Campus Networks における IPv6 導入ガイド

このマニュアルでは、キャンパス ネットワークにおける IPv6 の計画または導入の方法を説明します。このマニュアルでは、キャンパス設計の基本事項およびベスト プラクティス、IPv6 の基礎知識、トランジション メカニズム、または IPv4 と IPv6 の機能比較については言及しません。このマニュアルの目的についての詳しい説明と関連資料の一覧は、「マニュアルの対象」（p.3）を参照してください。

目次

Cisco Systems

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

OL-11818-01-J

概要

マニュアルの対象

読者は Cisco キャンパス設計のベスト プラクティスに基づく推奨事項と、IPv6 および関連するトランジション メカニズムについて基本事項を理解していることを前提とします。必要な基礎知識は、シスコおよび業界が提供している多数のマニュアルおよびトレーニングを通じて得ることができます。次に、関係する各分野について、推奨される情報源をいくつか示します。

- 『*Cisco Solution Reference Network Design (SRND) Campus Guides*』— http://www.cisco.com/en/US/netsol/ns656/networking_solutions_design_guidances_list.html#anchor2
- Cisco IPv6 CCO Web サイト — http://www.cisco.com/go/ipv6
- 『*Catalyst 6500 Series Cisco IOS Software Configuration Guide, 12.2SX*』— http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/swcg/index.htm
- 『*Catalyst 3750 Switch Software Configuration Guide, 12.2(25)SEE*』— http://www.cisco.com/univercd/cc/td/doc/product/lan/cat3750/12225see/scg/index.htm
- 『*Deploying IPv6 Networks*』Ciprian P. Popoviciu、Eric Levy-Abegnoli、Patrick Grossetete 著（ISBN-10:1-58705-210-5、ISBN-13:978-1-58705-210-1）— http://www.ciscopress.com/bookstore/product.asp?isbn=1587052105&rl=1
- go6 IPv6 ポータル –IPv6 ナレッジ センター — http://wiki.go6.net/index.php?title=Main_Page
- 6NET– 大規模な国際的 IPv6 パイロット ネットワーク — http://www.6net.org/

- IETF IPv6 ワーキング グループ — http://www.ietf.org/html.charters/ipv6-charter.html
- IETF IPv6 オペレーションズ ワーキング グループ — http://www.ietf.org/html.charters/v6ops-charter.html

マニュアルの形式と命名規則

このマニュアルでは、各種のキャンパス IPv6 導入モデルの概要を示し、導入に関する一般的な考慮事項のほか、モデル別の実装についての詳しい情報を提供します。

一般的な考慮事項および実装情報で示す設定例を示した章に加え、「付録 — 設定リスト」（p.66）に各キャンパス スイッチの設定全体を示します。

このマニュアル全体を通して、キャンパス IPv6 導入モデルに言及する場合、次の短縮形を使用します。

- デュアルスタック モデル（DSM）
- ハイブリッド モデル例 1（HME1）
- ハイブリッド モデル例 2（HME2）
- サービス ブロック モデル（SBM）

アクセス リスト（ACL）名、QoS（Quality of Service）ポリシー定義など、ユーザ定義のプロパティは、コマンド固有のポリシー定義と区別するため、すべて大文字で示します。

（注） 次の各セクションでは、該当するコマンドを赤のテキストで示します。

導入モデルの概要

ここでは、次の 3 つのキャンパス IPv6 導入モデルについて概要を示し、各モデルの利点や適用性について説明します。

- DSM
- ハイブリッド モデル
  - HME1 — Intra-Site Automatic Tunnel Addressing Protocol（ISATAP）＋デュアルスタック
  - HME2 — 手動設定トンネル＋デュアルスタック
- SBM — ISATAP、手動設定トンネル、およびデュアルスタックの組み合わせ

デュアルスタック モデル

概要

DSM は、完全にデュアルスタックのトランジション メカニズムをベースとしています。2 つのプロトコル スタックが同時にイネーブルに設定されているデバイスまたはネットワークは、デュアルスタック モードで動作します。デュアルスタックの従来の使用例としては、IPv4 と IPX、または IPv4 と Apple Talk の同じデバイスにおける併用があります。

既存の IPv4 環境に IPv6 を導入する方法として、デュアルスタックは最も多用途で望ましい方法です。IPv4 をイネーブルに設定できる箇所であれば IPv6 をイネーブルにすることができ、IPv6 のルーティング、ハイ アベイラビリティ、セキュリティを確保するための機能も同時に設定できます。状況によっては、IPv6 をサポートしていないレガシー アプリケーションまたはレガシー

ホストが存在するため、特定のインターフェイスまたはデバイスで IPv6 をイネーブルにしない場合もあります。逆に、IPv4 のサポートが不要になったインターフェイスまたはデバイスで、IPv6 のみをイネーブルにする場合もあります。

このマニュアルの各セクションの動作確認済みコンポーネントの部分では、DSM を正しく実装するための一般的な要件を簡単に説明します。最も重要な考慮事項は、キャンパス ネットワークのコンポーネント（スイッチなど）に IPv6 のハードウェア サポートがあるかどうかを確認することです。キャンパス ネットワークでは、リンク速度とキャパシティは、ユーザ数、アプリケーションのタイプ、予測される遅延などの問題によって左右される場合が多くあります。この環境では一般に高いデータ レートが要求されるので、ソフトウェア フォワーディングのみの機器で IPv6 ユニキャストまたはマルチキャスト レイヤ スイッチングをイネーブルにすることは推奨できません。テスト環境や小規模なパイロット ネットワークでは、ソフトウェア フォワーディングのみのスイッチング デバイスで IPv6 をイネーブルにしても問題無いかもしれませんが、実稼働キャンパス ネットワークでは適していません。

このソリューションの利点と欠点

キャンパスでの DSM による IPv6 の導入は、ハイブリッドおよびサービス ブロック モデルと比べてメリットがいくつかあります。DSM の主な利点は、キャンパス ネットワーク内でトンネリングが不要という点です。DSM は 2 つのプロトコルを「ships-in-the-night」と呼ばれる方法で実行します。これは、IPv4 と IPv6 が並行して動作しますが、ネットワーク リソースを共有する点を除いて、両者間に機能的な依存関係はありません。IPv4 と IPv6 はそれぞれ独立したルーティング、ハイ アベイラビリティ（HA）、QoS、セキュリティ、およびマルチキャスト ポリシーを使用します。デュアルスタックは、処理パフォーマンスの面でも有利です。カプセル化とルックアップ用の余分なオーバーヘッドのアカウントを持たずに、パケットが転送されるためです。

シスコのルーテッド アクセス設計をすでに導入している、または導入を計画しているお客様は、各ネットワーク デバイスが IPv6 をハードウェアでサポートしているので、IPv6 という選択肢もあることに気づかれるでしょう。ルーテッド アクセス設計での IPv6 の実装については、「デュアルスタック モデル — 実装」（p.33）で説明します。

DSM の主な欠点は、既存のネットワーク デバイスが IPv6 対応でない場合、ネットワーク機器のアップグレードが必要になる可能性がある点です。

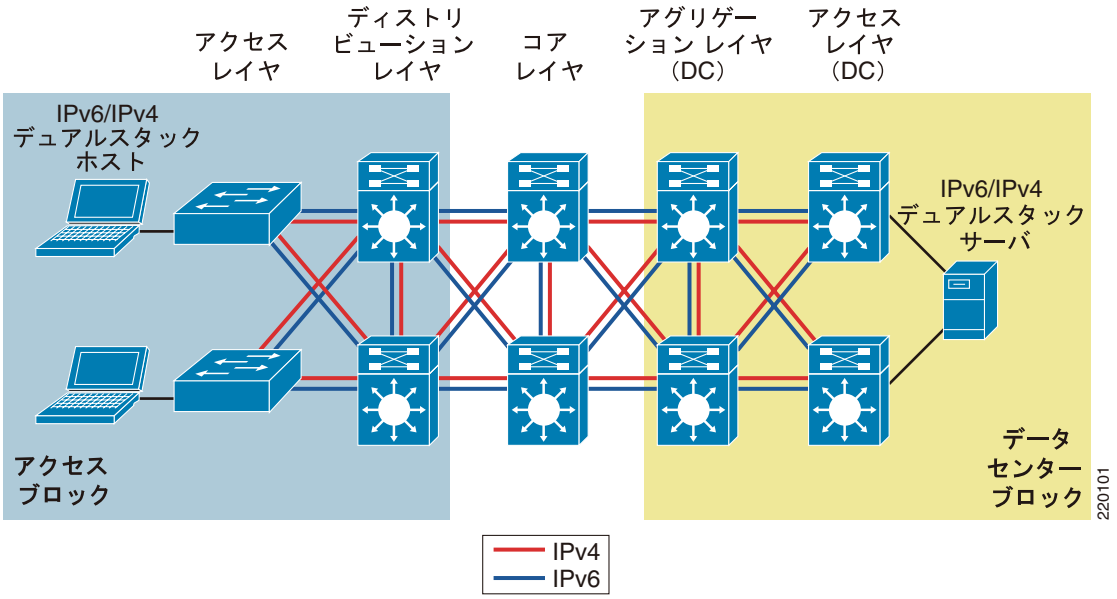
「まとめ」（p.63）で、各種のキャンパス設計モデルの利点と問題点を表形式で要約します。

ソリューション トポロジ

図 1 は、キャンパス ネットワークでの DSM ベースの導入例を示しています。この例は、このマニュアルで後述する詳細設定の基本となります。

（注） この図のデータセンター ブロックはあくまで参考用であり、このマニュアルでは説明しません。データセンターでの IPv6 の導入については、別のマニュアルで説明する予定です。

図 1　　デュアルスタック モデルの例



動作確認済みのコンポーネント

表 1 に、DSM 構成で使用し動作確認を行ったコンポーネントを示します。

表 1　　DSM で動作確認済みのコンポーネント

キャンパス レイヤ	ハードウェア	ソフトウェア
アクセス レイヤ	Cisco Catalyst 3750	Advanced IP Services — 12.2(25)SED1
	Catalyst 6500 Supervisor 32 または 720	Advanced Enterprise Services SSH — 12.2(18)SXF5
ホスト デバイス	各種ノート型パソコン — IBM、HP、および Apple	Microsoft Windows XP SP2、Vista RC1、Apple Mac OS X 10.4.7、および Red Hat Enterprise Linux WS
ディストリビューション レイヤ	Catalyst 6500 Supervisor 32 または 720	Advanced Enterprise Services SSH — 12.2(18)SXF5
コア レイヤ	Catalyst 6500 Supervisor 720	Advanced Enterprise Services SSH — 12.2(18)SXF5

ハイブリッド モデル

概要

ハイブリッド モデル ストラテジーでは、複数の独立したトランジション メカニズムを同じ設計目標のために使用します。特定のネットワーク環境に最も適した、任意のトランジション メカニズムの組み合わせを利用できる柔軟性が、ハイブリッド アプローチの重要な側面といえます。

ハイブリッド モデルは、既存のネットワーク インフラストラクチャの特性に、可能な限り適合します。トランジション メカニズムの選択は、ネットワーク要素の IPv6 ハードウェア機能、ホスト数、アプリケーションのタイプ、IPv6 サービスの場所、各種トランジション メカニズムに関するネットワーク インフラストラクチャ機能のサポートなど、複数の基準に基づいて行います。

このモデルで利用する主な IPv6 トランジション メカニズムは、次の 3 つです。

- デュアルスタック — 2 つのプロトコル スタック（IPv4 および IPv6）の導入
- ISATAP — 既存の IPv4 対応インフラストラクチャに依存する、ホスト / ルータ トンネリング メカニズム
- 手動設定トンネル — 既存の IPv4 対応インフラストラクチャに依存する、ルータ / ルータ トンネリング メカニズム

次の 2 つのセクションでは、ハイブリッド モデルについて、次の 2 つの具体例に沿って説明します。

- HME1 — ISATAP を介してアクセス レイヤのホストをコア レイヤ スイッチに接続、およびコア レイヤ以上のデュアルスタック
- HME2 — ディストリビューション レイヤとデータセンター アグリゲーション レイヤの間に手動設定トンネルを使用、およびアクセス / ディストリビューション レイヤのデュアルスタック

以下の各セクションでは、これらのモデルの概要を説明します。HME1 実装の詳細については、このマニュアルで後述します。

ハイブリッド モデル — 例 1

概要

HME1 は、基盤となるネットワーク インフラストラクチャが IPv6 をネイティブでサポートしていない場合にも、ホストに IPv6 サービスへのアクセスを提供します。

