ブロックのルートをコア スイッチに通知したあと、ただちにすべての接続サブネットのトラフィックを受信し始めます。

このトラフィックを転送するには、ディストリビューション スイッチでフローごとにネクストホップ隣接、つまり Address Resolution Protocol（ARP; アドレス解決プロトコル）テーブル エントリを調べる必要があります。この処理の復旧時間は、フローの数、ARP 要求に応答する端末の能力、およびディストリビューション スイッチの ARP スロットリング動作に依存します。

意図的な攻撃やスキャニング ワームの副作用の場合でも、DoS 攻撃を防止するために、すべての Cisco Catalyst スイッチには ARP 処理のレート制限メカニズムが実装されています。DoS 攻撃があった場合にスイッチはこれらの制限によって保護されますが、DoS 攻撃による急激なフラッディングなのか、有効なトラフィックの急激なフラッディングなのか区別できません。どちらの場合も、スイッチは生成された ARP 要求のレートを制限します。大量のアクティブ フローが存在する大規模キャンパス環境では、ディストリビューション スイッチがリブートされると大量の ARP アクティビティが急激に発生しますが、これはスイッチ固有の DoS プロテクション メカニズムにより抑制されます。

図 10 に、DoS プロテクションがルータのパフォーマンスに及ぼす影響を示します。

図 10　DoS プロテクションの影響



同時に存在するフローの数

多くのアクティビティ処理を行っているタイミングでスイッチがリブートされた場合、トラフィック フローに短期間の影響が出ます。ただし、この DoS プロテクション メカニズムでは、影響を上回る総合的な利点がもたらされます。

スタンバイ HSRP ディストリビューション スイッチの復旧

スタンバイ スイッチがリブートされた場合、前述のようにダウンストリーム フローに同様の影響を及ぼす可能性があります。ディストリビューション スイッチのリブート スケジュールを管理することで、潜在的な影響を緩和できます。HSRP とスパニング ツリーのステートはリブートでは変化しないので、アップストリーム フローは影響を受けません。

ディストリビューション スイッチ間のファイバの復旧

ディストリビューション スイッチ間のリンクをアクティブ化しても、アクティブなトラフィック フローには影響しません。ディストリビューション ブロックのルートはコアに集約されているので、新しいサブネットをアクティブ化してもトポロジのアップデートは発生しません。

構成 2 の結果 — HSRP、EIGRP（Rapid-PVST+ 使用）

障害の分析

構成 2 の特性は次のとおりです。

- デフォルト ゲートウェイ プロトコル — HSRP
- スパニング ツリー バージョン — Rapid-PVST+（per VLAN 802.1w）
- IGP — EIGRP

テスト結果の概要

表 7 に、テスト結果の概要を示します。

表 7　　構成 2 の障害テスト結果

障害ケース	アップストリーム復旧	ダウンストリーム復旧	復旧メカニズム
アクティブ HSRP へのアップリンク ファイバの障害	900 ミリ秒	700 ～ 1100 ミリ秒の間で変動	アップストリーム — HSRP ダウンストリーム — EIGRP
スタンバイ HSRP へのアップリンク ファイバの障害	0 ミリ秒	700 ～ 1100 ミリ秒の間で変動	アップストリーム — 損失なし ダウンストリーム — EIGRP
アクティブ HSRP ディストリビューション スイッチの障害	800 ミリ秒	200 ミリ秒	アップストリーム — HSRP ダウンストリーム — L3 イコール コスト パス
スタンバイ HSRP ディストリビューション スイッチの障害	0 ミリ秒	200 ミリ秒	アップストリーム — 損失なし ダウンストリーム — L3 イコール コスト パス
ディストリビューション スイッチ間のファイバの障害	0 ミリ秒	0 ミリ秒	アクティブ データ パスの損失なし

802.1w への変換の影響

スパニング ツリー プロトコルとして 802.1w を使用したディストリビューション ブロックにおける、リンクまたはノードの障害後のコンバージェンス特性は、802.1d を設定した同じトポロジにおけるコンバージェンス特性と変わりません。推奨される設計では、レイヤ 2 ループはすべてネットワークから排除されており、この設計では 802.1w により提供される、802.1d からのコンバージェンス時間の改善点を使用していません。前述のように、トラフィック フローの復元は HSRP、EIGRP、またはイコール コスト パス フェールオーバーのいずれかで実現されているので、トラフィック フローの復元にレイヤ 2 コンバージェンスを必要とするときはありません。

```
spanning-tree mode rapid-pvst  <<< Enable 802.1w per VLAN spanning tree
spanning-tree loopguard default
no spanning-tree optimize bpdu transmission
spanning-tree extend system-id
spanning-tree vlan 2-7,20-51,102-149,202-207,220-249,900 priority 28672
```

復旧の分析

構成 2 の特性は次のとおりです。

- デフォルト ゲートウェイ プロトコル — HSRP

- スパニング ツリー バージョン — Rapid-PVST+（per VLAN 802.1w）
- IGP — EIGRP

テスト結果の概要

表 8 に、テスト結果の概要を示します。

表 8　構成 2 の復旧テスト結果

復旧ケース	アップストリームの復旧	ダウンストリームの復旧	復旧メカニズム
アクティブ HSRP へのアップリンク ファイバの復旧	180 ミリ秒	180 ミリ秒	アップストリーム — 802.1w ダウンストリーム — 802.1w
スタンバイ HSRP へのアップリンク ファイバの復旧	0 ミリ秒	180 ミリ秒	アップストリーム — 損失なし ダウンストリーム — 802.1w
アクティブ HSRP ディストリビューション スイッチの復旧	180 ミリ秒	180 ミリ秒 ～ 6 秒の間で変動	アップストリーム — 802.1w ダウンストリーム — 802.1w、L3 イコール コスト パス、および ARP
スタンバイ HSRP ディストリビューション スイッチの復旧	180 ミリ秒	180 ミリ秒 ～ 6 秒の間で変動	アップストリーム — 802.1w ダウンストリーム — 802.1w、L3 イコール コスト パス、および ARP
ディストリビューション スイッチ間のファイバの復旧	0 秒	0 秒	アクティブ データ パスの損失なし

802.1w への変換の影響

802.1d の代わりに 802.1w を使用した場合、スイッチまたはリンクのアクティブ化のときに、音声トラフィックに軽微ですが無視できない影響があります。これはポートをアクティブ フォワーディング ステートに移行する方法に 2 つのプロトコル間で違いがあるからです。プライマリ スイッチ（優先ルート ブリッジの設定）がリブートされるか、またはアクセス スイッチに再接続されると、スパニング ツリーのトポロジ変更が必要になります。新しくアクティブになったルート ブリッジは、Bridge Protocol Data Unit（BPDU; ブリッジ プロトコル データ ユニット）フレームをセカンダリ ルートより低いプライオリティで送信し、ルート ブリッジの移動とそれに対応するレイヤ 2 トポロジの再計算をトリガーします。

802.1d トポロジの場合、ループのないトポロジなので、新しいトポロジへの移行により現在アクティブなポートがブロッキング ステートに移行されることはありません。したがってトラフィックは継続してセカンダリ ディストリビューション スイッチにブリッジングされ損失は発生しません。HSRP プリエンプトの使用により、アクティブ HSRP ゲートウェイはさらに 180 秒間セカンダリ スイッチ上に存続するので、ルート スイッチ上のポートがフォワーディング ステートに移行してもアクティブ トラフィック フローに影響しません。

802.1w トポロジの場合、プライマリ スイッチが再接続されると、アクセス スイッチ上のアップリンク ポートおよびプライマリ スイッチ上のダウンリンク ポートが指定ブロッキング ステートでアップになります。アクセス スイッチは新しくアクティブになったプライマリ ディストリビューション スイッチからより適切なルート BPDU を受信すると、最初にそのすべての非エッジ指定ポート（PortFast の設定されていないすべてのポート）をブロッキングしてトポロジの移行を開始します。すべての非エッジ ポートがブロックされると、アクセス スイッチは続いて新しいルート ブリッジとネゴシエーションを完了し、スパニング ツリー ループを引き起こすことなく、対応するアップリンク ポートを安全にフォワーディング ステートに移行します。新しいルート ポートがフォワーディング ステートに移行すると、アクセス スイッチは続いて、現在ブロックされている各指定ポートで同じネゴシエーション プロセスを完了し、必要な場合はそれらもフォワーディング ステートに移行します。

新しい ルート ポートへの移行時にすべての指定ポートをブロックする同期ステップは、802.1w スパニング ツリーのトポロジ計算に必要となりますが、副作用としてセカンダリ ディストリビューション スイッチへのアップリンクが一時的にブロッキングされます。セカンダリ ディストリビューション スイッチは依然としてアクティブ HSRP ゲートウェイなので、これによりすべてのアップストリーム トラフィックのアクティブ フォワーディング パスが失われます。ダウンストリーム トラフィックも同じ同期処理により影響を受けます。コアからセカンダリ ディストリビューション スイッチを通るトラフィックも、ポートのネゴシエーションとフォワーディング ステートに戻る期間中ブロックされます。

（注） 802.1w の動作の詳細については、次の URL にアクセスして『*Cisco AVVID Network Infrastructure:Implementing 802.1w and 802.1s in Campus Networks*』設計ガイドを参照してください。
http://www.cisco.com/application/pdf/en/us/guest/tech/tk621/c1501/ccmigration_09186a0080174993.pdf

構成 3 の結果 — HSRP、OSPF（Rapid-PVST+ 使用）

障害の分析

構成 3 の特性は次のとおりです。

- デフォルト ゲートウェイ プロトコル — HSRP
- スパニング ツリー バージョン — Rapid-PVST+（per VLAN 802.1w）
- IGP — OSPF

テスト結果の概要

表 9 に、テスト結果の概要を示します。

表 9　構成 3 の障害テスト結果

障害ケース	アップストリームの復旧	ダウンストリームの復旧	復旧メカニズム
アクティブ HSRP へのアップリンク ファイバの障害	900 ミリ秒	1650 ミリ秒	アップストリーム — HSRP ダウンストリーム — OSPF

表 9　構成 3 の障害テスト結果（続き）

スタンバイ HSRP へのアップリンク ファイバの障害	0 ミリ秒	1650 ミリ秒	アップストリーム — 損失なし ダウンストリーム — OSPF
アクティブ HSRP ディストリビューション スイッチの障害	800 ミリ秒	200 ミリ秒	アップストリーム — HSRP ダウンストリーム — L3 イコール コスト パス
スタンバイ HSRP ディストリビューション スイッチの障害	0 ミリ秒	200 ミリ秒	アップストリーム — 損失なし ダウンストリーム — L3 イコール コスト パス
ディストリビューション スイッチ間のファイバの障害	0 ミリ秒	0 ミリ秒	アクティブ データ パスの損失なし

OSPF への変換の影響

冗長キャンパス設計では、ネットワーク上で宛先への新しいルートの再計算が必要になるのは、アクセス スイッチとディストリビューション スイッチ間のアップリンク障害が発生した場合に限られます。他のすべての障害の場合、フォワーディング パスの復旧は、デフォルト ゲートウェイ（HSRP）の冗長性およびイコール コスト パスのルート変更のいずれかに依存します。アクセス スイッチのアップリンク障害の場合、冗長パスが存在できないのでネットワークはルート変更を開始する必要があります。この障害ケースの OSPF コンバージェンスは、EIGRP コンバージェンスよりも悪化する傾向があります。これは 2 つのプロトコル固有の動作の違いによるものです。

アクセス スイッチのアップリンク障害が発生すると、ディストリビューション スイッチはネットワークのルート変更をトリガーする必要が生じます。集約ルートをコアに通知するようにネットワークが設定されている場合（ディストリビューション ブロックがスタンドアロンの OSPF エリアとして設定されている場合）、この障害のルート変更は 2 つのディストリビューション スイッチを接続しているリンクを通ります。これとは逆に、ルート集約の必要のない単一エリアとしてキャンパス全体が設定されている場合、1 つのディストリビューション スイッチからダウンストリーム ルートが失われたことをコア ノードが確認すると、コア ノード上でルート変更が発生します。この時点まで EIGRP と OSPF の動作は一致しています。両プロトコルは集約ディストリビューション ブロック内か、または集約が設定されていない場合はコア内でルート変更を開始します。