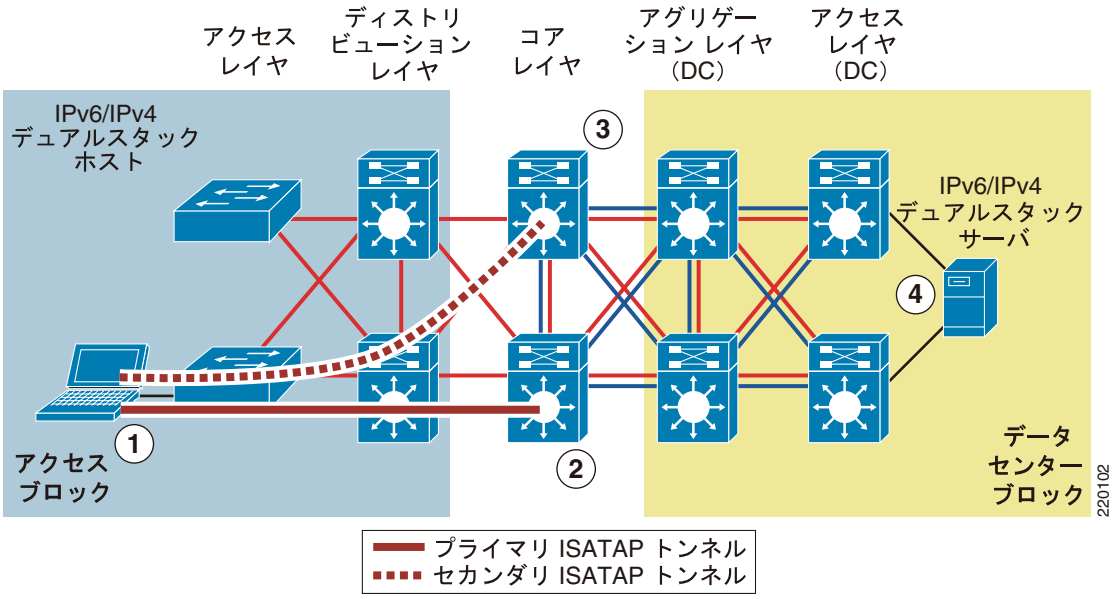
HME1 の重要な側面は、ディストリビューション レイヤが IPv6 対応ではない、またはイネーブル化できない場合でも、キャンパス アクセス レイヤに存在するホストが IPv6 サービスを使用できる点です。一般にディストリビューション レイヤ スイッチは、アクセス レイヤ デバイスへの最初のレイヤ 3 ゲートウェイです。既存のディストリビューション レイヤ スイッチに IPv6 機能がない場合、ホストは IPv6 アドレッシング（ステートレスな自動設定または DHCP for IPv6）ルータ情報にアクセスできず、結果的に IPv6 対応ネットワークの他の部分にアクセスできません。

IPv6 対応のホストでトンネリングを使用することにより、ディストリビューション レイヤから先にある IPv6 サービスへのアクセスを提供できます。例 1 では、アクセス レイヤのホストで ISATAP トンネリング メカニズムを使用して、IPv6 アドレッシングとオフリンク ルーティングを提供しています。アクセス レイヤの Microsoft Windows XP および Vista のホストでは、IPv6 をイネーブルにするとともに、静的な ISATAP ルータ定義または ISATAP ルータ アドレスに対応する DNS「A」レコード エントリを設定している必要があります。

（注） 設定の詳細については、「ネットワーク トポロジ」（p.46）を参照してください。

図 2 は、HME1 の基本的な接続フローを示しています。

図 2　　ハイブリッド モデル例 1 — 接続フロー



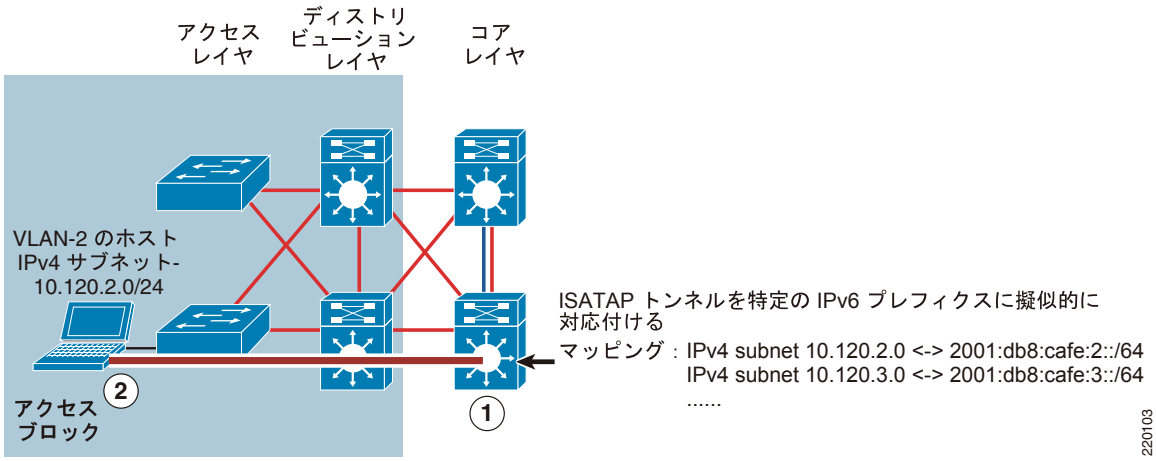
1. ホストがコア レイヤへの ISATAP トンネルを確立します。
2. コア レイヤ スイッチには ISATAP トンネル インターフェイスが設定されています。これらのスイッチは、ホストが確立した ISATAP トンネルの終端地点です。
3. ISATAP トンネルのハイ アベイラビリティを提供するため、1 対のコア レイヤ スイッチが ISATAP トンネル接続を受け入れるよう冗長に設定されています。両方のコア レイヤ スイッチに、同じ IPv4 アドレスを共有するループバック インターフェイスを設定することにより、冗長性が確保されます。両方のスイッチはこの冗長な IPv4 アドレスを ISATAP のトンネル ソースとして使用します。ホストが IPv4 ISATAP ルータ アドレスに接続するとき、2 つのスイッチのうちいずれか 1 つに接続します（これはロード バランスにすることも、いずれか一方のスイッチを優先するように設定することも可能です）。いずれか一方のスイッチで障害が発生すると、IPv4 Interior Gateway Protocol（IGP）がコンバージし、同じプライマリの IPv4 ISATAP アドレスを持つ、もう一方のスイッチを使用します。IGP コンバージェンス時間 + Neighbor Unreachability Detection（NUD）時間の満了で、フェールオーバーが実行されます。Microsoft Vista 構成の場合、ISATAP ルータ（コア スイッチ）の基本的なロード バランスを実装できます。Windows プラットフォームにおける Microsoft での ISATAP 実装についての詳細は、次の URL を参照してください。
   http://www.microsoft.com/downloads/details.aspx?FamilyId=B8F50E07-17BF-4B5C-A1F9-5A09E2AF698B&displaylang=en
4. デュアルスタックを設定されたサーバは、直接 IPv6 でアクセス可能なデュアルスタック対応のデータセンター ブロックを使用して、受信 IPv6 接続の受け入れと発信 IPv6 接続の確立を行います。

ISATAP トンネルを終端できる場所、およびホストが IPv6 上で到達できるリソースの制御を容易にするための方法の 1 つに、VLAN または IPv4 サブネットと ISATAP トンネルのマッチングの使用があります。

現在のネットワーク設計に、アクセス レイヤ スイッチのポートに対応付けられた固有の VLAN があり、そのスイッチに接続するユーザが所属する VLAN をベースとする IPv4 アドレッシングを受信している場合には、IPv6 および ISATAP トンネルを使用して、同じようなマッピングを行うことができます。

図 3 に、特定の VLAN および IPv4 サブネットのユーザを特定の ISATAP トンネルにマッチさせるプロセスを示します。

図 3　　ハイブリッド モデル例 1 — ISATAP トンネルのマッピング



1. コア レイヤ スイッチには、アドレス 10.122.10.2 のループバック インターフェイスが設定されています。これは ISATAP のトンネル ソースとして、10.120.2.0/24 サブネットに存在するユーザのみが使用します。
2. アクセス レイヤのホストは、特定の VLAN に対応付けられたポートに接続されます。この例では、VLAN は「VLAN-2」です。VLAN-2 のホストは、DHCP サーバ設定で IPv4 サブネット範囲（10.120.2.0/24）に対応付けられます。

ホストには、ISATAP ルータ値 10.122.10.2 を静的に割り当てます。この静的な割り当ては、いくつかの方法で実装できます。ホスト上のコマンド（**netsh interface ipv6 isatap set router 10.122.10.2** — 詳細についてはこのマニュアルで後述）で ISATAP ルータ設定を定義することができます。このコマンドは、手動で入力するか、または Microsoft SMS Server、Windows Scripting Host など、あらゆるスクリプト方式でスクリプト化することができます。このスクリプトによってホストの既存の IPv4 アドレスを検証し、ISATAP ルータをどの値に設定するかを決定できます。たとえば、スクリプトでホストの IPv4 アドレスを分析し、アドレス 10.120.2.x/24 の値「2」がサブネット値を表していると判別できます。スクリプトでは次に、ISATAP ルータ アドレス 10.122.10.2（ここで「2」はサブネットまたは VLAN 2 を表す）を使用してコマンドを適用できます。10.122.10.2 アドレスは、実際にはコア レイヤ スイッチのループバック アドレスであり、ISATAP のトンネル エンドポイントとして使用されます。

（注） 上記の方法による詳しい設定手順については、「ネットワーク トポロジ」（p.46）を参照してください。

次のような理由から、お客様に上記の方法の利用を推奨します。

- コントロールと分離 — 特定の IPv4 サブネットからの特定のリソースへのアクセスを禁止するセキュリティ ポリシーがあり、ACL を使用してそのポリシーを実施している場合。このポリシーを考慮せずに HME1 を実装すると、どうなるかを考えてみましょう。制限付きのリソースが IPv6 でアクセス可能な場合、以前は IPv4 でアクセスを禁止されていたユーザが、IPv6 を介して保護されたリソースにアクセスできるようになります。何百人、何千人ものユーザに ISATAP が設定されているにも関わらず、コア レイヤ デバイスで使用する ISATAP トンネル インターフェイスが 1 つだけだとすると、ACL 経由で送信元アドレスを制御するのは、スケーラビリティと管理の点で非常に難しくなります。VLAN と IPv4 サブネットでユーザを分離するのと同じ方法で、ISATAP トンネル別にユーザを論理的に分離すれば、IPv6 送信元、送信元 / 宛先、さらにはレイヤ 4 情報に基づいて、アクセスを許可または拒否する ACL を容易に配置できます。

- スケーラビリティ — キャンパス ネットワークの VLAN ごとのデバイス台数をコントロールすることが、長年にわたって共通のベスト プラクティスとされてきました。このプラクティスは、従来ブロードキャスト ドメインの制御に適用されてきました。IPv6 および ISATAP トンネルはブロードキャストを使用しませんが、スケーラビリティについて考慮が必要であることに変わりはありません。カスタマー サイトでの導入経験上、1 つまたは少数のトンネル インターフェイスで多数のホストを処理するよりも、多数のトンネル インターフェイスに少数のホストを分散させるべきであるという結論に達しました。ISATAP トンネル インターフェイスごとの最適なホスト数は不明ですが、1 つの ISATAP 構成に何千台ものホストが配置されないかぎり、重大な問題ではないと考えられます。しかしながら、シスコが発行するドキュメント（http://www.cisco.com/ipv6）および独立テスト機関による ISATAP スケーラビリティ テストの結果とベスト プラクティスには、引き続きご注意ください。

ソリューションの要件

HME1 ストラテジーに関する主なソリューション要件は、次のとおりです。

- ホスト マシンの OS で IPv6 および ISATAP がサポートされていること。
- コア レイヤ スイッチで IPv6/IPv4 デュアルスタックおよび ISATAP 機能がサポートされていること。

前述したように、エンタープライズ キャンパス環境内で IPv6 接続を提供するには、さまざまなトランジション メカニズムを組み合わせて使用できます。たとえば、上記の要件に関しては、次の 2 つの代替手段があります。

- アクセス レイヤで Linux、FreeBSD、Sun Solaris、Mac OS X など、複数の OS が使用されている場合には、ISATAP の代わりに 6to4 トンネリングを使用します。6to4 を使用する場合のセキュリティ面への影響については、各自ご確認ください。
- ネットワーク レイヤでコア レイヤ以外の場所（たとえば、データセンターのアグリゲーション レイヤなど）でトンネルを終端します。

（注） 6to4 およびコア レイヤ以外のトンネル終端については、このマニュアルでは説明しません。HME1 に関する導入上の推奨事項のなかで、予備的な選択肢としてのみ紹介しています。

このソリューションの利点と欠点

HME1 の主な利点は、（特にディストリビューション レイヤ スイッチの）アップグレードを必要とせず、既存のネットワーク機器を利用できる点です。現在使用中のディストリビューション レイヤ スイッチで、許容範囲の IPv4 サービスおよびパフォーマンスが提供されていて、スイッチが減価償却中であれば、HME1 は妥当な選択肢です。

ハイブリッド モデル、特に HME1 の欠点を理解しておくことが重要です。

- この設計の ISATAP 部分のスケーラビリティについては、まだ判明していません。次のような疑問点の答えがまだ出ていません。
  - スイッチのトンネル インターフェイス 1 つで終端できるホストの数はいくつか。
  - ISATAP トンネルのカプセル化 / 非カプセル化のトラフィック処理が個々のホストに与える CPU 負荷。
- ISATAP トンネルでは、IPv6 マルチキャストはサポートされていません。これは RFC 4214 で解決すべき制約事項です。
- ISATAP トンネルはコア レイヤで終端されるので、IPv6 トラフィックからはコア レイヤがアクセス レイヤのように認識されます。ネットワーク管理者およびネットワーク設計者はコア レイヤを設計する際、ネットワークにおけるコア レイヤの役割に最適化するように設計しており、一般に安定性、簡素性、高速性が要求されます。コア レイヤに新たなレベルのインテリジェンスを追加するのは、望ましくありません。

トンネリングを使用するすべての設計と同じように、考慮すべき事項としては、パフォーマンス、管理、セキュリティ、スケーラビリティ、およびアベイラビリティがあります。どのような場合でも、トンネルの使用よりも DSM 設計を推奨します。

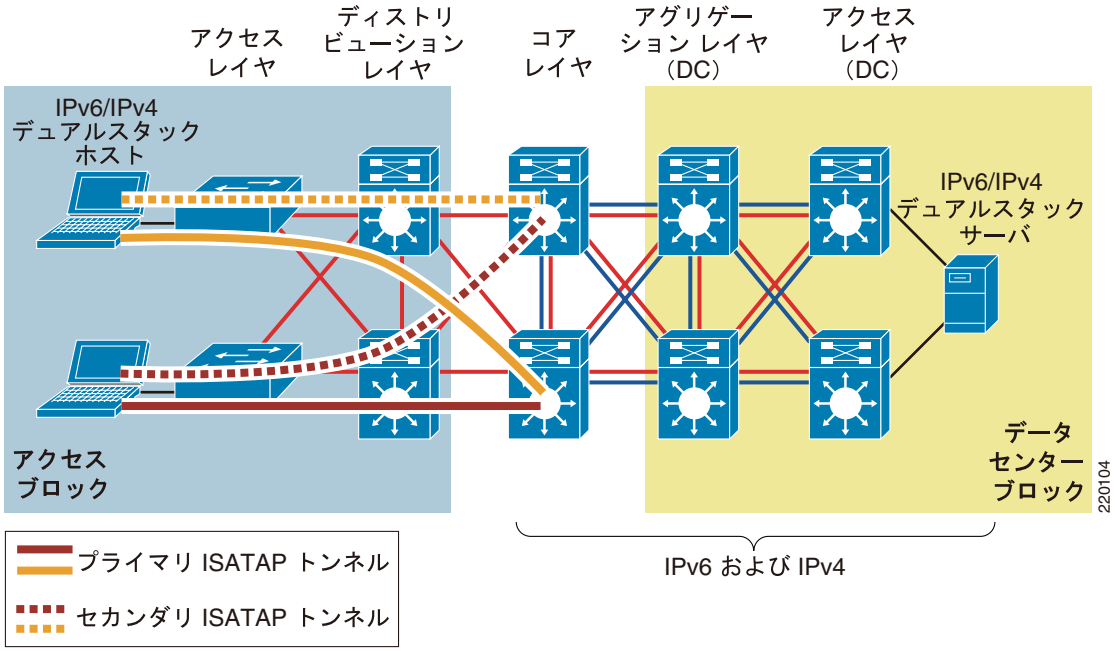
「まとめ」（p.63）では、各種のキャンパス設計モデルの利点と課題を表形式で要約します。

ソリューション トポロジ

図 4 は、キャンパス HME1 の概念図です。この例は、このマニュアルで後述する詳細設定の基本となります。

（注） この図のデータセンター ブロックはあくまで参考用であり、このマニュアルでは説明しません。データセンターでの IPv6 の導入については、別のマニュアルで説明する予定です。

図 4　　ハイブリッド モデル例 1



動作確認済みのコンポーネント

表 2 に、HME1 構成で使用し動作確認を行ったコンポーネントを示します。

表 2　　HME1 で動作確認済みのコンポーネント

キャンパス レイヤ	ハードウェア	ソフトウェア
アクセス レイヤ	Catalyst 3750	Advanced IP Services — 12.2(25)SED1
ホスト デバイス	各種のノート型パソコン — IBM、HP	Microsoft Windows XP SP2、Vista RC1
ディストリビューション レイヤ	Catalyst 3750	Advanced IP Services — 12.2(25)SED1

表 2　HME1 で動作確認済みのコンポーネント（続き）

キャンパス レイヤ	ハードウェア	ソフトウェア
	Catalyst 4500 Supervisor 5	Enhanced L3 3DES — 12.2.25.EWA6
	Catalyst 6500 Supervisor 2/MSFC2	Advanced Enterprise Services SSH — 12.2(18)SXF5
コア レイヤ	Catalyst 6500 Supervisor 720	Advanced Enterprise Services SSH — 12.2(18)SXF5

ハイブリッド モデル — 例 2

概要

HME2 は、コア レイヤでの IPv6 サポートがない場合に、このギャップを埋めることで、IPv6 サービスへのアクセスを提供します。この例では、デュアルスタックはアクセス / ディストリビューション レイヤでサポートされるほか、データセンターのアクセス レイヤおよびアグリゲーション レイヤでサポートされます。一般にコア レイヤが IPv6 対応でない理由は、コア レイヤにハードウェアベースの IPv6 サポートがまったくない場合か、IPv6 を限定的にサポートしていてもパフォーマンス能力が低い場合です。

この構成では、ディストリビューション レイヤとアグリゲーション レイヤの間でのみ、手動設定トンネルを使用します。各スイッチから 2 つのトンネルを使用して、冗長性とロード バランスを確保します。IPv6 の観点では、これらのトンネルはディストリビューションとアグリゲーション レイヤ スイッチの間の仮想リンクと考えることができます。トンネルには、デュアルスタック設定と同じ方法でルーティングと IPv6 マルチキャストを設定します。QoS に関する相違点は、**mls qos trust dscp** ステートメントをトンネル インターフェイスではなく、コアに接続する物理インターフェイスに適用する点のみです。トンネル トラフィックまたは IPv6 トラフィックに影響を与える可能性のある、特殊な QoS 設定をコアで使用する場合は、この設定を考慮する必要があります。コアの QoS ポリシーには、IPv6 パケットに関する可視性がないためです。ネットワーク コアのセキュリティについても、同様の考慮事項が当てはまります。コア レイヤに特殊なセキュリティ ポリシーが存在する場合、それらのポリシー（サポートされる場合）を、コアを通過するトンネル トラフィックに対応するように修正する必要があります。

手動設定トンネルの動作および設定についての詳細は、「その他の関連資料」（p.64）を参照してください。

このソリューションの利点と欠点

HME2 は、キャンパス コアをアップグレード中の場合、またはアップグレードを計画していて、コアのアップグレードを完了する前に IPv6 サービスへのアクセスが必要とされる場合に適したモデルです。

キャンパス内の大部分のトラフィックと同じように、IPv6 はできるだけ速く転送する必要があります。トンネリングを使用する場合は、IPv6 パケットのカプセル化 / 非カプセル化という余分なステップが加わるので、特に高速な転送が必要です。Catalyst 6500 Supervisor 32 および 720 などの Cisco Catalyst プラットフォームは、トンネリングされる IPv6 トラフィックをハードウェアで転送します。

HME2 は HME1 ほど多くのネットワークに適しているわけではありませんが、モデル概要のセクションでは 1 つの選択肢として紹介しています。このマニュアルの設定 / 実装のセクションには、HME2 は記載されていません。HME2 の実装は比較的分かりやすく、ルーティング、QoS、マルチキャスト、インフラストラクチャ セキュリティ、および管理については、デュアルスタック モデルの考慮事項とほぼ同じためです。

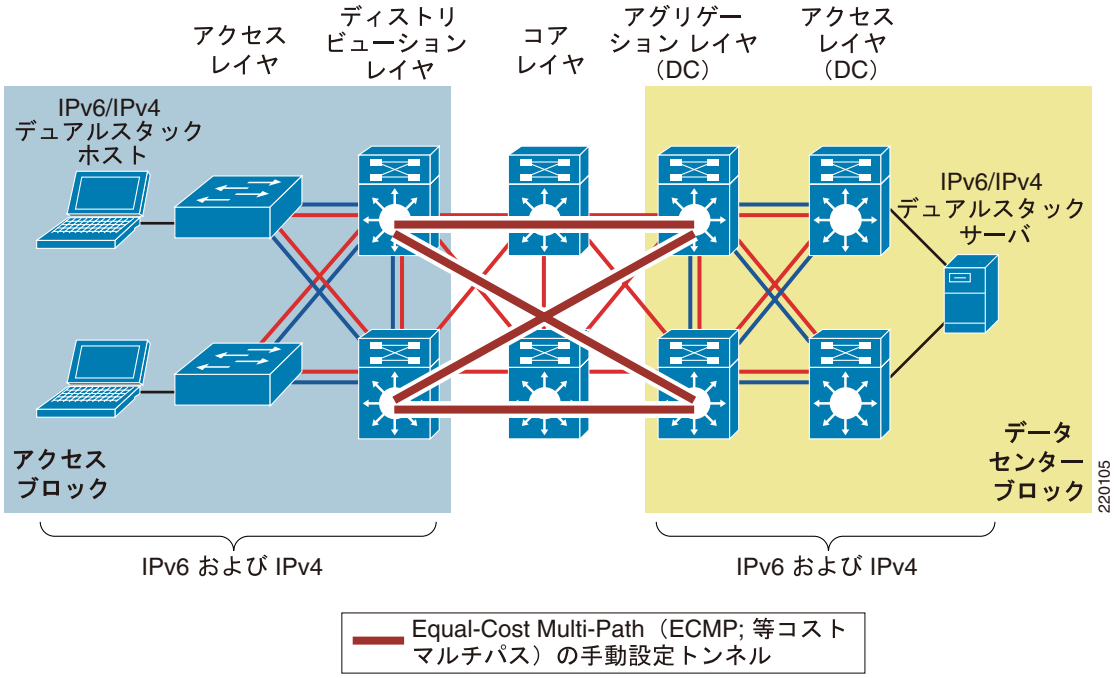
トンネリングを使用するすべての設計と同じように、考慮すべき事項としては、パフォーマンス、管理（静的トンネルの管理は一般に複雑です）、スケーラビリティ、およびアベイラビリティがあります。どのような場合でも、トンネルの使用よりも DSM 設計を推奨します。

「まとめ」（p.63）で、各種のキャンパス設計モデルの利点と問題点を表形式で要約します。

ソリューション トポロジ

図 5 は、HME2 の概念図です。前述したように、アクセス / ディストリビューション レイヤは（レイヤ 2 アクセスまたはレイヤ 3 ルーテッド アクセス モデルのいずれかで）IPv6 を完全にサポートしており、データセンターのアクセス / アグリゲーション レイヤも IPv6 をサポートしています。この例では、コア レイヤは IPv6 をサポートしていません。ディストリビューション / アグリゲーション レイヤ スイッチ間で、手動で冗長トンネルを設定し、コア レイヤの IPv6 転送機能を提供しています。

図 5　　ハイブリッド モデル例 2



動作確認済みのコンポーネント

表 3 に、HME2 構成で使用し動作確認を行ったコンポーネントを示します。

表 3　　HME2 で動作確認済みのコンポーネント

キャンパス レイヤ	ハードウェア	ソフトウェア
アクセス レイヤ	Catalyst 3750	Advanced IP Services — 12.2(25)SED1
	Catalyst 6500 Supervisor 32 または 720	Advanced Enterprise Services SSH — 12.2(18)SXF5
ホスト デバイス	各種ノート型パソコン — IBM、HP、および Apple	Microsoft Windows XP SP2、Vista RC1、Apple Mac OS X 10.4.7、および Red Hat Enterprise Linux WS

表 3　HME2 で動作確認済みのコンポーネント（続き）

キャンパス レイヤ	ハードウェア	ソフトウェア
ディストリビューション レイヤ	Catalyst 6500 Supervisor 32 または 720	Advanced Enterprise Services SSH — 12.2(18)SXF5
コア レイヤ	Catalyst 6500 Supervisor 2/MSFC2	Advanced Enterprise Services SSH — 12.2(18)SXF5
データセンター アグリゲーション レイヤ	Catalyst 6500 Supervisor 720	Advanced Enterprise Services SSH — 12.2(18)SXF5

サービス ブロック モデル

概要

SBM は、このマニュアルで説明するキャンパス モデルの中で最も特異です。サービス ブロック式の設計という概念は新しいものではありませんが、短期間で IPv6 サービスへのアクセスを提供するという課題に直面しているお客様には、SBM は独自の機能を提供します。サービス ブロック式アプローチは、他の設計分野でも使用されており、シスコのネットワーク仮想化（http://www.cisco.com/en/US/netsol/ns658/networking_solutions_package.html）では、この概念を「サービス エッジ」と呼んでいます。SBM は、既存の IPv4 ネットワークに影響を与えないオーバーレイ ネットワークとして導入することができ、完全に中央集中型であるという点が独特です。このオーバーレイ ネットワークは、既存の IPv4 ネットワークにほとんど変更を加えずに、アベイラビリティの高い IPv6 サービス、QoS 機能、IPv6 リソースへのアクセス制限を実現しながら、スピーディに実装できます。