EIGRP がこのルート変更を完了するために必要な時間は、クエリー処理と応答処理の効率に大きく依存します。適切に集約された設計では、クエリー処理の効率が高く、コンバージェンス時間が予測可能な範囲にあります。

（注）　EIGRP のコンバージェンス動作の詳細については、前述の障害ケース 1 の分析を参照してください。

EIGRP と比較した場合、OSPF がコンバージェンスを完了するために必要な時間は LSA アップデートを交換する時間、Shortest Path First（SPF）ツリーを計算する時間、およびこれらの両方のイベントの発生レートに対する制限メカニズムの存在によって決まります。

OSPF 構成の場合、実際のルートの変更は HELLO の消失とデッド タイマーの期限切れではトリガーされません。802.3z または 802.3ae のリモート障害検出機能によってインターフェイスがダウン状態になることでトリガーされます。リンク ダウン イベントが通知されると、OSPF プロセスは LSA プロパゲーション スロットル タイマーを開始します。ルータはすぐにはアップデート

を送信しません。ある時間（デフォルトで 0.5 秒）待機して LSA をバッファリングしてから送信します。LSA の送信後に新しい LSA アップデートを受信すると、もう 1 つのスロットル タイマーである SPF タイマーが開始されます。

この 2 番めのタイマーの期限が切れると SPF の計算が実行されます。新しいルートがあればルーティング テーブルに入力され、対応する CEF フォワーディング エントリが作成されます。LSA 伝播スロットル タイマーと SPF スロットル タイマーは、ネットワークの単一イベントに応答して実行される SFP 計算の回数を減らし、局所的なトポロジ情報による不正確または不完全なルート アップデートを抑制するために必要です。

このテスト時の記載されている 1600 ミリ秒のコンバージェンス時間は、リンク障害の検出、LSA の伝播、SPF の計算、および新しいルートの挿入（スロットル タイマーの時間を含む）に OSPF が費やした時間の合計です。これらのテスト ケースに関しては、ネットワーク内のすべてのノードの SPF タイマーは 1 秒に短縮されています（次の設定を参照）。

```
router ospf 100
 router-id 10.122.0.3
 log-adjacency-changes

timers spf 1 1  <<< Reduce SPF Timers to 1 second

 area 120 stub no-summary
 area 120 range 10.120.0.0 255.255.0.0
 network 10.120.0.0 0.0.255.255 area 120
 network 10.122.0.0 0.0.255.255 area 0
```

Cisco IOS Release 12.2(17b) SXA 以降、Sub-Sec SFP タイマーの導入によって SPF チューニングのコンフィギュレーション構文が変わりました。

```
router ospf 100
 router-id 10.122.0.3
 log-adjacency-changes

timers throttle spf 1000 1000 1000  <<< One second SPF using 12.2(17b)SXA and later
IOS

 area 120 stub no-summary
 area 120 range 10.120.0.0 255.255.0.0
 network 10.120.0.0 0.0.255.255 area 120
 network 10.122.0.0 0.0.255.255 area 0
```

（注） Sub-Sec の SFP スロットル タイマーを設定する方法については、次の CCO マニュアルを参照してください。
http://www.cisco.com/en/US/docs/ios/12_2t/ip_route/command/reference/p2ftospf.html

復旧の分析

構成 3 の特性は次のとおりです。

- デフォルト ゲートウェイ プロトコル — HSRP
- スパニング ツリー バージョン — Rapid-PVST+（per VLAN 802.1w）
- IGP — OSPF

テスト結果の概要

表 10 に、テスト結果の概要を示します。

表 10　構成 3 の復旧テスト結果

復旧ケース	アップストリームの復旧	ダウンストリームの復旧	復旧メカニズム
アクティブ HSRP へのアップリンク ファイバの復旧	180 ミリ秒	180 ミリ秒	アップストリーム — 802.1w ダウンストリーム — 802.1w
スタンバイ HSRP へのアップリンク ファイバの復旧	0 ミリ秒	180 ミリ秒	アップストリーム — 損失なし ダウンストリーム — 802.1w
アクティブ HSRP ディストリビューション スイッチの復旧	180 ミリ秒	180 ミリ秒 ～ 6 秒の間で変動	アップストリーム — 802.1w ダウンストリーム — 802.1w、L3 イコール コスト パス、および ARP
スタンバイ HSRP ディストリビューション スイッチの復旧	180 ミリ秒	180 ミリ秒 ～ 6 秒の間で変動	アップストリーム — 802.1w ダウンストリーム — 802.1w、L3 イコール コスト パス、および ARP
ディストリビューション スイッチ間のファイバの復旧	0 秒	0 秒	アクティブ データ パスの損失なし

OSPF への変換の影響

冗長キャンパス設計では、リンクがアクティブにされた場合とノードが再起動された場合のネットワークの動作は同じで、使用されるルーティング プロトコル（OSPF または EIGRP）とは関係ありません。トラフィックが失われるケースは、前述のテスト構成 1 および 2 での説明と同じです。802.1w の同期処理では、ルート ブリッジのトポロジ変更中にわずかですが目立ったトラフィックの損失が生じます。また、ARP DoS プロテクション機能では、前述の説明と同じ条件で同じトラフィックの中断が生じます。

構成 4 の結果 — GLBP、EIGRP（Rapid-PVST+ 使用）

障害の分析

構成 4 の特性は次のとおりです。

- デフォルト ゲートウェイ プロトコル — GLBP
- スパニング ツリー バージョン — Rapid-PVST+（per VLAN 802.1w）
- IGP — EIGRP

テスト結果の概要

表 11 に、テスト結果の概要を示します。

表 11　構成 4 の障害テスト結果（障害ケース）

障害ケース	アップストリームの復旧	ダウンストリームの復旧	復旧メカニズム
アクティブ GLBP へのアップリンク ファイバの障害	900 ミリ秒	800 ミリ秒	アップストリーム — GLBP ダウンストリーム — EIGRP
スタンバイ GLBP へのアップリンク ファイバの障害	900 ミリ秒	800 ミリ秒	アップストリーム — GLBP ダウンストリーム — EIGRP
アクティブ GLBP ディストリビューション スイッチの障害	800 ミリ秒	200 ミリ秒	アップストリーム — GLBP ダウンストリーム — L3 イコール コスト パス
スタンバイ GLBP ディストリビューション スイッチの障害	800 ミリ秒	200 ミリ秒	アップストリーム — GLBP ダウンストリーム — L3 イコール コスト パス
ディストリビューション スイッチ間のファイバの障害	0 ミリ秒	0 ミリ秒	アクティブ データ パスの損失なし

GLBP への変換の影響

同じタイマー設定を使用したときのファイバとノードの障害におけるワーストケースの復旧時間は、HSRP と GLBP ともに同じです。どちらの場合も、フェールオーバー メカニズムはネイバー通知の消失と仮想 MAC アドレスの引き継ぎに依存します。GLBP の実装では次の 2 つの違いがあります。

- 平均コンバージェンス時間は、どの単一コンポーネント障害時もフローの障害範囲が半分になるので、GLBP のほうが小さくなります。
- GLBP 設定では、アップリンクまたはディストリビューション スイッチの損失によって障害が発生します。

ダイナミック GLBP ロード バランシング メカニズムの特質により、各ディストリビューション スイッチをデフォルト ゲートウェイとして使用する端末数はどの時点でも全体の半数となります。端末の半数にアップストリーム トラフィックのトラフィック損失が生じ、端末の半数にダウンストリーム フローのトラフィック損失が生じるため、ワーストケースのコンバージェンスは GLBP を使用しても改善されません。統計上、アップストリームとダウンストリーム フローのどちらの影響をどの端末が受けたのかについて相関性はありません。最悪の場合、ネットワークのコンバージェンス中にすべての端末が停止する可能性があります。

（注） ダウンストリームのコンバージェンス時間を補完するために、テスト用の GLBP タイマーを選択しました。GLBP タイマーの値を小さくするとアップストリームのコンバージェンス時間が改善されますが、戻りパスのトラフィックには影響しません。

復旧の分析

構成 4 の特性は次のとおりです。

- デフォルト ゲートウェイ プロトコル — GLBP

- スパニング ツリー バージョン — Rapid-PVST+（per VLAN 802.1w）
- IGP — EIGRP

テスト結果の概要

表 12 に、テスト結果の概要を示します。

表 12　構成 4 の復旧テスト結果

復旧ケース	アップストリームの復旧	ダウンストリームの復旧	復旧メカニズム
アクティブ GLBP へのアップリンク ファイバの復旧	180 ミリ秒	180 ミリ秒	アップストリーム — 802.1w ダウンストリーム — 802.1w
スタンバイ GLBP へのアップリンク ファイバの復旧	0 ミリ秒	180 ミリ秒	アップストリーム — 損失なし ダウンストリーム — 802.1w
アクティブ GLBP ディストリビューション スイッチの復旧	180 ミリ秒	180 ミリ秒 ～ 6 秒の間で変動	アップストリーム — 802.1w ダウンストリーム — 802.1w、L3 イコール コスト パス、および ARP
スタンバイ GLBP ディストリビューション スイッチの復旧	180 ミリ秒	180 ミリ秒 ～ 6 秒の間で変動	アップストリーム — 802.1w ダウンストリーム — 802.1w、L3 イコール コスト パス、および ARP
ディストリビューション スイッチ間のファイバの復旧	0 秒	0 秒	アクティブ データ パスの損失なし

GLBP への変換の影響

デフォルト ゲートウェイの冗長性プロトコルを変更した場合、デバイスのアクティブ化への影響はありません。ネットワークにおける損失はすべてパケット損失によるもので、802.1w の同期処理、またはトラフィック量が非常に多いときに復旧に影響する ARP DoS プロテクション メカニズムのいずれかに起因するものです。

（注） これらの 2 つの動作に関する詳細については、前述のセクションを参照してください。

構成 5 の結果 — GLBP、EIGRP、Rapid-PVST+（レイヤ 2 ループ使用）

障害の分析

構成 5 の特性は次のとおりです。

- デフォルト ゲートウェイ プロトコル — GLBP
- スパニング ツリー バージョン — ループ型 Rapid-PVST+（per VLAN 802.1w）
- IGP — EIGRP

テスト結果の概要

表 13 に、テスト結果の概要を示します。

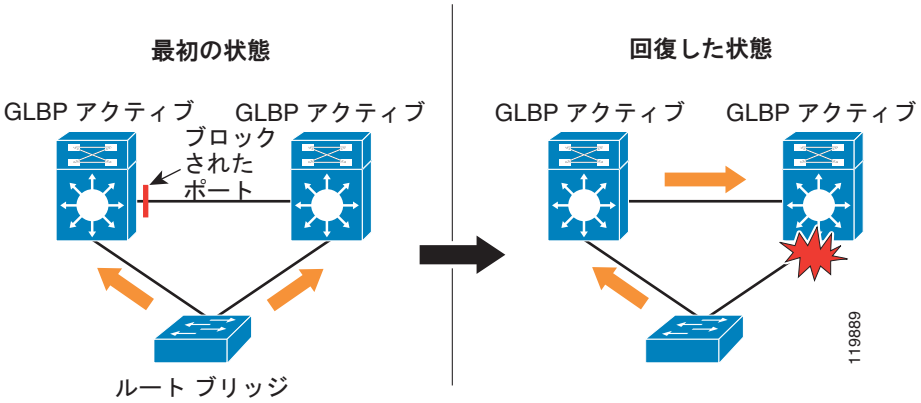
表 13　構成 5 の障害テスト結果（障害ケース）

	アップストリームの復旧	ダウンストリームの復旧	復旧メカニズム
アクティブ GLBP へのアップリンク ファイバの障害	400 ミリ秒	400 ミリ秒	アップストリーム — 802.1w ダウンストリーム — 802.1w
スタンバイ GLBP へのアップリンク ファイバの障害	400 ミリ秒	400 ミリ秒	アップストリーム — 802.1w ダウンストリーム — 802.1w
アクティブ GLBP ディストリビューション スイッチの障害	800 ミリ秒	200 ミリ秒	アップストリーム — GLBP ダウンストリーム — L3 イコール コスト パス
スタンバイ GLBP ディストリビューション スイッチの障害	800 ミリ秒	200 ミリ秒	アップストリーム — GLBP ダウンストリーム — L3 イコール コスト パス
ディストリビューション スイッチ間のファイバの障害	0 ミリ秒	0 ミリ秒	アクティブ データ パスの損失なし