既存のキャンパス ネットワークが IPv6 対応になった時点で、SBM を非集中型にすることができます。SBM への接続は、トンネル（ISATAP および / または手動設定）からデュアルスタック接続に変更します。すべてのキャンパス レイヤがデュアルスタック対応になった時点で、SBM を解体し、他の目的に用途転換することができます。

SBM 構成は、Supervisor 32 または Supervisor 720 を搭載した Catalyst 6500 スイッチの冗長ペアを基本とします。SBM のスケーラビリティに優れた冗長な構成を維持するうえで重要なのは、キャンパス ネットワーク全体で ISATAP、手動設定トンネル、およびデュアルスタック接続の負荷を処理するために、高性能なスイッチ、スーパーバイザ、およびモジュールを使用することです。トンネル数が増え、高いスループットが要求されるようになると、SBM にスイッチ ペアを追加して、負荷を分散する必要が生じる可能性があります。

このマニュアルで示す SBM の例と、HME1 および HME2 の例の組み合わせには、多くの類似点があります。既存の IPv4 ネットワークを、導入するオーバーレイ IPv6 ネットワークの基盤として使用します。アクセス レイヤのホストへのアクセスは、ISATAP によって提供されます（HME1 と同様）。データセンターのアグリゲーション レイヤから手動設定トンネルを使用して、データセンターのアクセス レイヤに存在するアプリケーションおよびサービスへの IPv6 アクセスを提供します（HME2 と同様）。コア レイヤと SMB スイッチの間に IPv4 ルーティングを設定し、IPv6-in-IPv4 トンネルを終端する目的で、SMB スイッチへの可視性を提供します。ただし、このマニュアルで説明する例では、キャンパス ネットワーク（アクセス、ディストリビューション、またはコア レイヤ）のいずれにも IPv6 機能が存在していないという極端なケースを分析します。このマニュアルで使用している SBM の例では、スイッチを冗長高速リンク経由でコア レイヤに直接接続しています。

このソリューションの利点と欠点

概念的に見た場合の SBM 実装の利点は、IPv6 サービスをホストに迅速に提供できる点、既存のネットワーク構成への影響が少ない点、および IPv6 対応のアプリケーションへのアクセスを柔軟に制御できる点です。

基本的に、SBM では次の機能により、IPv6 サービスの展開を迅速化できます。

- ISATAP によるユーザ単位および / または VLAN トンネル単位での設定により、接続のフローの制御や、IPv6 トラフィック使用状況の計測が可能です。
- SBM では ACL および / またはルーティング ポリシーにより、サーバ単位またはアプリケーション単位でアクセスを制御できます。このレベルの制御により、1 つ、少数、または多数の IPv6 対応サービスへのアクセスを可能にしながら、アップグレードまたは交換の時期まで、他のすべてのサービスを IPv4 のままにしておくことができます。その結果 IPv6 を「サービス単位で」導入できます。
- ISATAP、手動設定トンネル、およびデュアルスタック接続のハイ アベイラビリティを提供できます。
- ホストから IPv6 対応の ISP 接続へのアクセスには、柔軟なオプションがあり、IPv6 ベースのインターネット トラフィック専用の隔離された IPv6 接続を提供するか、または IPv4 と IPv6 の両方の ISP 接続のある既存のインターネット エッジ接続へのリンクを提供することができます。
- SBM の実装は、既存のネットワーク インフラストラクチャおよびサービスを中断しません。

HME1 および HME2 の項で説明したように、サービスへのアクセスを提供するための主要な手段としてトンネリング メカニズムに依存する設計には、欠点があります。SBM には、HME 設計と同じ欠点（トンネリングの多さ）があるだけでなく、HME1 や HME2 にはない、追加の機器のコストという問題も加わります。余分なスイッチ（SBM スイッチ）、SBM およびコア レイヤ スイッチに接続するためのラインカード、および必要なメンテナンスやソフトウェアにより、コストが増加します。

HME1、HME2、SBM にはこのような欠点があるため、シスコは常に DSM の導入を推奨します。

「まとめ」（p.63）で、各種のキャンパス設計モデルの利点と問題点を表形式で要約します。

ソリューション トポロジ

このマニュアルでは、SBM 設計の 2 つの部分について説明します。図 6 は設計の ISATAP 部分、図 7 は手動設定トンネルの部分を示しています。これらの図は、キャンパス ネットワークで成立する可能性のある多くの組み合わせのうち 2 つだけを示したものであり、IPv6 設計の目標と、キャンパス インフラストラクチャ内のプラットフォームとソフトウェアの機能に基づいて区別されています。

前述したように、データセンターに固有の設計とその課題については別のマニュアルで説明する予定です。このマニュアルではデータセンター レイヤについては詳しく説明しません。このマニュアルでは、完全を期するためにデータセンターの基本的な構成のみを示しています。データセンターの部分をできるだけ簡素化するために、データセンターのアグリゲーション レイヤには、SBM への手動設定トンネルと、アグリゲーション レイヤからアクセス レイヤへのデュアルスタックを使用しています。

図 6 には、アクセス レイヤのホストから SBM スイッチへの冗長な ISATAP トンネルが示されています。SBM スイッチは、IPv4 対応のリンク経由でコア レイヤ スイッチに直接リンクすることにより、キャンパス ネットワークの他の部分に接続されています。SBM スイッチ同士は、IPv4 および IPv6 ルーティングとハイ アベイラビリティのために使用されるデュアルスタック接続を介して、相互に接続されています。

図 6　サービス ブロック モデル — ホストの接続（ISATAP のレイアウト）

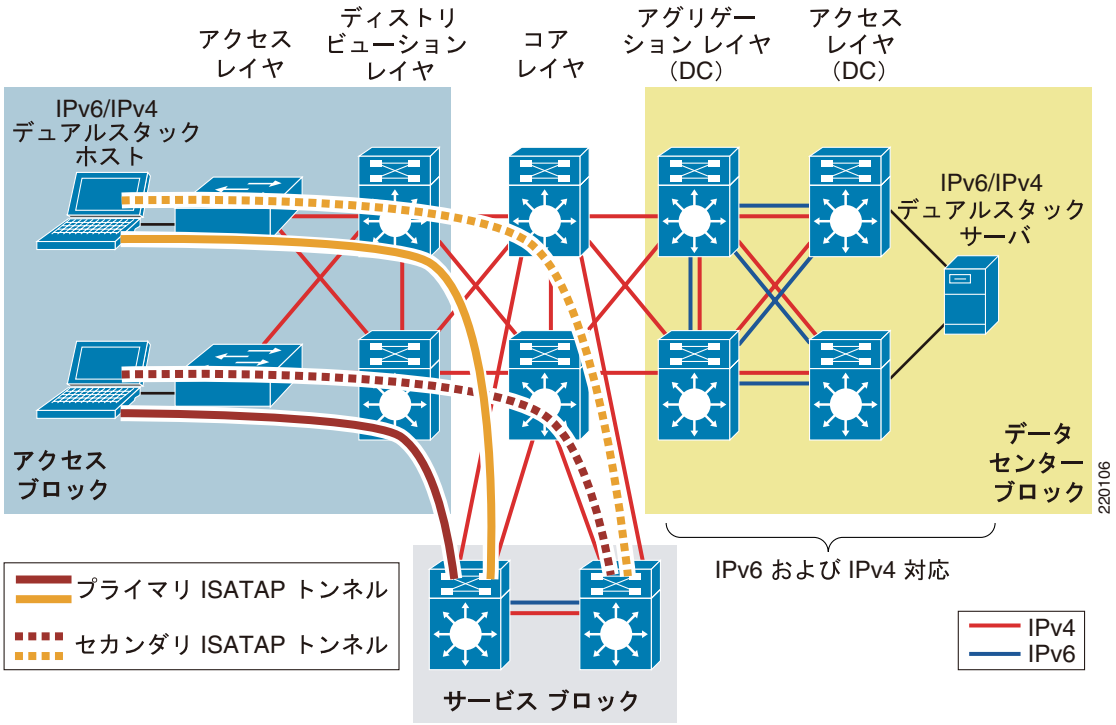
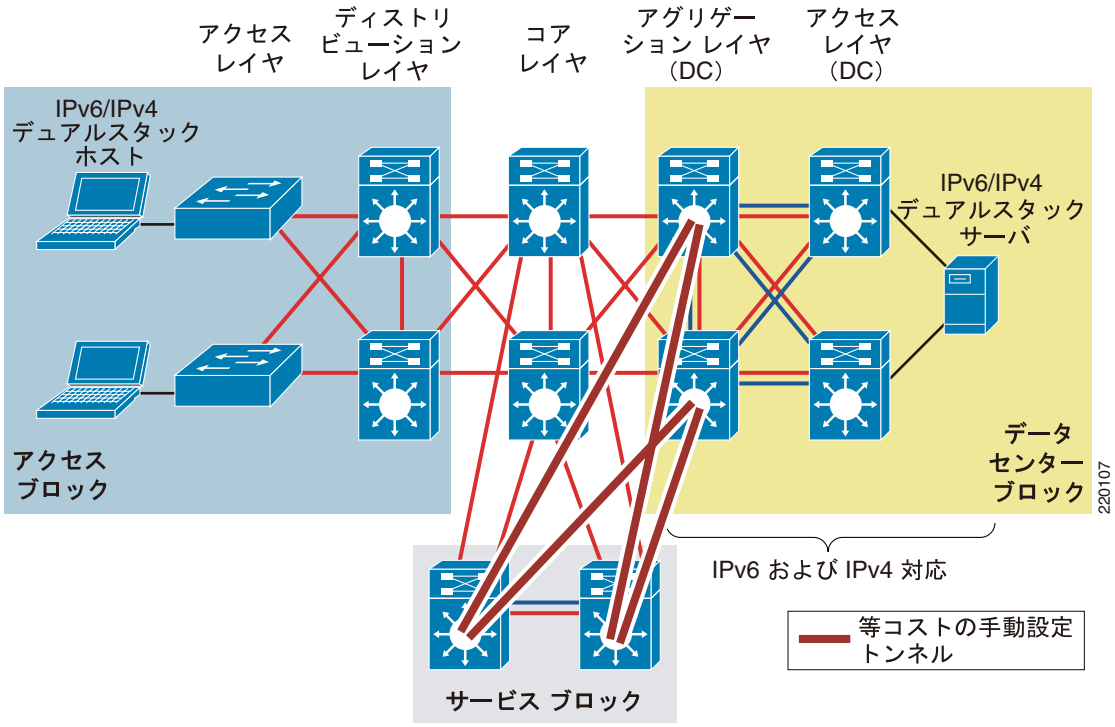


図 7 に、データセンターのアグリゲーション レイヤとサービス ブロックを接続する、手動設定の冗長なトンネルを示します。アクセス レイヤに存在するホストは、IPv6 を使用して、データセンターのアクセス レイヤにある IPv6 サービスに到達できます。この構成の詳細については、「まとめ」（p.63）を参照してください。

図 7　サービス ブロック モデル — データセンターの接続（手動設定トンネルのレイアウト）



動作確認済みのコンポーネント

表 4 に、SBM 構成で使用し動作確認を行ったコンポーネントを示します。

表 4　SBM で動作確認済みのコンポーネント

キャンパス レイヤ	ハードウェア	ソフトウェア
アクセス レイヤ	Catalyst 3750	Advanced IP Services — 12.2(25)SED1
	Catalyst 6500 Supervisor 32 または 720	Advanced Enterprise Services SSH — 12.2(18)SXF5
ホスト デバイス	各種のノート型パソコン — IBM、HP	Microsoft Windows XP SP2、Vista RC1
ディストリビューション レイヤ	Catalyst 3750	Advanced IP Services — 12.2(25)SED1
	Catalyst 4500 Supervisor 5	Enhanced L3 3DES — 12.2.25.EWA6
	Catalyst 6500 Supervisor 2/MSFC2	Advanced Enterprise Services SSH — 12.2(18)SXF5
コア レイヤ	Catalyst 6500 Supervisor 720	Advanced Enterprise Services SSH — 12.2(18)SXF5
サービス ブロック	Catalyst 6500 Supervisor 32 または 720	Advanced Enterprise Services SSH — 12.2(18)SXF5

一般的な考慮事項

このマニュアルで説明するすべての導入モデルに当てはまる、多くの考慮事項があります。ここでは、使用する導入モデルに関わらず、キャンパス ネットワークに IPv6 を導入する場合に考慮する必要のある一般的な事項について説明します。特定のモデルに関連して理解しておく必要のある考慮事項については、そのモデルを明記します。なお、モデル固有の考慮事項に対応する設定は、そのモデルの実装のセクションを参照してください。