アクセス VLAN にレイヤ 2 ループを導入する影響

レイヤ 2 スパニング ツリー ループを導入し、2 つのディストリビューション スイッチ間のトランクを通して VLAN を拡張すると、ループなしの設計と比較した場合に、単一ファイバ障害においてアップストリームとダウンストリームの両方のトラフィックの復旧時間が短縮されます。レイヤ 2 ループ型構成では、このトポロジでリンクが失われた場合の 802.1w の復旧に関しては HSRP と EIGRP にコンバージェンスは不要です（図 11 を参照）。

図 11　　レイヤ 2 ループ型構成での 802.1w の復旧



802.1w の導入前は、802.1d がリンクの障害を検出して冗長リンクのブロックを解除するよりもはるかに速く、HSRP と EIGRP のコンバージェンスを実行できました。ネットワークにループが導入されることにより、キャンパス設計の次の 2 つの機能が変更になります。

- 802.1w では、設定されている GLBP ピアのデッド タイマーが期限切れになる前に 2 つのピア間の接続を復元できます。これにより GLBP のフェールオーバーを回避できます。デッド タイマーが 800 ミリ秒に設定された GLBP と 802.1w では、400 ミリ秒を下回る時間で接続が復元されることが測定されました。
- 各ディストリビューション スイッチは各 VLAN 内に複数のポートを持っているため、ダウンストリーム ポートを 1 つ失っても autostate をトリガーしません。そのため、対応する Switched Virtual Interface（SVI; スイッチ仮想インターフェイス）はシャットダウンされません。その結果、EIGRP はルート コンバージェンスを開始せず、802.1w が 2 つのスイッチ間のレイヤ 2 接続を復元するまで待機してから、ネットワークは影響を受けたトラフィック フローを復元します。

ループ型レイヤ 2 トポロジを導入した場合、ディストリビューション スイッチの障害によるネットワーク コンバージェンス時間への影響はありません。この障害ではレイヤ 2 の冗長パスは存在しません。このため、ネットワークはデフォルト ゲートウェイの復旧を GLBP に依存し、ダウンストリーム トラフィックの復旧をコア内のイコール コスト パスに依存します。

（注）　レイヤ 2 スパニング ツリー ループをネットワークに導入するのは、現在推奨されるベスト プラクティスではありません。この構成を使用する設計を実装する前に、スパニング ツリー ループによりネットワークが停止する可能性があること、およびトラフィック復旧時間がわずかに改善される利点があることを比較検討してください。正しく使用すればループ型レイヤ 2 トポロジを使用するリスクの多くが軽減される機能（Loop Guard、UDLD、BPDU Guard）がありますが、レイヤ 2 サブネットの拡張を必要とするアプリケーションやビジネス要件がなければ、シスコはハイ アベイラビリティ キャンパス設計では L2 ループ構成を使用しないことを推奨します。最小のコンバージェンス復旧時間を提供する必要のあるネットワーク エンジニアの方は、このレイヤ 2 設計の実装ではなく、レイヤ 3 アクセス設計の採用検討してみてください。

復旧の分析

構成 5 の特性は次のとおりです。

- デフォルト ゲートウェイ プロトコル — GLBP
- スパニング ツリー バージョン — ループ型 Rapid-PVST+（per VLAN 802.1w）
- IGP — EIGRP

テスト結果の概要

表 14 に、テスト結果の概要を示します。

表 14　構成 5 の復旧テスト結果

復旧ケース	アップストリームの復旧	ダウンストリームの復旧	復旧メカニズム
アクティブ GLBP へのアップリンク ファイバの復旧	180 ミリ秒	180 ミリ秒	アップストリーム — 802.1w ダウンストリーム — 802.1w
スタンバイ GLBP へのアップリンク ファイバの復旧	0 ミリ秒	180 ミリ秒	アップストリーム — 損失なし ダウンストリーム — 802.1w
アクティブ GLBP ディストリビューション スイッチの復旧	180 ミリ秒	180 ミリ秒 ～ 6 秒の間で変動	アップストリーム — 802.1w ダウンストリーム — 802.1w、L3 イコール コスト パス、および ARP
スタンバイ GLBP ディストリビューション スイッチの復旧	180 ミリ秒	180 ミリ秒 ～ 6 秒の間で変動	アップストリーム — 802.1w ダウンストリーム — 802.1w、L3 イコール コスト パス、および ARP
ディストリビューション スイッチ間のファイバの復旧	0 秒	0 秒	アクティブ データ パスの損失なし

アクセス VLAN にレイヤ 2 ループを導入する影響

アクセス VLAN にスパニング ツリー ループを導入した場合、デバイスのアクティブ化によるアクティブなトラフィック フローへの影響に変わりはありません。ネットワーク内の損失は、すべてパケット損失によるものであり、802.1w の同期処理、または ARP DoS プロテクション メカニズムのいずれかに起因します。ARP DoS プロテクション メカニズムは、トラフィック量が非常に多い場合、復旧に影響します。

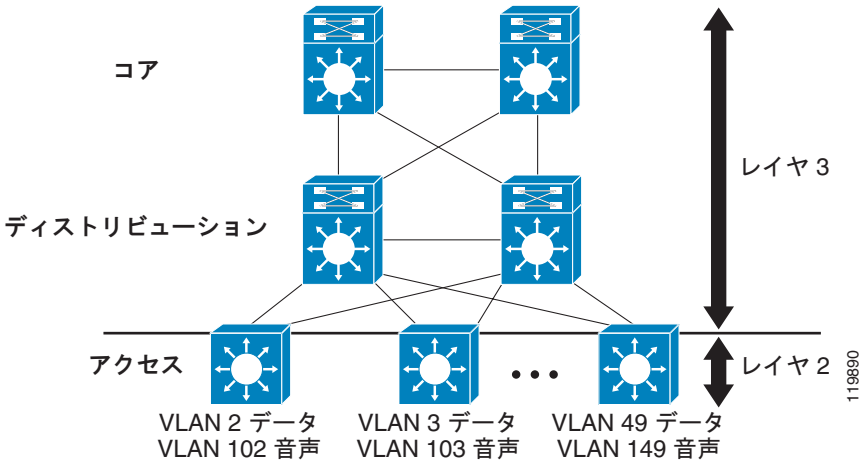
（注） これらの 2 つの動作に関する詳細については、前述の項を参照してください。

レイヤ 3 ディストリビューションのコンバージェンスを伴うレイヤ 3 ルーテッド アクセス — 結果および分析

レイヤ 3 ルーテッド アクセスの概要

標準のレイヤ 2 アクセス ディストリビューション ビルディング ブロック設計の代替案には、ルーテッド アクセス、つまりエッジまでレイヤ 3 を実装する設計があります（図 12 を参照）。

図 12　　レイヤ 3 ルーテッド アクセスの実装



音声 VLAN 102、103、および 149

この設計では、アクセス スイッチはキャンパス ルーティング プロトコルに参加する完全なレイヤ 3 ルーティング ノードとして設定されます。レイヤ 2 と 3 の境界は、ディストリビューション スイッチからキャンパス ネットワークのエッジにあるアクセス スイッチに移されます。ローカルの音声およびデータ VLAN からのトラフィックは、ディストリビューション スイッチへのブリッジド アップストリームではなく、ルーテッド アップストリームになります。

この設計は標準のディストリビューション ビルディング ブロックと非常に異なっているように見えますが、多くの類似点があります。両方の設計とも、各アクセス スイッチには専用の音声およびデータのサブネット（VLAN）が設定されています。また、ルーティング ノード間のすべてのリンクがポイントツーポイントとして設定されています。一番の違いはデフォルト ゲートウェイの場所です。

従来からの設計では、デフォルト ゲートウェイはディストリビューション ノードに存在し、アクセス スイッチとディストリビューション スイッチの間のリンクを使用してデータおよび音声 VLAN をディストリビューション ルータまで伸ばしています。レイヤ 3 アクセス設計では、デフォルト ゲートウェイはアクセス スイッチ上に存在し、アップリンクは /30 または /31 のアドレッシングを使用する専用のポイントツーポイント サブネットとして設定されています。

EIGRP の結果

EIGRP 障害結果

レイヤ 3 アクセス設計では考慮する障害ケースが少なくなります。レイヤ 2 と 3 の境界がディストリビューションからアクセス スイッチに移ることにより、一部の障害シナリオは該当しなくなりました。デフォルト ゲートウェイ機能がエッジ スイッチに分散されたことにより、冗長デフォルト ゲートウェイ メカニズムが不要になりました。キャンパス設計には、HSRP/GLBP のチューニングとコンバージェンス時間は影響しません。スパニング ツリー インスタンスは 1 つのスイッチで実行されるため、コンバージェンス時間に影響しません。このルーテッド アクセス キャンパスは、キャンパス スイッチの L3 コンバージェンス動作および使用するルーティングのコンバージェンス動作に全面的に依存します。

アクセス スイッチでレイヤ 3 を実行することにより、すべてのアップストリームとダウンストリーム トラフィック フローについて、ダイナミック ロード バランシングが行われます。アクセスおよびディストリビューション間のイコール コスト ルートにより、2 つのアップリンク間でコアへ向かうアップストリームの負荷が分割されます。各コア ノード上のイコール コスト パスにより、2 つのディストリビューション スイッチ間で負荷が分割され、その結果ディストリビューションからアクセスへのダウンストリームの戻りパスの負荷が対称になります。この負荷の均衡化または対称化により、レイヤ 3 キャンパス設計では、どのノードまたはリンクに障害が発生しても、ネットワーク内の最大でも約半分のトラフィック フローしか影響を受けなくなります。リンクまたはノードの障害で 1 つのパスに障害が生じた場合は、そのパスを使用するフローだけに影響が生じます。

（注） 対称負荷は統計上の数値です。フロー数だけが考慮され、ネットワークを中継するバイト数は考慮されていません。G.711 音声ストリームと端末ディスクのバックアップという 2 つのトラフィック フローだけの極端なケースでは、bps で測定された各アップリンク上の負荷は等しくありません。ただし、この 2 つのフローが 2 つのアップリンクそれぞれに転送される確率はどちらも同じです。フロー数が増えるに従い、測定される平均負荷の値はフロー数でもバイト数でも等しくなる傾向にあります。

レイヤ 3 アクセス設計では、コンバージェンス動作を評価する際に次の 3 つのケースを考慮する必要があります。

- アクセス スイッチとディストリビューション スイッチ間のアップリンク ファイバの障害
- ディストリビューション スイッチの障害
- ディストリビューション スイッチ間のファイバの障害

レイヤ 3 アクセス設計のダイナミック ロード バランシングの特性により、ケース 1 と 2 はアクセス スイッチからディストリビューション ノードの障害またはディストリビューション ノードへのアップリンクの障害に相当します。

表 15 に、この 3 つの障害ケースの結果を示します。

表 15　　3 つの障害ケースのテスト結果（障害ケース）

	アップストリームの復旧	ダウンストリームの復旧	復旧メカニズム
アップリンク ファイバ障害	150 ミリ秒	200 ミリ秒	アップストリーム — L3 イコール コスト パス ダウンストリーム — EIGRP

表 15　3 つの障害ケースのテスト結果（障害ケース）（続き）

ディストリビューション スイッチの障害	150 ミリ秒	200 ミリ秒	アップストリーム — L3 イコール コスト パス ダウンストリーム — EIGRP
ディストリビューション スイッチ間のファイバの障害	0 ミリ秒	0 ミリ秒	アクティブ データ パスの損失なし

アクセス スイッチとディストリビューション スイッチ間のアップリンク ファイバの障害

ルーテッド アクセス設計では、アクセス スイッチからコアへ向かって流れるアップストリーム トラフィックのコンバージェンス時間は、主にディストリビューション スイッチへのリンク損失の検出に依存します。リンク障害を検出すると、スイッチはリンク ダウン イベントを処理して、障害インターフェイスに関連するすべてのルートと CEF ハードウェア フォワーディング エントリを削除します。両方のディストリビューション スイッチから通知されるイコール コスト ルートを使用する推奨構成では、それに続いて、残っているハードウェア CEF エントリを使用しすべてのアップストリーム トラフィック フローが転送されます。イコール コスト ルート構成では、EIGRP がすべてのアップストリームの宛先への有効なルートを持っているので、ソフトウェアによるルートの再計算は必要ありません。

前述のルーテッド コア設計で注記したように、すべてのアップリンク インターフェイスで 802.3z または 802.3ae のリンク ネゴシエーションをイネーブルにしておき、ファイバ障害またはアップストリーム ノード障害に起因するリンク損失をリモート障害検出メカニズムが検出できるようにする必要があります。リンク ネゴシエーションをディセーブルにすると、アップストリーム フローとダウンストリーム フローともにコンバージェンス時間が増加します。

アクセスとディストリビューション間のファイバ障害時におけるダウストリームの復旧時間は EIGRP のルート変更に依存します。冗長レイヤ 3 アクセス キャンパスでは、1 つを除くすべてのケースでルーティング プロトコルのコンバージェンスを不要にすることができます。各ディストリビューション スイッチは、アクセス スイッチごとに音声およびデータ サブネットへのパスを 1 つ持っています。このパスが失われると、ディストリビューション スイッチはそのリンクに対応するアクセス ネットワークまたはルートを対象に EIGRP アクティブ ステートに移行します。ディストリビューション ノードは、両方のコア スイッチとディストリビューション ピアに代替パスの照会を行います。

最適なコンバージェンスを得られるように、シスコは各ディストリビューション ビルディング ブロック内のすべてのルートをアップストリームからコアに集約することを推奨します。コア上に集約ルートが存在するとコア ノードはネットワークの他の部分にクエリーを伝播しないので、クエリーの抑制とコンバージェンス時間の抑制に役立ちます。クエリー処理を迅速に完了する能力は、生成側スイッチと受信側スイッチの EIGRP クエリーを処理する能力にも左右されます。

スイッチに高い CPU 負荷をもたらすワーム、DDoS 攻撃、スパニング ツリーのループなどの異常なイベントからネットワークを確実に保護することも、コンバージェンス時間を確実に予測するために必要です。

ディストリビューション スイッチの障害

ディストリビューション ノードの障害の場合、アクセス スイッチからコアに向かって流れるアップストリーム トラフィックの復旧は、ディストリビューション スイッチへのリンク損失の検出に依存します。スイッチ間のファイバの損失またはディストリビューション スイッチの障害は、アクセス スイッチには同じイベントとして表れます。この動作および注意事項は前述の場合と同じです。

ディストリビューション スイッチの障害時のダウンストリームのコンバージェンスは、コア スイッチのイコール コスト パス障害の動作に依存します。各コア スイッチは、ディストリビューション ブロック ネットワークへの 2 つのイコール コスト ルートを持っています。ディストリビューション スイッチいずれかに障害が発生すると、コア スイッチは無効なルートおよび対応

するハードウェア CEF エントリを削除します。EIGRP はディストリビューション ブロック ネットワークに対する有効なルートを持っており、どのルートに対してもアクティブにならず、ルートの再計算を実行しません。

ディストリビューション スイッチ間のファイバの障害

正常な動作状態では、ディストリビューション スイッチ間のファイバ パスで音声データまたはアプリケーション データ トラフィックが伝送されることはありません。このパスは、アクセスとディストリビューション間のリンク障害が発生した場合に、アプリケーションと音声トラフィックのバックアップ パスとして機能します（前述の構成 1 を参照）。したがって、単一障害のシナリオでは、このリンクが失われても音声とアプリケーション トラフィックのフローに影響しません。

EIGRP の復旧結果

前述のレイヤ 3 コア設計におけるコンポーネントの復旧の調査から分かるように、レイヤ 3 アクセス設計でのリンクとノードの復旧は非常に安定しており、予測可能なプロセスです。レイヤ 3 フォワーディングは、新しいリンクのアクティブ化を反映してルーティング テーブルが変更されるまで発生しません。ルーティング テーブルのアップデートは、新しくアクティブ化されたリンクの両側でネイバーディスカバリとネゴシエーションを完了するまで発生しません。

フォワーディング テーブルは、音声とデータ トラフィックを正常に転送できることがすべてのスイッチで確認されるまで変更されません。エンドツーエンド IGP を使用すると、レイヤ 3 アクセス スタティック ルート設計に関連する問題を回避できます。これは、トラフィックの転送が確認済みの有効なネットワーク パスではなく、リンク アクティブ化だけに基づいて行われるという問題です。EIGRP アクセス設計を使用すると、スタティック ルートの実装に関連するブラック ホールの問題を回避できます。

リンクおよびデバイスの復旧のコンバージェンスのケースは、次のように障害シナリオのコンバージェンス ケースと同じです（表 16 を参照）。

- アクセスとディストリビューション スイッチの間のアップリンク ファイバ復旧
- ディストリビューション スイッチの復旧
- ディストリビューション スイッチ間のファイバ復旧

表 16　EIGRP の復旧ケース

	アップストリームの復旧	ダウンストリームの復旧	復旧メカニズム
アップリンク ファイバの復旧	0 秒	0 秒	アクティブ データ パスの損失なし
ディストリビューション スイッチの復旧	0 秒	0 秒	アクティブ データ パスの損失なし
ディストリビューション スイッチ間のファイバ復旧	0 秒	0 秒	アクティブ データ パスの損失なし

冗長設計のリンクまたはノードの復旧時に、アクティブなフォワーディング パスは失われません。2 つめのリンクまたはノードのアクティブ化により、EIGRP ネイバーディスカバリ / 確立が行われ、2 つめのイコール コスト ルートがルーティング テーブルに挿入されるか、または既存ルートが新規のより適切なコストのルートに置き換えられます。新しいルートが確立されると、各スイッチは自身のハードウェア CEF エントリをアップデートして新しいルートを反映させ、新しいパスを通してすべての既存フローと新しいフローを転送します。ルーティング プロトコルのアップデート処理中、スイッチは既存のハードウェア フォワーディング エントリを継続して使用するので、新しいルートの挿入が原因でデータを失うことはありません。

アクセスとディストリビューションの間のリンクの復旧により、アクセス スイッチにアップストリーム ネットワークへの 2 つめのイコール コスト ルートが追加されます。ディストリビューション スイッチは、復旧されたファイバを使用してより適切なルートを学習し、古いルートと CEF エントリを新しいルートに交換します。ディストリビューション スイッチは、コアへのアップストリーム リンクに集約範囲が設定されているので、新しいルート情報をコアに伝播しません。EIGRP 設計では、アップリンクをアクティブ化することによる影響はほとんどありません。

ディストリビューション スイッチの復旧により、2 つめのイコール コスト パスがアクセス スイッチとコア スイッチの両方に挿入されます。その結果、コア スイッチはディストリビューション ブロック集約アドレス範囲への 2 つめのルートを学習し、アクセス スイッチは 2 つめのデフォルト ルートを学習します。どちらの場合も、2 つめのイコール コスト ルートを挿入することによる影響は無視できます。コア スイッチは、より適切なパスを学習したのではなく、同じネットワークに対する同じコストを持った 2 つめのトポロジとルート エントリであったことから、アップデートされたルーティング情報を他の接続スイッチに伝播することはしません。EIGRP 設計では、アップリンクをアクティブ化することによる影響はほとんどありません。

大規模なオーバーサブスクライブ型ネットワークの場合、新しいルート（より適切なパス ルートまたは 2 つめのイコール コスト ルート）を挿入している間の移行期間に、新しい パス上で送信された既存フローのパケットの順序が前後して到着する可能性があります。これは、元のパスの負荷が高いことによる重大な輻輳が原因となり、伝送遅延が生じる場合にのみ発生することがあります。

大規模なオーバーサブスクライブ型（ワーストケース）負荷を使用したテスト時に、アクティブな音声フローの 0.003 パーセントに満たない割合で、単一パケット損失が発生したことが測定されました。2 つめのリンクのアクティブ化により生じた、この非常に低いレベルのパケット損失とそれに関連する低いレベルのジッタによる影響および音声ストリームのフォワーディング パスのダイナミックな変更による影響は、テスト ストリームの MOS スコアの記録には表れませんでした。冗長レイヤ 3 キャンパス設計では、既存のトラフィック フローに動作上の影響を及ぼすことなく新しいリンクまたはノードをアクティブ化することができます。

OSPF の結果

OSPF の障害結果

ルーテッド レイヤ 3 アクセス設計では、IGP の選択肢を変更しても、ネットワークの設計の大幅な変更や、評価対象の障害ケースの変更が生じることはありません。EIGRP での分析と同じ次の 3 つの障害イベントを OSPF でも調査する必要があります。

- アクセスとディストリビューション スイッチの間のアップリンク ファイバ障害
- ディストリビューション スイッチの障害
- ディストリビューション スイッチ間のファイバの障害

EIGRP から OSPF に変換した場合、最初の障害ケースの、ネットワークのコンバージェンス動作が影響を受けます。これは障害が発生したときのルーティング プロトコルの動作に違いがあるためです（表 17 を参照）。

表 17　　OSPF の障害結果（障害ケース）

	アップストリームの復旧	ダウンストリームの復旧	復旧メカニズム
アップリンク ファイバ障害	150 ミリ秒	1650 ミリ秒	アップストリーム — L3 イコール コスト パス ダウンストリーム — OSPF

表 17　OSPF の障害結果（障害ケース）（続き）

ディストリビューション スイッチの障害	150 ミリ秒	200 ミリ秒	アップストリーム — L3 イコール コスト パス ダウンストリーム — OSPF
ディストリビューション スイッチ間のファイバの障害	0 ミリ秒	0 ミリ秒	アクティブ データ パスの損失なし

アクセス スイッチとディストリビューション スイッチの間のアップリンク ファイバの障害

OSPF 環境で、アクセス スイッチからコアに向かって流れるアップストリーム トラフィックの復旧が主としてディストリビューション スイッチへのリンク損失の検出に依存する点は、EIGRP と変わりません。リンク障害を検出すると、スイッチはリンク ダウン イベントを処理して、障害インターフェイスに関連するすべてのルートと CEF ハードウェア フォワーディング エントリを削除します。

アップストリームの復旧を高速に行うための基本的な設計上の推奨事項は、EIGRP ネットワークの場合と同じように OSPF ネットワークにも当てはまります。それはディストリビューションとアクセスの間のイコール コスト ルートを通知し、リンク ネゴシエーションがイネーブルになっていることを確認することです。

アクセスとディストリビューションの間のファイバ障害時におけるダウストリームの復旧時間は OSPF のルート変更に依存します。このパスが失われると、ディストリビューション スイッチは LSA スロットル タイマーの時間だけ待機したあと、リンク ステータスの変更を知らせる LSA を生成します。スイッチは自身の新しい LSA をフラッディングさせると、SPF スロットル タイマーに基づいた設定時間を待機し、エリア内の他のスイッチにより通知される LSA の受信を待機します。このタイマーが期限切れになると、SPF 計算が実行され、新しいルートおよび対応するハードウェア CEF エントリが挿入されます。