このマニュアルで説明するキャンパス IPv6 モデルはすべて、既存のキャンパス ネットワーク設計を利用し、物理アクセス、VLAN、IPv4 ルーティング（トンネル）、QoS（トンネル）、インフラストラクチャ セキュリティ（トンネルの保護）、およびアベイラビリティ（デバイス、リンク、トランク、およびルーティング）を提供するための基盤としています。デュアルスタックを使用する場合、シスコのキャンパス設計ベストプラクティスの資料に記載されているほとんどすべての設計原則が、IPv4 と IPv6 の両方に適用されます。

このマニュアルに記載された IPv6 キャンパス モデルの導入を開始する前に、シスコのキャンパスに関するベスト プラクティスの推奨事項を理解しておくことが重要です。

シスコのキャンパス設計ベスト プラクティスの資料は、次の URL の「Campus」セクションを参照してください。
http://www.cisco.com/go/srnd

アドレッシング

前述したように、このマニュアルは入門書ではないため、IPv6 アドレッシングの基本事項については説明していません。ただし、ネットワーク デバイスのアドレッシングに関する重要な考慮事項をいくつか説明します。

ほとんどの場合、point-to-point（p2p; ポイントツーポイント）リンクでは /64 プレフィクスを使用すれば問題ありません。IPv6 は大きいアドレス スペースを使用するように設計されているので、アドレス管理が充分ではない場合でも、お客様がアドレスの制約を経験することはないはずです。

p2p リンクに /64 プレフィクスを使用することを無駄と考えるネットワーク管理者もいます。p2p リンクに、より長いプレフィクスを使用するという慣例については、IPv6 コミュニティで盛んに議論されてきました。さらに厳密なアドレス スペースの制御を希望する場合は、IPv4 で /30 を使用するのと同様、p2p リンクで /126 プレフィクスを使用すると安全です。

RFC 3627（http://www.ietf.org/rfc/rfc3627.txt）に、/127 プレフィクスの使用は有害であり、避けるべきである理由が説明されています。

一般に、p2p リンクでは /64 または /126 を使用することをシスコは推奨します。

IETF では、さまざまなアドレス タイプおよびプレフィクス リンクに関するアドレス割り当てのガイドラインを文書化する作業を続けています。IETF の IPv6 オペレーションズ ワーキング グループによる成果は、次の URL で確認できます。
http://www.ietf.org/html.charters/v6ops-charter.html

このマニュアルで示す p2p 設定では、/64 プレフィクスを使用しています。

物理接続

IPv6 における物理接続についての考慮事項は IPv4 と同じものに加えて、次の 3 つの要素があります。

- 既存のトラフィックと新しいトラフィックの両方に十分な帯域幅を確保すること

  これは新しいテクノロジー、プロトコル、またはアプリケーションを導入する場合には常に重要です。

- IPv6 によるリンク上での Maximum Transmission Unit（MTU; 最大伝送ユニット）の取り扱い方法を理解しておくこと

  このマニュアルは入門書ではないため、IPv6 の基本的なプロトコル動作や仕様については説明しません。IPv6 における MTU およびフラグメンテーションについての詳細は、次の資料を参照することを推奨します。IPv6 における MTU および Path MTU Discovery（PMTUD）について基本事項を知るには、次の URL に掲載されている RFC 2460 および RFC 1981 が適しています。

  - http://www.ietf.org/rfc/rfc2460.txt
  - http://www.ietf.org/rfc/rfc1981.txt

- ワイヤレス LAN（WLAN）上の IPv6

  IPv6 は、レイヤ 2 スイッチ上で動作する場合と同様に、WLAN アクセス ポイント上でも正常に動作します。ただし、WLAN 環境での IPv6 の仕様には、IPv6 による WLAN デバイス（AP およびコントローラ）の管理や、AP またはコントローラベースの QoS、VLAN、および ACL による IPv6 トラフィックの制御が含まれる点に注意する必要があります。WLAN デバイスでこれらのインテリジェントなサービスを利用するには、AP および / またはコントローラ デバイスで IPv6 がサポートされていることが前提となります。

シスコは、Cisco IP Phone ポートに直接接続された IPv6 対応ホストの使用をサポートしています。Cisco IP Phone ポートはスイッチ ポートであり、Catalyst レイヤ 2 スイッチにホストを直接接続する場合と同じように動作します。

このマニュアルで説明する IPv6 モデルを実装する前に、上記の考慮事項に加えて、ホストとネットワーク機器の既存のトラフィック プロファイル、メモリ、および CPU 利用率を綿密に分析することを推奨します。また、Service Level Agreement（SLA; サービス レベル契約）を完成させておくことを推奨します。

VLAN

IPv6 における VLAN についての考慮事項は、IPv4 と同様です。デュアルスタック構成を使用する場合、IPv4 と IPv6 の両方が同じ VLAN を通過します。トンネリングを使用する場合、IPv4 とトンネリングされた IPv6（プロトコル 41）トラフィックが VLAN を通過します。このマニュアルで説明する導入モデルでは、プライベート VLAN の使用については言及されておらず、動作確認もされていませんが、今後のキャンパス IPv6 マニュアルには記載される予定です。

（IP Phone による）音声 VLAN とトランキングされたデータ VLAN での IPv6 の使用が、完全にサポートされています。

現時点での VLAN 設計に関する推奨事項については、「その他の関連資料」（p.64）に記載されている、シスコのキャンパス設計ベスト プラクティスの資料を参照してください。

ルーティング

キャンパス ネットワークで実行する IGP の選択は、プラットフォームの機能、IT スタッフの専門知識、トポロジ、ネットワークの規模など、さまざまな要因に基づきます。このマニュアルでは、IGP for IPv4 は EIGRP ですが、OSPFv2 for IPv4 も使用できます。キャンパス内の IGP には、OSPFv3 for IPv6 を使用します。

（注） このマニュアルの作成時点では、Cisco IOS では EIGRP for IPv6 が使用可能ですが、Catalyst プラットフォームにはまだ実装されていません。今後のテストおよびマニュアルでは、EIGRP for IPv6 および OSPFv3 for IPv6 の両方について、設計と設定に関する推奨事項を反映させる予定です。最新情報については、次の URL にある CCO のリンクを参照してください。
http://www.cisco.com/go/ipv6

前述したように、シスコではキャンパス設計に関する最新のベスト プラクティスの実装に取り組んでいます。可能な限り最新のベスト プラクティスに従って、IPv4 および IPv6 の IGP をチューニングしています。安定性とスケーラビリティが高く、コンバージェンスの速いネットワークを提供するように IGP をチューニングすることは、ネットワーク設計における最優先事項の 1 つにする必要があります。

OSPFv3 に関して注意すべき最後の考慮事項として、このマニュアルの作成時点では、テスト対象の Cisco Catalyst プラットフォームに IPsec for OSPFv3 は実装されていません。IPsec for OSPFv3 は、OSPFv3 ネイバー接続とルーティング アップデートの認証と暗号化を提供します。IPsec for OSPFv3 についての詳細は、次の URL を参照してください。
http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/ipv6_c/sa_ospf3.htm#wp1160900

ハイ アベイラビリティ

ハイ アベイラビリティ（HA）については、ほとんどの側面がこのマニュアルで扱う範囲外にあります。HA に関する要件および推奨事項の多くは、シスコの既存のキャンパス設計ベスト プラクティスを活用することで達成できます。このマニュアルで説明する主な HA コンポーネントは、次のとおりです。

- 冗長ルーティングおよびフォワーディング パス ― トンネルに冗長パスが必要な場合には EIGRP for IPv4 を使用し、デュアルスタックを使用する場合には OSPFv3 for IPv6 を使用するとともに、Cisco Express Forwarding（CEF; シスコ エクスプレス フォワーディング）の機能を使用することで達成できます。
- ISATAP および手動設定トンネルを終端する、冗長レイヤ 3 スイッチ ― HME1、HME2、および SBM 設計においては、冗長なハードウェアに加えて、冗長なトンネル（ISATAP および手動設定）を実装することが重要です。実装セクションでは、HME1 および SBM 設計における冗長トンネルの設定および結果を具体的に示します。
- ファーストホップ ゲートウェイのハイ アベイラビリティ ― DSM 設計では、アクセス レイヤのホストにとって最初のレイヤ 3 デバイスが、ディストリビューション レイヤ スイッチです。従来のキャンパス設計では、Hot Standby Routing Protocol（HSRP）、Gateway Load Balancing Protocol（GLBP）、または Virtual Router Redundancy Protocol（VRRP; 仮想ルータ冗長プロトコル）などのファーストホップ冗長性プロトコルを使用して、ファーストホップ冗長性を提供しています。

（注） このマニュアルの作成時点では、Cisco IOS における IPv6 用に HSRP および GLBP が使用可能ですが、Catalyst プラットフォームにはまだ実装されていません。

キャンパス プラットフォームでのファーストホップ冗長性プロトコルの欠如に対処するには、プライマリのディストリビューション スイッチの障害に備えて、ある程度の冗長性を提供する方式を実装する必要があります。IPv6 用の近隣探索（RFC 2461）は、Neighbor Unreachability Detection（NUD）を実装します。NUD は、ホストのデフォルト ゲートウェイ リストに存在するルータ（ネイバー）が到達不能であるかどうかをホストが判別できるメカニズムです。ホストはローカル リンク上のルータから、定期的なルータ アドバタイズメント（RA）を通じて、NUD 値（到達可能時間）を受信します。デフォルトの到達可能時間は 30 秒です。

ホストは NUD を使用して、IPv6 ユニキャスト トラフィック用のプライマリ ゲートウェイが到達不能であるかどうかを判別します。タイマーが起動され、そのタイマー（到達可能時間の値）が満了すると、ネイバーはデフォルト ゲートウェイ リスト内で次に使用可能なルータへの IPv6 ユニキャスト トラフィックの送信を開始します。デフォルト設定では、ホストは 30 秒以内にデフォルト ゲートウェイ リスト内の次のゲートウェイを使用します。

アクセス レイヤ側の VLAN では、**(config-if)#ipv6 nd reachable-time 5000** コマンドを使用して、到達可能時間を 5000 ミリ秒（5 秒）に調整することを推奨します。この値を使用すると、ホストは 5 秒以内でセカンダリ ディストリビューション レイヤ スイッチに切り替えることができます。

最近のテストによると、Cisco Catalyst スイッチに接続するホストで、推奨されるキャンパス HA 設定とともに、到達可能時間に 5 秒を使用すれば、1 秒以上かかる IPv6 トラフィックのフェールオーバーはほとんど発生しません。到達可能時間は、ホストが次のゲートウェイに移るまでの最大時間であることを忘れないでください。

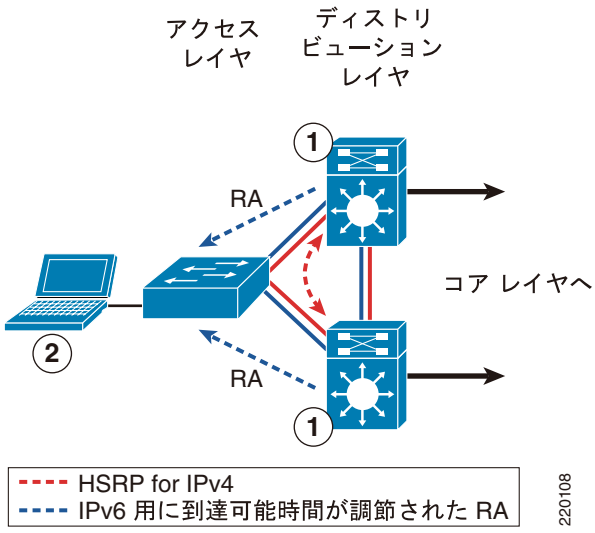
NUD について注意すべき問題として、Microsoft Windows XP および 2003 のホストは、ISATAP インターフェイスで NUD を使用しません。つまり、トンネル インターフェイス上で IPv6 のデフォルト ゲートウェイが到達不能になった場合、他のトンネルおよびゲートウェイへのトンネルを再確立するまでに、相当な時間がかかることを意味します。Microsoft Windows Vista および Windows Server コード名「Longhorn」では、ISATAP インターフェイスで NUD を有効にすることができます。ホストで直接、**netsh interface ipv6 set interface** *interface_Name_or_Index* **nud=enabled** をイネーブルにできます。

NUD 値の調整は、ホストが存在するリンク /VLAN でのみ行う必要があります。HSRP for IPv6 または GLBP for IPv6 などの実際のファーストホップ冗長性プロトコルをサポートするスイッチでは、到達可能時間を調整する必要はありません。

以上、フェールオーバーの決定プロセスについて、きわめて単純化して説明しました。ホストがネイバーの損失を判別する動作は非常に複雑であり、このマニュアルでは詳しく扱いません。NUD の動作についての詳細は、次の URL を参照してください。
http://www.ietf.org/rfc/rfc2461.txt

図 8 に、2 つのディストリビューション レイヤ スイッチから IPv6 RA を受信する、アクセス レイヤのデュアルスタック ホストを示します。これら 2 つのディストリビューション スイッチでは、HSRP、GLBP、または VRRP for IPv6 によるファーストホップ冗長性は使用されていません。NUD メカニズムを調整することで、ファーストホップ ゲートウェイの損失をホストが大まかに判断できるようになります。

図 8　　ディストリビューション レイヤから調整済みの NUD 値を受信するホスト



1. 両方のディストリビューション レイヤ スイッチで、ホストへの VLAN インターフェイスに到達可能時間 5000 ミリ秒を設定します。

```
interface Vlan2
 description ACCESS-DATA-2
 ipv6 address 2001:DB8:CAFE:2::A111:1010/64
 ipv6 nd reachable-time 5000
```

新しい到達可能時間が RA を介してそれぞれのインターフェイスから送信されます。

2. ホストはディストリビューション レイヤ スイッチから RA を受信し、ローカルの「到達可能時間」を新しい値に変更します。IPv6 をサポートする Windows ホストでは、次のコマンドを実行すると新しい到達可能時間を表示できます。

```
netsh interface ipv6 show interface [[interface=]<string>]
```

QoS

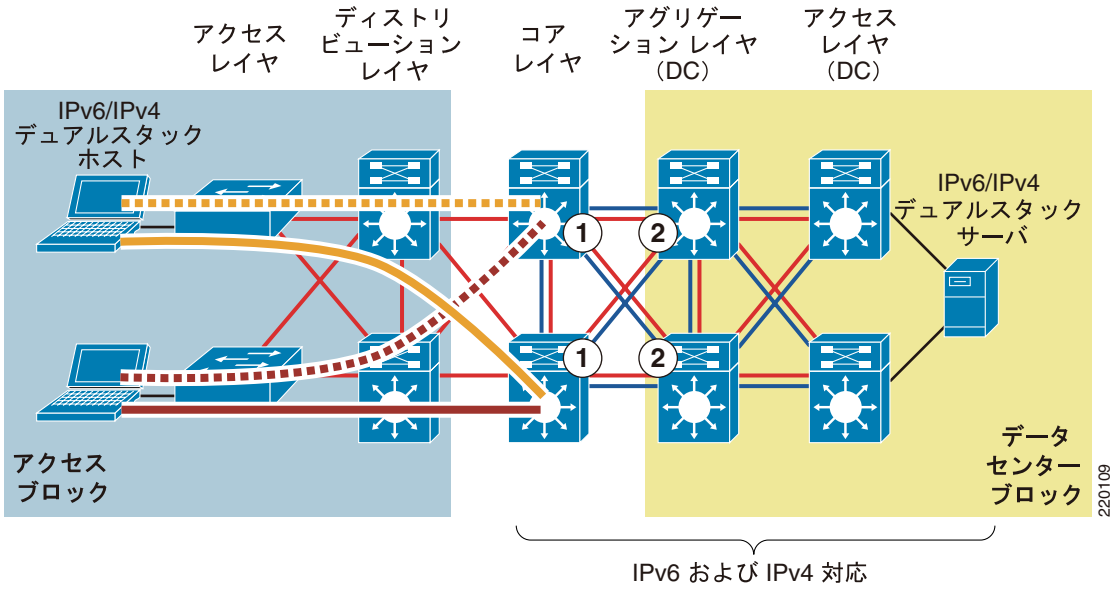
DSM では、既存の IPv4 QoS ポリシーを簡単に拡張し、キャンパス ネットワークで伝送される新しい IPv6 トラフィックを含めることができます。QoS ポリシーはプロトコル依存（IPv4 または IPv6）ではなく、アプリケーション依存および / またはサービス依存になるように実装することを推奨します。既存の QoS ポリシーで、特定のアプリケーションについて固有の分類、ポリシング、およびキューイングを使用している場合は、そのアプリケーション向けの IPv4 トラフィックも IPv6 トラフィックも同じようにポリシーで処理する必要があります。

トンネル トラフィックの QoS ポリシーに関しては、特殊な考慮事項があります。ISATAP トンネル トラフィックの QoS は、少々制限があります。ISATAP トンネルを使用する場合、IPv6 パケットの入力分類は、入トラフィックの信頼または分類を行う場所として推奨されているアクセス レイヤで行うことはできません。HME1 および SBM 設計では、アクセス レイヤに IPv6 サポートがありません。トンネルはアクセス レイヤのホストとコア レイヤ（HME1）または SBM スイッチとの間で使用されるので、入力分類を実行することができません。

トンネル トラフィックの非カプセル化後に、IPv6 の QoS ポリシーを実装することもできますが、この方法にも固有の問題があります。IPv6 トラフィックを非カプセル化するまで入力マーキングを実行できないため、トンネル IPv6 トラフィックは、トンネルの宛先に到達した後でも分類することができません（入力分類およびマーキングは、トンネル インターフェイスではなく物理インターフェイスで実行されます）。非カプセル化され、スイッチによって転送される IPv6 トラフィックには、出力分類ポリシーを実装できます。アップストリーム スイッチに信頼、ポリシング、およびキューイング ポリシーを実装することにより、IPv6 トラフィックを適切に処理できます。

図 9 に、HME1 で ISATAP を使用する場合に IPv6 QoS ポリシーを適用できるポイントを示します。この図のデュアルスタック リンクには、IPv4 と IPv6 の両方に適用される QoS ポリシーがありますが、これらのポリシーはシスコのキャンパス QoS 推奨事項に従っているので省略します。シスコのキャンパス QoS に関する資料については、「その他の関連資料」（p.64）を参照してください。

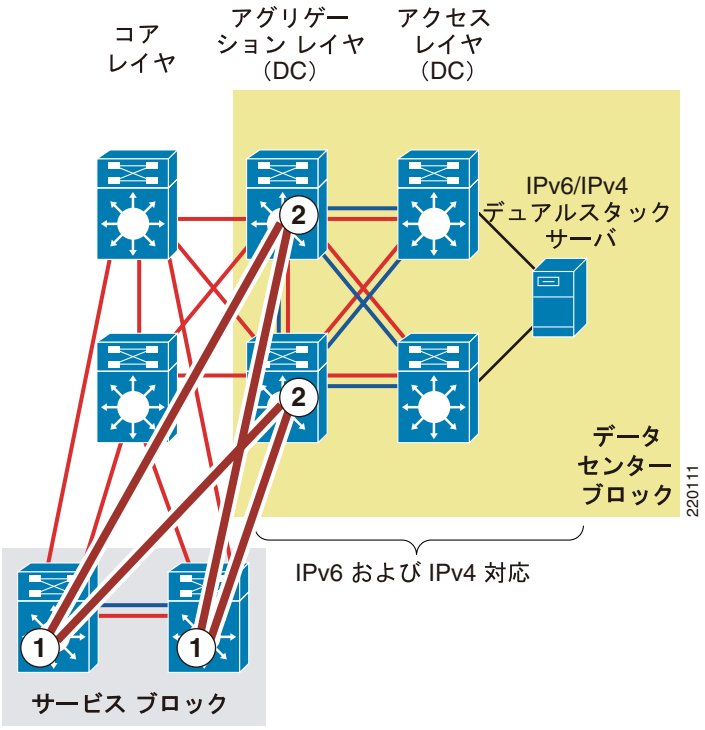
図 9　　QoS ポリシーの実装 — HME1



1. HME1 で分類とマーキングを最初に実装する場所は、コア レイヤ スイッチの出力インターフェイスです。前述したように、アクセス レイヤのホストからコア レイヤまで、IPv6 パケットがトンネリングされます。IPv6 パケットはコア レイヤに達するまで、非カプセル化された「見える」状態ではありません。分類とマーキングのための QoS ポリシーは、ISATAP トンネルの入力側で適用することはできないので、出力側で初めてポリシーを適用します。
2. 分類されマーキングされた IPv6 パケット（上記 1 を参照）が、アップストリーム スイッチ（たとえば、アグリゲーション レイヤ スイッチ）で検証できるようになり、適切な QoS ポリシーを入力側で適用できます。これらのポリシーには、信用（入力）、ポリシング（入力）、およびキューイング（出力）が含まれます。

図 10 に、SBM で ISATAP と手動設定トンネルを使用する場合に、IPv6 QoS ポリシーを適用できるポイントを示します。

図 10　　QoS ポリシーの実装 — SBM（ISATAP および手動設定トンネル）



1. SBM スイッチが ISATAP インターフェイスから着信する IPv6 パケットを受信します。このパケットは非カプセル化されており、手動設定トンネル インターフェイスの出力側で分類およびマーキングのポリシーを適用できます。
2. IPv6 パケットがアグリゲーション レイヤの手動設定トンネル インターフェイスから出ると、アップストリーム スイッチ（アグリゲーション レイヤおよびアクセス レイヤ）で信頼、ポリシング、およびキューイング ポリシーを適用できます。

（注）　このマニュアルの作成時点で、Catalyst 6500 Supervisor 32/720 では、IPv6 パケットに対する出力側でのユーザ単位のマイクロフロー ポリシング機能はサポートされていません。この機能がサポートされるようになった時点で、入力側での分類とマーキングに、ユーザ単位でのマイクロフロー出力ポリシングを、同じスイッチ上で組み合わせることができます。SBM 設計では、このマニュアルのリリース時点で、IPv6 パケットのポリシングは入力側で行う必要があり、入力インターフェイスはトンネルであってはなりません。詳細については、次の URL にある PFC3 QoS ドキュメントを参照してください。
http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/swcg/qos.htm

DSM モデルについては、IPv4 への QoS ポリシーの実装に関する推奨事項が IPv6 にも適用されるので、ここでは示しません。また、HME2 における QoS の考慮事項は図 10 と同じため、ここでは省略します。

Modular QoS CLI（MQC）に関する限り、主な考慮事項は、QoS の「match」および「set」ステートメントから「ip」キーワードを削除することです。IPv6 および IPv4 をサポートするために QoS 構文が変更され、表 5 に示す新しい設定基準を使用できます。

表 5　新しい設定基準

IPv4 のみの QoS 構文	IPv4/IPv6 QoS 構文
match ip dscp	match dscp
match ip precedence	match precedence
set ip dscp	set dscp
set ip precedence	set precedence

IPv6 と IPv4 の両方に使用することができ、CLI に変更を加える必要のない QoS 機能があります（例：WRED、ポリシング、および WRR）。

各モデルの実装セクションでは、特定のアプリケーション用のクラス定義、対応する DSCP 値のマッピング、帯域幅とキューイングに関する推奨事項など、詳しい QoS 設定については説明しません。キャンパスでの QoS 関連の推奨事項は、CCO のほか、Cisco Press の書籍『*End-to-End QoS Network Design*』に詳しく記載されています。

シスコのキャンパス QoS に関する推奨事項および Cisco Press の書籍については、「その他の関連資料」（p.64）を参照してください。

セキュリティ

既存の IPv4 キャンパス ネットワークで起こりがちな脅威や攻撃の多くは、IPv6 にも当てはまります。不正アクセス、スプーフィング、ルーティング攻撃、ウイルス / ワーム、DoS、man-in-the-middle 攻撃などは、IPv4 と IPv6 のどちらにも起こりうる脅威のうちごく一部です。

IPv6 には、IPv4 にはまったく当てはまらない、あるいは IPv4 と同じようには起こらない新しい脅威の可能性が多くあります。IPv6 では、ネイバーおよびルータ アドバタイズメントと検出、ヘッダー、フラグメンテーションなどの取り扱い方法が本質的に違います。このような相違点や可能性をすべて勘案すると、IPv6 のセキュリティに関する説明は総じて非常に複雑なトピックになり、セキュリティに関する詳しい推奨事項は、このマニュアルで扱う範囲を超えています。IPv6 におけるセキュリティの脅威を特定して解決するために、シスコおよび業界全体において、さまざまな取り組みが行われています。このマニュアルでは、キャンパスで解決できるいくつかの問題を指摘するとともに、IPv6 デュアルスタックおよびトンネル トラフィックの保護について基本的な例を示します。

（注）　このマニュアルで示す例は、推奨事項またはガイドラインではなく、読者がキャンパスに IPv6 を導入する際に、自社のセキュリティ ポリシーを入念に分析できるようにすることを目的としています。

すべてのキャンパス モデルに当てはまる、ネットワーク デバイスの保護に関する一般的なセキュリティ ガイドラインは、次のとおりです。

- キャンパス スイッチの適切なアドレス プランニングを通じて、偵察を困難にすること
  - キャンパス ネットワーク デバイス（L2 および L3 スイッチ）のアドレッシングは、入念に計画する必要があります。一般的な推奨事項としては、スイッチの 64 ビット インターフェイス ID が、すべてのデバイスでランダムな値になるようにアドレッシング プランを工夫することです。スイッチの望ましくないインターフェイス ID の例は、VLAN 2 のアドレスが 2001:db8:cafe:2::1/64 で、VLAN 3 のアドレスが 2001:db8:cafe:3::1/64 であるような場合です（ここでの ::1 は、スイッチのインターフェイス ID です）。これではアドレスが簡単に推測できるので、キャンパス インフラストラクチャ デバイスに共通するアドレッシングを攻撃者にすぐに見抜かれてしまいます。別の方法としては、キャンパス内の全デバイスのインターフェイス ID をランダムにします。前出の VLAN 2 および VLAN