トポロジの再計算には本質的にプロセッサとメモリにより大きな負荷がかかり、常にエリア内のすべてのルータが関与することから、OSPF はトポロジ変更の回数と頻度を減らすために LSA と SPF のスロットリング メカニズムを実装しています。コンバージェンスに要する時間とダウンストリーム トラフィック フローの復元に要する時間は、主として OSPF スロットル タイマーの設定に依存します。この時間はさらに、スイッチの LSA を処理する能力と SPF を計算する能力にも依存します。スイッチに高い CPU 負荷をもたらす異常なイベント（ワーム、DDoS 攻撃、スパニング ツリーのループ）からネットワークを確実に保護することも、コンバージェンス時間を確実に予測するために必要です。

ディストリビューション スイッチの障害

ディストリビューション ノードの障害の場合、アクセス スイッチからコアに向かって流れるアップストリーム トラフィックの復旧は、依然としてディストリビューション スイッチへのリンク損失の検出に依存します。スイッチ間のファイバの損失またはディストリビューション スイッチの障害は、アクセス スイッチには同じイベントとして表れます。この動作および注意事項は前述の場合と同じです。

ディストリビューション スイッチの障害時のダウンストリームのコンバージェンスは、コア スイッチのイコール コスト パス障害の動作に依存します。各コア スイッチは、ディストリビューション ブロック ネットワークへの 2 つのイコール コスト ルートを持っています。ディストリビューション スイッチいずれかに障害が発生すると、コア スイッチは無効なルートおよび対応するハードウェア CEF エントリを削除します。リンク損失により、両方のコア ルータおよびそのピアのディストリビューション スイッチ上の OSPF は LSA フラッディングを開始し、OSPF エリア内のすべてのスイッチは SPF 計算を完了する必要があります。冗長キャンパス設計では、障害のディストリビューション ノードに直接接続されている 3 台のスイッチを除いて、エリア内のどのスイッチにもこのプロセスによるルーティングの変更は起きません。

ディストリビューション スイッチ間のファイバの障害

正常な動作状態では、ディストリビューション スイッチ間のファイバ パスで音声データまたはアプリケーション データ トラフィックが伝送されることはありません。このパスは、アクセスとディストリビューションの間のリンク障害が発生した場合に、アプリケーションと音声トラフィックのバックアップ パスとして機能します（前述のケース 1 を参照）。したがって、単一障害のシナリオでは、このリンクが失われた場合に OSPF エリア内のすべてのスイッチで LSA フラッディングと SPF 再計算が行われますが、音声とアプリケーション トラフィック フローへの影響はありません。

OSPF の復旧結果

ルーテッド アクセス OSPF 設計でのリンクとノードの復旧は、1 つの重要な例外がありますが、ほぼ予測が可能です。通常、レイヤ 3 フォワーディングは、新しいリンクのアクティブ化を反映してルーティング テーブルが変更されるまで発生しません。ルーティング テーブルのアップデートは、新しくアクティブにされたリンクの両側でネイバーディスカバリとネゴシエーションを完了するまで発生しません。フォワーディング テーブルは、音声とデータ トラフィックを正常に転送できることがすべてのスイッチで確認されるまで変更されません。このケースの例外については、復旧ケース 2：ディストリビューション スイッチの復旧の分析に含めて下記に説明します。

- アクセスとディストリビューション スイッチの間のアップリンク ファイバ復旧
- ディストリビューション スイッチの復旧
- ディストリビューション スイッチ間のファイバ復旧

表 18 に、テスト結果の概要を示します。

表 18　OSPF の復旧結果（復旧ケース）

	アップストリームの復旧	ダウンストリームの復旧	復旧メカニズム
アップリンク ファイバの復旧	0 秒	0 秒	アクティブ データ パスの損失なし
ディストリビューション スイッチの復旧	0–>45 秒	0 秒	アクティブ データ パスの損失なし
ディストリビューション スイッチ間のファイバ復旧	0 秒	0 秒	アクティブ データ パスの損失なし

アクセスとディストリビューション スイッチの間のアップリンク ファイバ復旧

冗長設計のリンクまたはノードの復旧時に、アクティブなフォワーディング パスは失われません。2 つめのリンクまたはノードのアクティブ化により、OSPF ネイバーディスカバリ / 確立が行われ、2 つめのイコール コスト ルートがルーティング テーブルに挿入されるか、または既存ルートが新規のより適切なコストのルートに置き換えられます。新しいルートが確立されると、各スイッチは自身のハードウェア CEF エントリをアップデートして新しいルートを反映させ、新しいパスを通してすべての既存フローと新しいフローを転送します。ルーティング プロトコルのアップデート処理中、スイッチは既存のハードウェア フォワーディング エントリを継続して使用するので、新しいルートの挿入が原因でデータを失うことはありません。

アクセスとディストリビューションの間のリンクの復旧により、アクセス スイッチにアップストリーム ネットワークへの 2 つめのイコール コスト ルートが追加されます。ディストリビューション スイッチは、復旧されたファイバを使用してより適切なルートを学習し、古いルートと CEF エントリを新しいルートに交換します。ディストリビューション スイッチは、コアへのアップストリーム リンクに集約範囲が設定されているので、新しいルート情報をコアに伝播しません。OSPF 設計では、アップリンクをアクティブ化することによる影響はほとんどありません。

大きなオーバーサブスクライブ型ネットワークの場合、新しいルート（より適切なパス ルートまたは 2 つめのイコール コスト ルート）を挿入している間の移行期間に、新しいパス上で送信された既存フローのパケットの順序が前後して到着する可能性があります。これは、元のパスの負荷が高いことによるひどい輻輳が原因となり、伝送遅延が生じる場合にのみ発生することがあります。大きなオーバーサブスクライブ型（ワーストケース）負荷を使用したテスト時に、アクティブな音声フローの 0.003 パーセントに満たない割合で、単一パケット損失が発生したことが測定されました。

2 つめのリンクのアクティブ化により生じた、この非常に低いレベルのパケット損失とそれに関連する低いレベルのジッタによる影響および音声ストリームのフォワーディング パスのダイナミックな変更による影響は、テスト ストリームの MOS スコアの記録には表れませんでした。冗長レイヤ 3 キャンパス設計では、既存のトラフィック フローに動作上の影響を及ぼすことなく新しいリンクまたはノードをアクティブ化することができます。

ディストリビューション スイッチの復旧

ディストリビューション スイッチの復旧時の動作は、そのディストリビューション スイッチの OSPF エリア階層内における役割により異なります。ここに記載されている結果は、次の OSPF 設計に基づいています。

- ディストリビューション ビルディング ブロックが 1 つの OSPF エリアになっている
- ディストリビューション エリアが完全スタブ エリアとして実行されている
- ディストリビューション スイッチが Area Border Router（ABR; エリア境界ルータ）になっている

ディストリビューション スイッチがアクティブ化されると、コアのコンバージェンスが生じ、2 つめの ABR が追加され対応する集約ルートがエリア 0 に通知されます。この処理はデータを損失することなく完了します。エリア内のコンバージェンスでは、完全スタブ エリアに付随する固有の問題が生じる可能性があります。ディストリビューション ABR はアクティブ化されると、2 つ以上のネイバーとの確立が完了するとすぐにダウンストリームのネイバー アクセス スイッチにデフォルト ルートを通知し始めます。このデフォルト ルートの通知は、コアとのネイバー関係の形成によるものでなく、アクセス スイッチを含む他のスイッチとのネイバー関係を使用して生成されます。

その結果、ディストリビューション ルータは、コアにデータをルーティングできるようになる前に、アクセス スイッチにデフォルト ルートを通知する可能性があります。アクセス スイッチは 2 つのデフォルト ルートを持ちます。1 つはコアに転送を行っている既存のディストリビューション スイッチからのもので、もう 1 つはコアにアクセスできない新しくアクティブ化されたスイッチからのものです。ディストリビューション スイッチがトラフィックをブラック ホール化する時間は、ラインカードの起動する順序、CPU、他のスイッチの負荷などいくつもの要素に依存します。

（注） OSPF 設計の選択肢に関する説明および根拠の詳細については、ハイ アベイラビリティ キャンパスおよびキャンパス レイヤ 3 アクセスの設計ガイドを参照してください。

ディストリビューション スイッチ間のファイバ復旧

正常な動作状態では、ディストリビューション スイッチ間のファイバ パスで音声データまたはアプリケーション データ トラフィックが伝送されることはありません。このパスは、アクセスとディストリビューションの間のリンク障害が発生した場合に、アプリケーションと音声トラフィックのバックアップ パスとして機能します（前述のケース 1 を参照）。このリンクをアクティブ化すると、OSPF 内のすべてのスイッチで LSA フラッディングと SPF 再計算が行われますが、音声またはデータ トラフィックの損失は発生しません。

テスト構成

ここでの内容は、つぎのとおりです。

- コア スイッチ構成（p.41）
- レイヤ 2 アクセスおよびディストリビューション ブロックのスイッチ構成（p.44）
- レイヤ 3 アクセスおよびディストリビューション ブロックのスイッチ構成（p.53）

コア スイッチ構成

すべてのテスト ケースに使用されたコアスイッチの構成を下記に示します。階層型設計ルールに従うことで、コア構成を変更することなくディストリビューション ビルディング ブロック内の構成を変更することができました。同様に残りの個別のテスト ケースで変更が必要になることはありませんでした。

このテスト設計は、複雑なポリシー管理を導入しないというベスト プラクティスの推奨事項に従いましたが、1 つ例外があります。コア スイッチはマルチキャスト ルート ポイントとして設定されました。これはマルチキャスト設計オプションの代表ケースとして選択されました。

（注） マルチキャスト設計オプションの詳細については、次の Web サイトにアクセスして『*Multicast Design Guides*』を参照してください。
http://www.cisco.com/en/US/tech/tk828/tech_design_guides_list.html

コア スイッチ構成（EIGRP）

```
key chain eigrp
 key 100

  key-string 7 01161501
!
! Enabled spanning tree as a fail-safe practice
spanning-tree mode rapid-pvst
!
redundancy

 mode sso

 main-cpu
  auto-sync running-config
  auto-sync standard

!
! Configure necessary loopback interfaces to support Multicast MSDP and Anycast for
! RP redundancy
interface Loopback0

 description MSDP PEER INT

 ip address 10.122.10.2 255.255.255.255
!
interface Loopback1

 description ANYCAST RP ADDRESS

 ip address 10.122.100.1 255.255.255.255
!
interface Loopback2
```

```
 description Garbage-CAN RP

 ip address 2.2.2.2 255.255.255.255
!
! Configure point to point links to Distribution switches
interface TenGigabitEthernet3/1

 description 10GigE to Distribution 1
! Use of /31 addressing on point to point links optimizes use of IP address space in
! the campus

 ip address 10.122.0.27 255.255.255.254

 ip pim sparse-mode
! Reduce EIGRP hello and hold timers to 1 and 3 seconds. In a point-point L3 campus
! design the EIGRP timers are not the primary mechanism used for link and node
! failure detection. They are intended to provide a fail-safe mechanism only.

 ip hello-interval eigrp 100 1
 ip hold-time eigrp 100 3
 ip authentication mode eigrp 100 md5
 ip authentication key-chain eigrp 100 eigrp
 load-interval 30

! Reduce carrier delay to 0. Tuning carrier delay no longer has an impact on GigE and
! 10GigE interfaces but is recommended to be configured as a best practice for network
! operational consistency

 carrier-delay msec 0
! Configure trust DSCP to provide for maximum granularity of internal QoS queuing

 mls qos trust dscp
!
router eigrp 100
! Passive all interfaces not intended to form EIGRP neighbors

 passive-interface Loopback0
 passive-interface Loopback1
 passive-interface Loopback2
 network 10.0.0.0
 no auto-summary

! Explicitly configure the EIGRP router id as a best practice when using Anycast and/or
! any identical loopback address on multiple routers.

 eigrp router-id 10.122.0.1
!
! Multicast route point and MSDP configuration.

! For a detailed explanation on the specifics of the configuration below please see
! the campus chapter of the multicast design guides.
ip pim rp-address 2.2.2.2
ip pim rp-address 10.122.100.1 GOOD-IPMC override
ip pim accept-register list PERMIT-SOURCES
ip msdp peer 10.122.10.1 connect-source Loopback0
ip msdp description 10.122.10.1 ANYCAST-PEER-6k-core-left
ip msdp cache-sa-state
ip msdp originator-id Loopback0
!
ip access-list standard GOOD-IPMC
```

```
 permit 224.0.1.39
 permit 224.0.1.40
 permit 239.192.240.0 0.0.3.255
 permit 239.192.248.0 0.0.3.255

!

ip access-list extended PERMIT-SOURCES
 permit ip 10.121.0.0 0.0.255.255 239.192.240.0 0.0.3.255
 permit ip 10.121.0.0 0.0.255.255 239.192.248.0 0.0.3.255
```