3 の例で言うと、VLAN 2 には 2001:db8:cafe:2::a010:f1a1 など、VLAN 3 には 2001:db8:cafe:3::c801:167a などのアドレスを使用します（ここでの「a010:f1a1」は、スイッチの VLAN 2 のインターフェイス ID です）。

アドレッシングに関する上記の考慮事項は、運用上、相応の難しさを伴います。ネットワーク デバイスとアドレッシングの運用管理を容易にするには、インターフェイス ID のランダム化によるセキュリティと、ランダムなアドレスを使用してデバイスの導入と管理を行う能力との間で、適切なバランスを取る必要があります。

- キャンパス スイッチへの管理アクセスの制御
  - モデルごとに、すべてのキャンパス スイッチについて、管理目的でのスイッチ アクセスを保護するための設定があります。スイッチにはいずれも、管理およびルーティング用のループバック インターフェイスが設定されています。ループバック インターフェイスの IPv6 アドレスは、前述したように、推測されやすいインターフェイス ID 値を使用しないアドレッシング アプローチを採用しています。次の例では、インターフェイス ID は「::A111:1010」を使用しています。

```
interface Loopback0
ipv6 address 2001:DB8:CAFE:6507::A111:1010/128
no ipv6 redirects
```

IPv6 による特定のスイッチへのアクセスをさらに厳密に制限するには、ACL を使用し、ループバック インターフェイスを経由する管理インターフェイス（line vty）へのアクセスを許可します。許可するソース ネットワークは、エンタープライズ IPv6 プレフィクスからです。ACL の生成に拡張性を持たせ、広い範囲のネットワーク デバイスに対応できるようにするには、スイッチの特定のインターフェイスにフィルタリングを適用する代わりに、デバイスへの管理アクセスを制御する主な方法として、エンタープライズ プレフィクス全体を許可するように ACL を定義します。次のエンタープライズ サイト（単なる例）で使用している IPv6 プレフィクスは、2001:db8:cafe::/48 です。

```
ipv6 access-list MGMT-IN
remark Permit MGMT only to Loopback0
permit tcp 2001:DB8:CAFE::/48 host 2001:DB8:CAFE:6507::A111:1010
deny ipv6 any any log-input
!
line vty 0 4
session-timeout 3
access-class MGMT-IN-v4 in
password 7 08334D400E1C17
ipv6 access-class MGMT-IN in                    #Apply IPv6 ACL to restrict access
logging synchronous
login local
exec prompt timestamp
transport input ssh                             #Accept access to VTY via SSH
```

  - SNMP（簡易ネットワーク管理プロトコル）の実行に関するセキュリティ要件は、IPv4 と同様です。SNMP が必要な場合、SNMP バージョンを選択したあと、アクセス制御と認証 / 暗号化の方式を選択する必要があります。

このマニュアルで説明するキャンパス モデルでは、SNMPv3（AuthNoPriv）を使用して、データセンターに存在する Cisco NMS サーバのポーリング機能を提供しています。このマニュアルのキャンパス スイッチで使用している SNMPv3 設定の例は次のとおりです。

```
snmp-server contact John Doe - ipv6rocks@cisco.com
snmp-server group IPv6-ADMIN v3 auth write v1default
snmp-server user jdoe IPv6-ADMIN v3 auth md5 cisco1234
```

  - HTTP によるアクセスの制御 — このマニュアルの作成時点では、Cisco Catalyst スイッチは、IPv6 HTTP ACL によるスイッチへのアクセス制御をサポートしていません。IPv4 用に現在「ip http access-class」という ACL を使用しているスイッチでは、IPv6 に対して同

じレベルの保護が与えられないので、このことは非常に重要です。つまり、従来は IPv4 で HTTP/HTTPS によるアクセスを禁止されていたサブネットまたはユーザが、IPv6 を介してスイッチにアクセスできるようになることを意味します。

- IPv6 トラフィック ポリシング ― トラフィック ポリシングは、QoS および / またはセキュリティ機能と考えることができます。アグリゲート ベース、またはユーザ単位マイクロフロー ベースで、トラフィックをポリシングしなければならない場合があります。このマニュアルで説明するキャンパス モデルでは、IPv6 ポリシング（特にユーザ単位マイクロフロー ポリシング）を実装するのに適している場所は、次のとおりです。
  - DSM ― IPv6 トラフィックのユーザ単位マイクロフロー ポリシングは、Catalyst 6500 ディストリビューション レイヤ スイッチの入トラフィックに対して実行されます（理想的）。
  - HME1 ― IPv6 トラフィックのユーザ単位マイクロフロー ポリシングは、Catalyst 6500 データセンター アグリゲーション レイヤ スイッチ（キャンパス アクセス レイヤのホストから）の入トラフィックに対して実行されます。これは理想的というわけではありません。コア レイヤ スイッチで入力マイクロフロー ポリシングを行うのが望ましいのですが、このモデルでは、トンネル インターフェイスには入力ポリシングを適用できないので、その次のレイヤで行う必要があります。
  - HME2 ― IPv6 トラフィックのユーザ単位マイクロフロー ポリシングは、Catalyst 6500 ディストリビューション レイヤ スイッチの入トラフィックに対して実行されます（理想的）。
  - SBM ― IPv6 トラフィックのユーザ単位マイクロフロー ポリシングは、このマニュアルで説明する SBM の例では難しい問題です。SBM では、サービス ブロック スイッチは Catalyst 6500 であり PFC3 カードを搭載しています。PFC3 を搭載した Catalyst 6500 は、ユーザ単位の入力マイクロフロー ポリシングをサポートしていますが、現時点ではユーザ単位の IPv6 出力マイクロフロー ポリシングをサポートしていません。このマニュアルの SBM の例では、IPv6 がサービス ブロック スイッチ上の ISATAP と手動設定トンネル インターフェイスの間を通過します。入力ポリシングは ISATAP トンネルにも、手動設定トンネル インターフェイスにも適用できないので、サービス ブロック内でポリシングを実行するのに適した場所がありません。

  IPv6 ユーザ単位マイクロフロー ポリシングの基本的な実装例を次に示します。この例では、IPv6 トラフィックをマッチし、シスコが推奨する QoS ポリシー設定に基づいて特定の DSCP 値を設定する QoS ポリシーが、ダウンストリーム スイッチに設定されています。次に示すスイッチの設定では、ユーザ単位のフロー ベースで（この例では IPv6 送信元アドレスに基づいて）ポリシングが実行されます。各フローは 5 Mbps にポリシングされ、このプロファイルを超過するとドロップされます。

```
mls qos
!
class-map match-all POLICE-MARK
  match access-group name V6-POLICE-MARK
!
policy-map IPv6-ACCESS
  class POLICE-MARK
     police flow mask src-only 5000000 8000 conform-action transmit exceed-action drop
  class class-default
   set dscp default
!
ipv6 access-list V6-POLICE-MARK
 permit ipv6 any any
!
interface GigabitEthernet3/1
 mls qos trust dscp
 service-policy input IPv6-ACCESS
```

（注） この例は、シスコのキャンパス QoS に関する推奨事項に基づくものではなく、ユーザ単位マイクロフロー ポリシングの設定がどのようなものであるかを具体的に示しているに過ぎません。

マイクロフロー ポリシングに関する詳細は、次の URL を参照してください。

- http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/swcg/qos.htm
- Enterprise QoS SRND — http://www.cisco.com/go/srnd

（注） このマニュアルの作成時点では、Catalyst 6500 Supervisor 32 および 720 は、IPv6 ユーザ単位マイクロフロー ポリシングと、IPv6 マルチキャスト ルーティングの両方を、ハードウェアでイネーブルに設定することができません。スーパーバイザは、ハードウェアでのポリシング、またはハードウェアでの IPv6 マルチキャスト ルーティング / フォワーディングをサポートしていますが、これらを同時にはサポートしません。スイッチに **ipv6 multicast-routing** コマンドがすでに設定されている状態で、IPv6 ユーザ単位マイクロフロー ポリシングのポリシーを適用すると、IPv6 パケットがソフトウェア スイッチングされるというメッセージが表示されます。逆に、スイッチのインターフェイスに IPv6 ユーザ単位マイクロフロー ポリシングのポリシーを適用し、**ipv6 multicast-routing** コマンドをイネーブルにした場合にも、同じメッセージが表示されます（下記参照）。

次に、この警告メッセージの例を示します。

006256: *Aug 31 08:23:22.426 mst: %FM_EARL7-2-IPV6_PORT_QOS_MCAST_FLOWMASK_CONFLICT: IPv6 QoS Micro-flow policing configuration on port GigabitEthernet3/1 conflicts for flowmask with IPv6 multicast hardware forwarding on SVI interface Vlan2, IPv6 traffic on the SVI interface may be switched in software

006257: *Aug 31 08:23:22.430 mst: %FM_EARL7-4-FEAT_QOS_FLOWMASK_CONFLICT: Features configured on interface Vlan2 conflict for flowmask with QoS configuration on switch port GigabitEthernet3/1, traffic may be switched in software

- コントロール プレーン ポリシング（CoPP）— このマニュアルで説明するキャンパス モデルに関しては、CoPP は Catalyst 6500 Supervisor 32/720 にのみ該当します。CoPP は、DoS などの不要トラフィックによる Multiswitch Feature Card（MSFC）リソースへの悪影響を防止することにより、MSFC を保護します。重要なコントロール プレーン / 管理トラフィックが優先されます。PFC3 を搭載した Catalyst 6500 は、IPv6 トラフィックに対する CoPP をサポートしています。CoPP の設定には、さまざまな要因が関係します。具体的なポリシーはケースバイケースで判断するので、導入に関する推奨事項を 1 つにまとめることはできません。

  CoPP に関する詳細は、次の URL を参照してください。
  http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/swcg/dos.htm

- アクセス レイヤからの入トラフィックの制御 — ソース トラフィックに対して許可されるプレフィクスをフィルタリングします。これは一般的にはディストリビューション レイヤ スイッチ（DSM）の VLAN インターフェイスの入力側で実行しますが、HME1 または SBM では ISATAP トンネル インターフェイスの入力側に適用することもできます。ソース プレフィクスに基づく IPv6 トラフィックの制御は、単純なスプーフィングからネットワークを保護するのに役立ちます。

  VLAN で特定の IPv6 プレフィクスだけを許可する、基本的な ACL の例を次に示します。

```
ipv6 access-list VLAN2-v6-INGRESS
remark PERMIT ICMPv6 PACKETS FROM HOSTS WITH PREFIX 2001:DB8:CAFE:2::/64
permit icmp 2001:DB8:CAFE:2::/64 any
remark PERMIT IPv6 PACKETS FROM HOSTS WITH PREFIX 2001:DB8:CAFE:2::64
permit ipv6 2001:DB8:CAFE:2::/64 any
remark PERMIT ALL ICMPv6 PACKETS SOURCED BY HOSTS USING THE LINK-LOCAL PREFIX
permit icmp FE80::/10 any
remark DENY ALL OTHER IPv6 PACKETS AND LOG
```

```
deny ipv6 any any log-input
!
interface Vlan2
 ipv6 traffic-filter VLAN2-v6-INGRESS in
```

（注） Cisco IOS IPv6 ACL には、IPv6 近隣探索のための暗黙的な permit エントリが含まれています。**deny ipv6 any any** を設定すると、この暗黙的な近隣探索エントリが上書きされます。手動で設定した catch-all deny ステートメントをロギング目的で使用する場合、次の 2 つの permit エントリを追加する必要がある点に注意してください。
permit icmp any any nd-na
permit icmp any any nd-ns

上記の VLAN2-v6-INGRESS の例では、近隣探索の必要性に加えて、VLAN2 でのリンク動作に必要なその他の ICMPv6 サービスに対応するために、より寛容なエントリ（**permit icmp FE80::/16 any**）を作成しています。ブロックすべき / ブロックすべきでない各種の ICMPv6 タイプについて具体的に説明した、RFC、草稿、および IPv6 導入資料があります。ICMPv6 パケットのフィルタリングについて説明されている IETF へのリンクおよび Cisco Press の書籍については、「その他の関連資料」（p.64）を参照してください。

- Microsoft Teredo の使用禁止 — Teredo は、Network Address Translation（NAT; ネットワーク アドレス変換）ゲートウェイの後ろ側に存在するホストに IPv6 サポートを提供します。Teredo が引き起こす、いくつかのセキュリティ上の脅威については、十分に理解する必要があります。キャンパス ネットワークにおける Teredo に関する適切なセキュリティ推奨事項が定義されるまでは、Microsoft Windows XP SP2 および Vista では Tredo をディセーブルに設定してください。さらなる予防策として、Teredo によるキャンパス ネットワーク外部でのトンネルの確立を防止するために、UDP ポート 3544 をブロックする ACL を設定することを検討してください（この設定は、アクセス レイヤまたはそのアップストリーム、たとえば境界ルータなどで行うことができます）。Teredo に関する情報は、次の URL を参照してください。
  - http://www.microsoft.com/technet/prodtechnol/winxppro/maintain/teredo.mspx
  - http://www.microsoft.com/technet/community/columns/cableguy/cg1005.mspx#EVF