コア スイッチ構成（OSPF）

```
!
! Enabled spanning tree as a fail-safe practice
spanning-tree mode rapid-pvst
!
redundancy

 mode sso

 main-cpu
  auto-sync running-config
  auto-sync standard

!
! Configure necessary loopback interfaces to support Multicast MSDP and Anycast for
! RP redundancy
interface Loopback0

 description MSDP PEER INT

 ip address 10.122.10.2 255.255.255.255
!
interface Loopback1

 description ANYCAST RP ADDRESS

 ip address 10.122.100.1 255.255.255.255
!
interface Loopback2

 description Garbage-CAN RP

 ip address 2.2.2.2 255.255.255.255
!
! Configure point to point links to Distribution switches
interface TenGigabitEthernet3/1

 description 10GigE to Distribution 1
! Use of /31 addressing on point to point links optimizes use of IP address space in
! the campus

 ip address 10.122.0.25 255.255.255.254

 ip pim sparse-mode
! Reduce OSPF hello and dead timers to 1 and 3 seconds. In a point-point L3 campus
! design the OSPF timers are not the primary mechanism used for link and node
! failure detection. They are intended to provide a fail-safe mechanism only.
```

```
 ip ospf hello-interval 1
 ip ospf dead-interval 3
 load-interval 30

! Reduce carrier delay to 0. Tuning carrier delay no longer has an impact on GigE and
! 10GigE interfaces but is recommended to be configured as a best practice for network
! operational consistency

carrier-delay msec 0
! Configure trust DSCP to provide for maximum granularity of internal QoS queuing

 mls qos trust dscp
!
router ospf 100
! Explicitly configure the OSPF router id as a best practice when using Anycast and/or
! any identical loopback address on multiple routers.

 router-id 10.122.0.1

 log-adjacency-changes
! Tune the SPF throttle timers down from the defaults. Please refer to the HA Campus
! Design Guides for details on specific tuning recommendations.

 timers spf 1 1
 passive-interface Loopback0
 passive-interface Loopback1
 passive-interface Loopback2
 network 10.122.0.0 0.0.255.255 area 0.0.0.0

!
! Multicast route point and MSDP configuration.
! For a detailed explanation on the specifics of the configuration below please see
! the campus chapter of the multicast design guides.
ip pim rp-address 2.2.2.2
ip pim rp-address 10.122.100.1 GOOD-IPMC override
ip pim accept-register list PERMIT-SOURCES
ip msdp peer 10.122.10.1 connect-source Loopback0
ip msdp description 10.122.10.1 ANYCAST-PEER-6k-core-left
ip msdp cache-sa-state
ip msdp originator-id Loopback0
!
ip access-list standard GOOD-IPMC

 permit 224.0.1.39
 permit 224.0.1.40
 permit 239.192.240.0 0.0.3.255
 permit 239.192.248.0 0.0.3.255

!

ip access-list extended PERMIT-SOURCES
 permit ip 10.121.0.0 0.0.255.255 239.192.240.0 0.0.3.255
 permit ip 10.121.0.0 0.0.255.255 239.192.248.0 0.0.3.255
```

レイヤ 2 アクセスおよびディストリビューション ブロックのスイッチ構成

ここでは、前述の最初のテスト ケースで使用された構成について説明します。テストの特性は次のとおりです。

- デフォルト ゲートウェイ プロトコル ― HSRP
- スパニング ツリー バージョン ― PVST+（per VLAN 802.1d）
- IGP ― EIGRP

その他のテスト ケースにおけるこの基本構成からの変更内容は、前述の結果の項に記載されています。インターフェイス設定および VLAN 設定の出力例は、あくまでも参考として示されています。推奨される設定の詳細については、『*Designing a Campus Network for High Availability*』を参照してください。

ディストリビューション 1 ― ルート ブリッジおよび HSRP プライマリ

```
! Use vtp transparent mode, configure all VLANs explicitly
vtp domain campus-test
vtp mode transparent
! Enable UDLD aggressive mode as a fail safe mechanism
udld aggressive

! Enable 802.1d per VLAN spanning tree enhancements.
spanning-tree mode pvst
spanning-tree loopguard default
no spanning-tree optimize bpdu transmission
spanning-tree extend system-id
spanning-tree uplinkfast
spanning-tree backbonefast
! Configure root bridge priority. Note use of extended system-id
spanning-tree vlan 2-7,20-51,102-149,202-207,220-249 priority 24576
!
! Define unique voice and data vlans for each access switch
vlan 4

 name Data_VLAN-4507-SupII+
vlan 7
 name Data_VLAN-6500-Sup2-CatOS
vlan 104
 name Voice_VLAN-4507-SupII+
vlan 107
 name Voice_VLAN-6500-Sup2
vlan 204
 name Trunk_VLAN-4507-SupII+
vlan 207

 name Trunk_VLAN-6500-Sup2-CatOS
!
! Define a local loopback address to provide a sink hole route point for
! invalid multicast groups
interface Loopback2

 description Garbage-CAN RP

 ip address 2.2.2.2 255.255.255.255
!
! Configure point to point Layer 3 interface uplinks to core switches
interface TenGigabitEthernet4/1

 description 10 GigE to Core 1
 ip address 10.122.0.26 255.255.255.254
 ip pim sparse-mode

! Reduce EIGRP hello and hold timers to 1 and 3 seconds and enable MD5
```

```
! route authentication
 ip hello-interval eigrp 100 1
 ip hold-time eigrp 100 3
 ip authentication mode eigrp 100 md5
 ip authentication key-chain eigrp 100 eigrp

! Advertise a summary route for the entire distribution block upstream to the

! core
 ip summary-address eigrp 100 10.120.0.0 255.255.0.0 5
 load-interval 30

! Reducing carrier delay to 0 as a
 carrier-delay msec 0
! Trust inbound DSCP markings

 mls qos trust dscp
!
interface TenGigabitEthernet4/2

 description 10 GigE to Core 2
 ip address 10.122.0.30 255.255.255.254
 ip pim sparse-mode
 ip hello-interval eigrp 100 1

 ip hold-time eigrp 100 3
 ip authentication mode eigrp 100 md5
 ip authentication key-chain eigrp 100 eigrp
 ip summary-address eigrp 100 10.120.0.0 255.255.0.0 5
 load-interval 30
 mls qos trust dscp

!

interface TenGigabitEthernet4/3
 description 10GigE to Distribution-2
 ip address 10.122.0.21 255.255.255.254
 ip pim sparse-mode
 ip hello-interval eigrp 100 1
 ip hold-time eigrp 100 3
 ip authentication mode eigrp 100 md5
 ip authentication key-chain eigrp 100 eigrp
 load-interval 30
 mls qos trust dscp

!
! Configure Layer 2 trunk connections to downstream access switches
interface GigabitEthernet3/3

 description to 4507_SupII+_Access
 no ip address
 load-interval 30

! Trust inbound DSCP markings
 mls qos trust dscp
 switchport
 switchport trunk encapsulation dot1q

! Configure trunk to use a dedicated native VLAN to protect against VLAN hoping
 switchport trunk native vlan 204
! Manually prune all VLANs from trunk other than dedicated voice and data
 switchport trunk allowed vlan 4,104
```

```
! Configure switchport to bypass Trunk and Etherchannel negotiation
 switchport mode trunk
 switchport nonegotiate

!

interface GigabitEthernet3/6
 description to 6500_Sup1A_Access
 no ip address
 load-interval 30
 mls qos trust dscp
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 207
 switchport trunk allowed vlan 7,107
 switchport mode trunk
 switchport nonegotiate

!
! Define the Layer 3 SVI for each voice and data VLAN
interface Vlan4

 description Data VLAN for 4507 SupII+
 ip address 10.120.4.3 255.255.255.0
! Enable loose uRPF to mitigate against spoofed source IP addressing
 ip verify unicast source reachable-via any

! Define ip-helper to forward DHCP requests
 ip helper-address 10.121.0.5
 no ip redirects

! Reduce PIM query interval to 250 msec
 ip pim query-interval 250 msec
 ip pim sparse-mode
 load-interval 30

! Define HSRP default gateway with 250/800 msec hello and hold timers
 standby 1 ip 10.120.4.1
 standby 1 timers msec 250 msec 800

! Set preempt delay large enough to allow network to stabilize before HSRP

! switches back on power on or link recovery
 standby 1 preempt delay minimum 180
! Enable HSRP authentication

 standby 1 authentication ese
!
interface Vlan7

 description Data VLAN for 6500 Sup2 CatOS
 ip address 10.120.7.3 255.255.255.0
 ip verify unicast source reachable-via any
 ip helper-address 10.121.0.5
 no ip redirects
 ip pim query-interval 250 msec
 ip pim sparse-mode
 load-interval 30
 standby 1 ip 10.120.7.1
 standby 1 timers msec 250 msec 800
 standby 1 preempt delay minimum 180
 standby 1 authentication ese
```

```
!

interface Vlan104
 description Voice VLAN for 4507 SupII+
 ip address 10.120.104.3 255.255.255.0
 ip verify unicast source reachable-via any
 ip helper-address 10.121.0.5
 no ip redirects
 ip pim query-interval 250 msec
 ip pim sparse-mode
 load-interval 30
 standby 1 ip 10.120.104.1
 standby 1 timers msec 250 msec 800
 standby 1 preempt delay minimum 180
 standby 1 authentication ese

!

interface Vlan107
 description Voice VLAN for 6500 Sup2 CatOS
 ip address 10.120.107.3 255.255.255.0
 ip verify unicast source reachable-via any
 ip helper-address 10.121.0.5
 no ip redirects
 ip pim query-interval 250 msec
 ip pim sparse-mode
 load-interval 30
 standby 1 ip 10.120.107.1
 standby 1 timers msec 250 msec 800
 standby 1 preempt delay minimum 180
 standby 1 authentication ese

!
router eigrp 100
! Passive all interfaces except the core uplinks and link top peer distribution

 passive-interface default
 no passive-interface TenGigabitEthernet4/1
 no passive-interface TenGigabitEthernet4/2
 no passive-interface TenGigabitEthernet4/3

! Specify EIGRP advertise routes for all distribution access and core uplink

! subnets
 network 10.120.0.0 0.0.255.255
 network 10.122.0.0 0.0.0.255
 no auto-summary

! Explicitly configure the EIGRP router id as a best practice when using Anycast and/or
! any identical loopback address on multiple routers.
 eigrp router-id 10.122.0.3

! Define the valid multicast RP and garbage can RP. See the Multicast Design

! Guide for details on this configuration
ip pim rp-address 10.122.100.1 GOOD-IPMC override
ip pim rp-address 2.2.2.2
ip pim spt-threshold infinity
!
!
ip access-list standard GOOD-IPMC
```

```
 permit 224.0.1.39
 permit 224.0.1.40
 permit 239.192.240.0 0.0.3.255
 permit 239.192.248.0 0.0.3.255
```

ディストリビューション 2 — セカンダリ ルート ブリッジおよび HSRP スタンバイ

```
! Use vtp transparent mode, configure all VLANs explicitly
vtp domain campus-test
vtp mode transparent
! Enable UDLD aggressive mode as a fail safe mechanism
udld aggressive

! Enable 802.1d per VLAN spanning tree enhancements.
spanning-tree mode pvst
spanning-tree loopguard default
no spanning-tree optimize bpdu transmission
spanning-tree extend system-id
spanning-tree uplinkfast
spanning-tree backbonefast
! Configure root bridge priority as secondary. Note use of extended system-id
spanning-tree vlan 2-7,20-51,102-149,202-207,220-249 priority 28672
!
vlan 4

 name Data_VLAN-4507-SupII+
vlan 7
 name Data_VLAN-6500-Sup2-CatOS
vlan 104
 name Voice_VLAN-4507-SupII+
vlan 107
 name Voice_VLAN-6500-Sup2
vlan 204
 name Trunk_VLAN-4507-SupII+
vlan 207

 name Trunk_VLAN-6500-Sup2-CatOS
!
! Define a local loopback address to provide a sink hole route point for
! invalid multicast groups
interface Loopback2

 description Garbage-CAN RP

 ip address 2.2.2.2 255.255.255.255
!
! Configure point to point Layer 3 interface uplinks to core switches
interface TenGigabitEthernet4/1

 description 10 GigE to Core 1
 ip address 10.122.0.34 255.255.255.254
 ip pim sparse-mode

! Reduce EIGRP hello and hold timers to 1 and 3 seconds and enable MD5

! route authentication
 ip hello-interval eigrp 100 1
 ip hold-time eigrp 100 3
 ip authentication mode eigrp 100 md5
 ip authentication key-chain eigrp 100 eigrp
```

```
! Advertise a summary route for the entire distribution block upstream to the
! core

ip summary-address eigrp 100 10.120.0.0 255.255.0.0 5
 load-interval 30
! Reducing carrier delay to 0 as a
 carrier-delay msec 0
! Trust inbound DSCP markings

 mls qos trust dscp
!
interface TenGigabitEthernet4/2

 description 10 GigE to Core 2
 ip address 10.122.0.38 255.255.255.254
 ip pim sparse-mode
 ip hello-interval eigrp 100 1
 ip hold-time eigrp 100 3
 ip authentication mode eigrp 100 md5
 ip authentication key-chain eigrp 100 eigrp
 ip summary-address eigrp 100 10.120.0.0 255.255.0.0 5
 load-interval 30
 mls qos trust dscp

!

interface TenGigabitEthernet4/3
 description 10GigE to Distribution-2
 ip address 10.122.0.22 255.255.255.254
 ip pim sparse-mode
 ip hello-interval eigrp 100 1
 ip hold-time eigrp 100 3
 ip authentication mode eigrp 100 md5
 ip authentication key-chain eigrp 100 eigrp
 load-interval 30
 mls qos trust dscp

!
! Configure Layer 2 trunk connections to downstream access switches
interface GigabitEthernet3/3

 description to 4507_SupII+_Access
 no ip address
 load-interval 30

! Trust inbound DSCP markings
 mls qos trust dscp
 switchport
 switchport trunk encapsulation dot1q

! Configure trunk to use a dedicated native VLAN to protect against VLAN hoping
 switchport trunk native vlan 204
! Manually prune all VLANs from trunk other than dedicated voice and data
 switchport trunk allowed vlan 4,104

! Configure switchport to bypass Trunk and Etherchannel negotiation
 switchport mode trunk
 switchport nonegotiate

!

interface GigabitEthernet3/6
 description to 6500_Sup1A_Access
 no ip address
```

```
 load-interval 30
 mls qos trust dscp
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 207
 switchport trunk allowed vlan 7,107
 switchport mode trunk
 switchport nonegotiate

!
! Define the Layer 3 SVI for each voice and data VLAN
interface Vlan4

 description Data VLAN for 4507 SupII+
 ip address 10.120.4.2 255.255.255.0
! Enable loose uRPF to mitigate against spoofed source IP addressing

ip verify unicast source reachable-via any

! Define ip-helper to forward DHCP requests
 ip helper-address 10.121.0.5
 no ip redirects

! Reduce PIM query interval to 250 msec
 ip pim query-interval 250 msec
 ip pim sparse-mode
 load-interval 30

! Define HSRP default gateway with 250/800 msec hello and hold timers
 standby 1 ip 10.120.4.1
 standby 1 timers msec 250 msec 800

! Raising HSRP priority forces this switch to be active HSRP gateway

 standby 1 priority 150
! Set preempt delay large enough to allow network to stabilize before HSRP
! switches back on power on or link recovery

 standby 1 preempt delay minimum 180
! Enable HSRP authentication

 standby 1 authentication ese
!
interface Vlan7

 description Data VLAN for 6500 Sup2 CatOS
 ip address 10.120.7.2 255.255.255.0
 ip verify unicast source reachable-via any
 ip helper-address 10.121.0.5
 no ip redirects
 ip pim query-interval 250 msec
 ip pim sparse-mode
 load-interval 30
 standby 1 ip 10.120.7.1
 standby 1 timers msec 250 msec 800
 standby 1 priority 150
 standby 1 preempt delay minimum 180
 standby 1 authentication ese

!

interface Vlan104
 description Voice VLAN for 4507 SupII+
 ip address 10.120.104.2 255.255.255.0
```

```
 ip verify unicast source reachable-via any
 ip helper-address 10.121.0.5
 no ip redirects
 ip pim query-interval 250 msec
 ip pim sparse-mode
 load-interval 30
 standby 1 ip 10.120.104.1
 standby 1 timers msec 250 msec 800
 standby 1 preempt delay minimum 180
 standby 1 authentication ese

!

interface Vlan107
 description Voice VLAN for 6500 Sup2 CatOS
 ip address 10.120.107.2 255.255.255.0
 ip verify unicast source reachable-via any
 ip helper-address 10.121.0.5
 no ip redirects
 ip pim query-interval 250 msec
 ip pim sparse-mode
 load-interval 30
 standby 1 ip 10.120.107.1
 standby 1 timers msec 250 msec 800
 standby 1 preempt delay minimum 180
 standby 1 authentication ese

!
router eigrp 100
! Passive all interfaces except the core uplinks and link top peer distribution

passive-interface default
 no passive-interface TenGigabitEthernet4/1
 no passive-interface TenGigabitEthernet4/2
 no passive-interface TenGigabitEthernet4/3

! Specify EIGRP advertise routes for all distribution access and core uplink

! subnets
 network 10.120.0.0 0.0.255.255
 network 10.122.0.0 0.0.0.255
 no auto-summary
 eigrp router-id 10.122.0.4

! Define the valid multicast RP and garbage can RP. See the Multicast Design
! Guide for details on this configuration
ip pim rp-address 10.122.100.1 GOOD-IPMC override
ip pim rp-address 2.2.2.2
ip pim spt-threshold infinity
!
!
ip access-list standard GOOD-IPMC

 permit 224.0.1.39
 permit 224.0.1.40
 permit 239.192.240.0 0.0.3.255
 permit 239.192.248.0 0.0.3.255
```

IOS アクセス スイッチ（4507/SupII+）

```
vtp mode transparent
udld aggressive
! Auto QoS defined policier
policy-map autoqos-voip-policy

  class class-default

 dbl
! Enable 802.1d per VLAN spanning tree enhancements.
spanning-tree loopguard default
spanning-tree extend system-id
spanning-tree uplinkfast
spanning-tree backbonefast
! Define dedicated voice, data and trunk VLAN for this access switch
vlan 4

 name Data
vlan 104
 name Voice
vlan 204

 name Trunk
! Define switchport trunk uplink to distribution
interface GigabitEthernet1/1

 description Uplink to Distribution Switch 1
 switchport trunk encapsulation dot1q
! Define a unique trunk vlan in order to prevent vlan hopping attacks
 switchport trunk native vlan 204
! Explicitly configure voice and data vlan on trunk
 switchport trunk allowed vlan 4,104

! Explicitly enable trunking and disable Etherchannel negotiation
 switchport mode trunk
 switchport nonegotiate
 load-interval 30

! Auto QoS defined configuration for voice enabled uplink
 qos trust cos
 service-policy output autoqos-voip-policy
 auto qos voip trust
 tx-queue 3

bandwidth percent 33
   priority high
   shape percent 33

 spanning-tree link-type point-to-point
!
interface GigabitEthernet1/2

 description Uplink to Distribution Switch 2
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 204
 switchport trunk allowed vlan 4,104
 switchport mode trunk
 switchport nonegotiate
 load-interval 30
 qos trust cos
 service-policy output autoqos-voip-policy
```

```
 auto qos voip trust
 tx-queue 3

   bandwidth percent 33
   priority high
   shape percent 33

 spanning-tree link-type point-to-point
!
! Define access ports using the recommended Smartports configuration. Please
! see the following for more information on smartports

http://www.cisco.com/en/US/docs/switches/lan/catalyst3750/software/release/12.2_40_se/conf
iguration/guide/swmacro.html

!

interface FastEthernet2/1
 switchport access vlan 4
 switchport mode access
 switchport voice vlan 104
 switchport port-security
 switchport port-security aging time 2
 switchport port-security violation restrict
 switchport port-security aging type inactivity
 qos trust device cisco-phone
 qos trust cos
 service-policy output autoqos-voip-policy
 auto qos voip cisco-phone
 tx-queue 3

   priority high

   shape percent 33
 spanning-tree portfast
 spanning-tree bpduguard enable

!
! Define switch management address on data vlan
interface Vlan4

 ip address 10.120.4.4 255.255.255.0
```

CatOS アクセス スイッチ（6500/Sup2）

```
set vtp domain campus-test
set vtp mode transparent
set vlan 7 name Data type ethernet mtu 1500 said 100007 state active
set vlan 107 name Voice type ethernet mtu 1500 said 100107 state active
set vlan 207 name Uplink type ethernet mtu 1500 said 100207 state active

#ip
set interface sc0 7 10.120.7.4/255.255.255.0 10.120.7.255

#uplinkfast groups
set spantree uplinkfast enable rate 0 all-protocols off

#module 1 : 2-port 1000BaseX Supervisor
set vlan 207  1/1-2
set udld aggressive-mode enable 1/1-2
clear trunk 1/1  1-6,8-106,108-206,208-1005,1025-4094
```

```
set trunk 1/1  nonegotiate dot1q 7,107,207
clear trunk 1/2  1-6,8-106,108-206,208-1005,1025-4094
set trunk 1/2  nonegotiate dot1q 7,107,207
set spantree guard loop 1/1-2
set port qos 1/1-2 trust trust-dscp
set port qos 1/1-2 policy-source local
set port channel 1/1-2 mode off

! Define access ports using the recommended Smartports configuration. Please
! see the following for more information on Smartports,

http://www.cisco.com/en/US/docs/switches/lan/catalyst3750/software/release/12.2_40_se/conf
iguration/guide/swmacro.html

!
set port enable 4/1
set port l2protocol-tunnel 4/1 cdp stp vtp dis
set port membership 4/1 static
set port host 4/1
set spantree bpdu-guard 4/1 enable
set vlan 7 4/1
set port auxiliaryvlan 4/1 107
set port inlinepower 4/1 auto
set cdp enable 4/1
set port qos 4/1 autoqos voip ciscoipphone
set port security 4/1 enable age 2 maximum 1 violation restrict
```

レイヤ 3 アクセスおよびディストリビューション ブロックのスイッチ構成

次に、前述のレイヤ 3 アクセス テスト ケースで使用された構成を示します。

- スパニング ツリー バージョン — Rapid-PVST+（per VLAN 802.1w）
- IGP — EIGRP

その他のテスト ケースにおけるこの基本構成からの変更内容は、前述の結果の項に記載されています。推奨される設定の詳細については、『*Designing a Campus Network for High Availability*』を参照してください。

ディストリビューション ノード EIGRP

（注） ディストリビューション スイッチは 2 つとも対称構成です。

```
key chain eigrp

 key 100
key-string 7 01161501
!
<Configure spanning tree as a redundant protective mechanism>
spanning-tree mode rapid-pvst

spanning-tree loopguard default
!
<Configure point to point Layer 3 links to each of the access switches>
interface GigabitEthernet3/1
```

```
 description Link to Access Switch

<configure the switch to switch link using a /30 or /31 subnet>
 ip address 10.120.0.204 255.255.255.254
 ip pim sparse-mode

<specify the use of 1 second hello and 3 second dead timers for EIGRP>
 ip hello-interval eigrp 100 1
 ip hold-time eigrp 100 3

<enable eigrp MD5 authentication>
 ip authentication mode eigrp 100 md5
 ip authentication key-chain eigrp 100 eigrp
 logging event link-status
 load-interval 30

<Set carrier delay to 0. On Catalyst 6500 this will have no effect on GigE ports however
it is necessary on 3x50 series switches and should be consistently configured for best
practices>

 carrier-delay msec 0
<Trust the dscp settings in all packets sourced from the access. We are extending the
trust boundary to the access switch>

 mls qos trust dscp
!
!
<Configure point to point L3 links to each of the core switches>
interface TenGigabitEthernet4/1

 description 10 GigE to Core 1

<configure the switch to switch link using a /30 or /31 subnet>
 ip address 10.122.0.26 255.255.255.254
 ip pim sparse-mode

<specify the use of 1 second hello and 3 second dead timers for EIGRP>
 ip hello-interval eigrp 100 1
 ip hold-time eigrp 100 3

<Configure EIGRP authentication on all links>
 ip authentication mode eigrp 100 md5
 ip authentication key-chain eigrp 100 eigrp

<Advertise a summary address for the entire distribution block upstream to the core>
 ip summary-address eigrp 100 10.120.0.0 255.255.0.0 5
 logging event link-status
 load-interval 30
 carrier-delay msec 0

<Trust all DSCP markings from the core of the network>

 mls qos trust dscp
!
!
<Configure a point to point Layer 3 link between distribution switches>

interface TenGigabitEthernet4/3

 description 10 GigE to Distribution 2
```

```
<configure the switch to switch link using a /30 or /31 subnet>
 ip address 10.122.0.21 255.255.255.254
 ip pim sparse-mode

<specify the use of 1 second hello and 3 second dead timers for EIGRP>
 ip hello-interval eigrp 100 1
 ip hold-time eigrp 100 3

<Configure EIGRP authentication on all links>
 ip authentication mode eigrp 100 md5
 ip authentication key-chain eigrp 100 eigrp
 logging event link-status
 load-interval 30
 mls qos trust dscp

!
!
router eigrp 100

<Passive all interfaces not connected to another Layer 3 switch>

 passive-interface GigabitEthernet2/1
<Specify which networks should be routed by EIGRP. Include the distribution block and the
core links>

 network 10.120.0.0 0.0.255.255

 network 10.122.0.0 0.0.0.255
<Apply a distribute list filtering all routes other than select default(s) to the access
switches>

 distribute-list Default out GigabitEthernet3/1
 distribute-list Default out GigabitEthernet3/2
 . . .
 distribute-list Default out GigabitEthernet9/14
 distribute-list Default out GigabitEthernet9/15
 no auto-summary

! Explicitly configure the EIGRP router id as a best practice when using Anycast and/or
! any identical loopback address on multiple routers.
 eigrp router-id 10.122.0.3

!
ip classless
no ip http server
ip pim rp-address 10.122.100.1 GOOD-IPMC override
ip pim rp-address 2.2.2.2
ip pim spt-threshold infinity
!
!
ip access-list standard Default

 permit 0.0.0.0

ip access-list standard GOOD-IPMC
 permit 224.0.1.39
 permit 224.0.1.40
 permit 239.192.240.0 0.0.3.255
 permit 239.192.248.0 0.0.3.255
```

アクセス ノード EIGRP（冗長スーパーバイザ）

```
key chain eigrp

 key 100
key-string 7 01161501
!
<Configure spanning tree as a redundant protective mechanism>
spanning-tree mode rapid-pvst
spanning-tree loopguard default
!
redundancy

 mode sso
 main-cpu

  auto-sync running-config
auto-sync standard
!
<Create a local Data and Voice VLAN>
vlan 6

 name Access-Data-VLAN
!
vlan 106

 name Access-Voice-VLAN
!
interface Loopback22

 ip address 2.2.2.2 255.255.255.255
!
<Define the uplink to the Distribution switches as a point to point Layer 3 link>
interface GigabitEthernet1/1

description Uplink to Distribution 1
 ip address 10.120.0.205 255.255.255.254
 ip pim sparse-mode

<Reduce EIGRP hello and dead timers to 1 and 3 seconds>
 ip hello-interval eigrp 100 1
 ip hold-time eigrp 100 3

<Enable EIGRP MD5 authentication>
 ip authentication mode eigrp 100 md5
 ip authentication key-chain eigrp 100 eigrp
 logging event link-status
 load-interval 30
 carrier-delay msec 0
 mls qos trust dscp

!

interface GigabitEthernet2/1
 description Uplink to Distribution 2
 ip address 10.120.0.61 255.255.255.252
 ip pim sparse-mode
 ip hello-interval eigrp 100 1
 ip hold-time eigrp 100 3
 ip authentication mode eigrp 100 md5
 ip authentication key-chain eigrp 100 eigrp
 logging event link-status
 load-interval 30
```

```
 carrier-delay msec 0
 mls qos trust dscp

!
<Define Switched Virtual Interfaces's for both access Data and Voice VLANs>
interface Vlan6

 ip address 10.120.6.1 255.255.255.0
 ip helper-address 10.121.0.5
 no ip redirects
 ip pim query-interval 250 msec
 ip pim sparse-mode
 load-interval 30

!

interface Vlan106
 ip address 10.120.106.1 255.255.255.0
 ip helper-address 10.121.0.5
 no ip redirects
 ip pim query-interval 250 msec
 ip pim sparse-mode
 load-interval 30

!
<Configure EIGRP as an EIGRP stub router, advertising connected routes upstream to the
distribution>
router eigrp 100

 network 10.120.0.0 0.0.255.255
 no auto-summary
 eigrp stub connected
 eigrp router-id 10.122.0.22

!
ip classless
no ip http server
ip pim rp-address 10.122.100.1 GOOD-IPMC override
ip pim rp-address 2.2.2.2
ip pim spt-threshold infinity
!
ip access-list standard GOOD-IPMC

  permit 224.0.1.39
  permit 224.0.1.40
  permit 239.192.240.0 0.0.3.255
  permit 239.192.248.0 0.0.3.255
```

ディストリビューション ノード OSPF

（注） 両方のディストリビューション スイッチは対称構成です。

```
key chain eigrp
 key 100

  key-string 7 01161501
!
<Configure spanning tree as a redundant protective mechanism>
spanning-tree mode rapid-pvst
spanning-tree loopguard default
```

```
!
<Configure point to point Layer 3 links to each of the access switches>
interface GigabitEthernet3/1

 description Link to Access Switch

<configure the switch to switch link using a /30 or /31 subnet>
 ip address 10.120.0.204 255.255.255.254
 ip pim sparse-mode

<specify the use of 1 second hello and 3 second dead timers>
 ip ospf hello-interval 1
 ip ospf dead-interval 3

<enable eigrp MD5 authentication>
 ip authentication mode eigrp 100 md5
 ip authentication key-chain eigrp 100 eigrp
 logging event link-status
 load-interval 30

<Set carrier delay to 0. On Catalyst 6500 this will have no effect on GigE ports however
it is necessary on 3x50 series switches and should be consistently configured for best
practices>

 carrier-delay msec 0
<Trust the dscp settings in all packets sourced from the access. We are extending the
trust boundary to the access switch>

 mls qos trust dscp
!
!
<Configure point to point L3 links to each of the core switches>
interface TenGigabitEthernet4/1

 description 10 GigE to Core 1

<configure the switch to switch link using a /30 or /31 subnet>
 ip address 10.122.0.26 255.255.255.254
 ip pim sparse-mode

<specify the use of 1 second hello and 3 second dead timers>
 ip ospf hello-interval 1
 ip ospf dead-interval 3
 logging event link-status
 load-interval 30
 carrier-delay msec 0

<Trust all DSCP markings from the core of the network>

 mls qos trust dscp
!
!
<Configure a point to point Layer 3 link between distribution switches>
interface TenGigabitEthernet4/3

 description 10 GigE to Distribution 2

<configure the switch to switch link using a /30 or /31 subnet>
 ip address 10.122.0.21 255.255.255.254
 ip pim sparse-mode
```

```
<specify the use of 1 second hello and 3 second dead timers>
 ip ospf hello-interval 1
 ip ospf dead-interval 3
 logging event link-status

load-interval 30
 mls qos trust dscp

router ospf 100
! Explicitly configure the OSPF router id as a best practice when using Anycast and/or
! any identical loopback address on multiple routers.

 router-id 10.122.0.3
 log-adjacency-changes
 area 120 stub no-summary
 area 120 range 10.120.0.0 255.255.0.0
 timers throttle spf 1000 1000 1000
 network 10.120.0.0 0.0.255.255 area 120
 network 10.122.0.0 0.0.255.255 area 0
```

アクセス ノード OSPF（冗長スーパーバイザ）

```
!
<Configure spanning tree as a redundant protective mechanism>
spanning-tree mode rapid-pvst
spanning-tree loopguard default
!
redundancy

 mode sso
 main-cpu

  auto-sync running-config
auto-sync standard
!
vlan 4

 name cr8-4507-1-Data-VLAN
!
vlan 104

 name cr8-4507-1-Voice-VLAN
!
<Define the uplink to the Distribution switches as a point to point Layer 3 link>
interface GigabitEthernet1/1

 description Uplink to Distribution 1
 ip address 10.120.0.205 255.255.255.254
 ip pim sparse-mode

<Reduce hello and dead timers to 1 and 3 seconds>
 ip ospf hello-interval 1
 ip ospf dead-interval 3

<Enable EIGRP MD5 authentication>
 ip authentication mode eigrp 100 md5
 ip authentication key-chain eigrp 100 eigrp
 logging event link-status
 load-interval 30
```

```
 carrier-delay msec 0
 mls qos trust dscp

!

interface GigabitEthernet2/1
 description Uplink to Distribution 2
 ip address 10.120.0.61 255.255.255.252
 ip pim sparse-mode
 ip ospf hello-interval 1
 ip ospf dead-interval 3
 ip authentication mode eigrp 100 md5
 ip authentication key-chain eigrp 100 eigrp
 logging event link-status
 load-interval 30
 carrier-delay msec 0
 mls qos trust dscp

<Define Switched Virtual Interfaces's for both access Data and Voice VLANs>

interface Vlan4
 ip address 10.120.4.1 255.255.255.0
 ip helper-address 10.121.0.5
 no ip redirects
 ip pim query-interval 250 msec
 ip pim sparse-mode
 load-interval 30

!

interface Vlan104
 ip address 10.120.104.1 255.255.255.0
 ip helper-address 10.121.0.5
 no ip redirects
 ip pim query-interval 250 msec
 ip pim sparse-mode
 load-interval 30

!

router ospf 100
 router-id 10.122.0.22
 log-adjacency-changes
 area 120 stub no-summary
 timers throttle spf 1000 1000 1000
 network 10.120.0.0 0.0.255.255 area 120
```