  IPv6 セキュリティに関するその他の情報は、「その他の関連資料」（p.64）を参照してください。

マルチキャスト

IPv6 マルチキャストは、すべてのエンタープライズ ネットワーク設計の重要なサービスであり、IPv6 におけるマルチキャストの要件によっては、このマニュアルで説明するモデルについて再考する必要が生じる場合があります。IPv6 マルチキャストと各種モデルについて理解しておくべき最も重要な問題は、ISATAP 上では IPv6 マルチキャストがサポートされない点です。これは機器またはソフトウェアの制約ではなく、ISATAP トンネリング メカニズムの欠点です（RFC4214）。

IPv6 マルチキャストの導入で考慮すべき最も重要な要因の 1 つは、ホスト / グループの制御をアクセス レイヤで適切に処理することです。IPv6 における Multicast Listener Discovery（MLD）は、IPv4 における Internet Group Management Protocol（IGMP; インターネット グループ管理プロトコル）に相当します。どちらもマルチキャスト グループ メンバーシップの制御に使用されます。MLD スヌーピングは、レイヤ 2 スイッチがマルチキャスト トラフィックの配信を、リスナーのあるポートだけに制限するための機能です。この機能がなければ、1 つのレシーバー（またはレシーバーのグループ）だけを対象とするマルチキャスト トラフィックが、アクセス レイヤ スイッチのすべてのポートにフラッディングされることになります。アクセス レイヤでは、スイッチが MLD バージョン 1 および / またはバージョン 2 に対応する MLD スヌーピングをサポートしていることが重要です（これはアクセス レイヤでデュアルスタックを実行する場合にのみ適用されます）。

（注） このマニュアルの作成時点では、MLDv2 のホスト実装例が非常に少数でした。MLDv2 はさまざまな Linux および BSD 実装でサポートされており、Microsoft Windows Vista でもサポートされています。PIM-SSM ベースの構成では、MLDv2 が重要です。MLDv2 と PIM-SSM の併用は、様々な IPv6 マルチキャスト構成向けの優れた組み合わせです。まだ MLDv2 をサポートしていないホストもあります。Cisco IOS では、PIM-SSM で使用するために MLDv1 レポートを MLDv2 レポートにマッピングする、SSM マッピングという機能を提供しています。詳細については、次の URL を参照してください。
http://www.cisco.com/en/US/partner/products/ps6350/products_configuration_guide_chapter09186a00801d6618.html#wp1290106

このマニュアルでは、IPv6 マルチキャスト対応のアプリケーションは、DSM および HME2 モデルでのみサポートされます。どちらのモデルでも、ISATAP 設定を使用していないからです。この設計で動作確認済みのマルチキャスト対応アプリケーションは、Embedded-RP および PIM-SSM グループを使用する Windows Media Services および VideoLAN Media Client（VLC）です。マルチキャスト送信元は、データセンター アクセス レイヤの Microsoft Windows Server 2003、Longhorn、および Red Hat 4.0 サーバで稼働しています。

CCO および業界のいくつかのドキュメントで、IPv6 マルチキャストについて詳しく解説されています。このマニュアルでは、IPv6 マルチキャストをイネーブルにするコマンドと、Embedded-RP 定義の要件についての一般的な説明を除いて、設定に関する注意事項は記載していません。詳細については、次の URL にあるシスコの IPv6 マルチキャストに関する Web ページを参照してください。
http://www.cisco.com/en/US/products/ps6594/products_ios_protocol_group_home.html

管理

IPv6 の管理ツールと計測機能は現在開発中であり、完成までに長い期間を要します。従来使用されてきた管理ツールの多くは、IPv6 にも対応します。このマニュアルでは、キャンパス ネットワークの管理については、基本的な管理サービス（Telnet、SSH、および SNMP）についてのみ考慮します。説明されている各種キャンパス モデル内の IPv6 対応デバイスはすべて、SNMP を除く上記サービスにより、IPv6 を介して管理することができます。このマニュアルの作成時点では、説明されている Catalyst スイッチは、IPv6 トランスポート上の SNMP をまだサポートしていません。ただし、IPv6 固有の MIB/ トラップ / 情報の管理は、Catalyst プラットフォームで IPv4 トランスポート上の SNMP を使用することによりサポートされます。

管理において綿密な調査が必要とされるもう 1 つの分野は、アドレス管理です。IPv6 について初歩的なレベルで分析しただけでも、IPv6 アドレス構造の導入と管理が、大規模かつ複雑になる可能性があることがわかります。多数のネットワーク デバイスを対象とする大規模な 16 進アドレスの導入は、いずれかの段階で自動化するか、少なくとも現在よりもユーザフレンドリーにする必要があります。アドレス管理の問題については、業界でも推奨事項とソリューションを提供するための努力が続けられています。シスコは、このような活動の最前線に位置しています。

現時点で、キャンパス スイッチへのアドレス プレフィクスの導入に役立つ方法の 1 つは、「汎用プレフィクス」機能を使用することです。汎用プレフィクス機能を使用すると、スイッチのグローバル コンフィギュレーションで、ユーザフレンドリーな名前を使用してプレフィクスを定義することができます。インターフェイス単位でユーザフレンドリーな名前を使用し、インターフェイスの通常の IPv6 プレフィクス定義の代わりとすることができます。汎用プレフィクス機能の使用例を次に示します。

- 汎用プレフィクスの定義：

```
6k-agg-1(config)#ipv6 general-prefix ESE-DC-1 2001:DB8:CAFE::/48
```

- インターフェイス単位で汎用プレフィクスを「ESE-DC-1」と言う名前で設定：

```
6k-agg-1(config-if)#ipv6 address ESE-DC-1 ::10:0:0:F1A1:6500/64
```

- 汎用プレフィクスがインターフェイスに正しく割り当てられたかどうかを確認：

```
6k-agg-1#show ipv6 interface vlan 10
Vlan10 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::211:BCFF:FEC0:C800
  Description: VLAN-SERVERFARM-WEB
  Global unicast address(es):
    2001:DB8:CAFE:10::F1A1:6500, subnet is 2001:DB8:CAFE:10::/64
```

（注） 汎用プレフィクス機能は、汎用プレフィクスの値を変更すれば、迅速にルータ番号の付け替えを実行できるため、番号の付け替えが必要とされる場合に役立ちます。

汎用プレフィクス機能の詳細については、Cisco IOS IPv6 マニュアル ページ（「その他の関連資料」[p.64]）を参照してください。

シスコはさまざまなネットワーク管理製品（DNS、DHCPv6、デバイス管理、モニタリング、ネットワーク管理、トラブルシューティング、およびレポート）で、IPv6 対応ネットワーク デバイスの管理をサポートしています。各種のシスコ ネットワーク管理ソリューションについての詳細は、次の URL を参照してください。
http://www.cisco.com/en/US/products/sw/netmgtsw/index.html

スケーラビリティとパフォーマンス

このマニュアルは、テスト対象の各種プラットフォームに関するスケーラビリティおよびパフォーマンス情報の分析を目的とはしていません。キャンパスにおける IPv6 のプランニングと導入では、スケールとパフォーマンスに関して、プラットフォーム別の観点ではなく、一般的な考慮事項を中心とします。

読者は既存のキャンパス ネットワークのリンク、メモリ、および CPU 利用率を全般的に把握している必要があります。これらのうち一つでもすでに逼迫しているものがある場合、IPv6 などの新しいテクノロジー、機能、またはプロトコルを設計に追加すると、惨事を招きかねません。ただし、IPv6 を実装した結果、キャンパス ネットワーク リンクでのトラフィック利用率が変化するのは珍しいことではありません。IPv6 の導入によって、従来 IPv4 のみだったアプリケーション トランスポートのユーザが IPv6 を利用するようになり、IPv4 トラフィックの利用率が減少するケースが非常に多く見られます。ルーティングのために通常発生する制御トラフィックと、ISATAP または手動設定トンネルを使用する場合はトンネル オーバーヘッドによって、ネットワーク全体の利用率が増加します。

DSM におけるスケーラビリティとパフォーマンスに関する考慮事項は次のとおりです。

- ルーテッド アクセス設計（アクセス レイヤ）— スケーラビリティに関する主な考慮事項の 1 つは、アクセス（ルーテッド アクセス）またはディストリビューション レイヤ スイッチで 2 つのプロトコルを実行することです。ルーテッド アクセスまたはディストリビューション レイヤで、スイッチは IPv4 と IPv6 の両方のネイバー情報を追跡しなければなりません。IPv4 での Address Resolution Protocol（ARP; アドレス解決プロトコル）と同様に、IPv6 にはネイバー キャッシュが存在します。ここで特に考慮しなければならないのは、IPv4 の場合、通常 IPv4 アドレスと MAC アドレスの間に 1 対 1 のマッピングがあるのに対し、IPv6 の場合、ホストが使用する複数の IPv6 アドレス（たとえば、リンクローカル、ユニークローカル、および複数のグローバル アドレス）と、スイッチのネイバー キャッシュ内の 1 つの MAC アドレスとの間で、複数のマッピングが存在する場合がある点です。次に、ディストリビューション レイヤの Catalyst 6500 上で、MAC アドレス「000d.6084.2c7a」のホストに対応する ARP エントリおよびネイバー キャッシュ エントリの例を示します。

  ディストリビューション レイヤのホストに対応する ARP エントリ：

```
Internet  10.120.2.200           2   000d.6084.2c7a  ARPA   Vlan2
```

  IPv6 ネイバー キャッシュ エントリ：

```
2001:DB8:CAFE:2:2891:1C0C:F52A:9DF1          4 000d.6084.2c7a  STALE Vl2
2001:DB8:CAFE:2:7DE5:E2B0:D4DF:97EC         16 000d.6084.2c7a  STALE Vl2
FE80::7DE5:E2B0:D4DF:97EC                   16 000d.6084.2c7a  STALE Vl2
```

ネイバー キャッシュを見ると、このホストに対応する 3 つのエントリがリストされています。最初のアドレスは、割り当てられている 2 つのグローバル IPv6 アドレスの 1 つ（オプション）であり、グローバル IPv6 アドレスが IPv6 プライバシ拡張機能によって生成されたことを反映しています。2 番めのアドレスは、ステートレスな自動設定によって割り当てられたもう 1 つのグローバル IPv6 アドレス（オプション）です（このアドレスは DHCPv6 によって静的に定義または割り当てられる場合もあります）。そして 3 番めのアドレスは、ホストが生成したリンクローカル アドレス（必須）です。ホストで使用するアドレス タイプに応じて、1 つのホストに対応するエントリ数は、最低 1（リンクローカル アドレス）から非常に多数になる場合があります。

ルーテッド アクセスおよびディストリビューション レイヤで使用するプラットフォームのネイバー テーブル機能を検証し、これらのテーブルが通常のネットワーク動作中に満杯にならないようにすることが非常に重要です。エントリを早期にタイムアウトさせるためのタイマーの調節、ネイバー アドバタイズメントのレート制限、IPv6 近隣探索ベースの攻撃による DoS からのアクセス レイヤ スイッチの保護などについて、推奨事項を決定するために、さらにテストを実施する予定です。

IPv6 マルチキャストについての考慮事項がもう 1 つあります。前述したように、IPv6 マルチキャストを使用する場合は、レイヤ 2 で IPv6 マルチキャスト フレームがすべてのポートにフラッディングされないようにするため、アクセス レイヤで MLD スヌーピングのサポートを確保することが重要です。

- ディストリビューション レイヤ — 上記の ARP/ ネイバー キャッシュの問題に加えて、DSM のディストリビューション レイヤ スイッチについては、次の 2 つの考慮事項があります。
  - IPv6 ルーティングおよびフォワーディングは、ハードウェアで実行する必要があります。
  - ACL エントリの処理をハードウェアで実行することは必須です。ディストリビューション レイヤにおける IPv6 ACL の主な使用目的は、QoS（アクセス レイヤからの入力パケットの分類とマーキング）、セキュリティ（アクセス レイヤの入力トラフィックに対する DoS、スヌーピング、および不正アクセスの抑制）、および QoS とセキュリティの組み合わせによる、スイッチのコントロール プレーンに対する攻撃からの保護です。
- コア レイヤ — スケーラビリティとパフォーマンスに関する考慮事項は、ディストリビューション レイヤと同様です。

HME1 におけるスケーラビリティとパフォーマンスに関する考慮事項は次のとおりです。

- アクセス レイヤ — HME1 を使用する場合、アクセス レイヤに関してスケーラビリティとパフォーマンスの考慮事項は特にありません。HME1 ではアクセス レイヤが IPv6 をサポートしないので、説明すべき事項はほとんどありません。リンク上のトラフィック量（トンネリングされた IPv6 トラフィック）が増える可能性があるので、考慮すべき唯一の問題はリンク利用率です。ただし前述したように、IPv6 を導入した結果、ユーザが従来 IPv4 のみだったアプリケーションに IPv6 を使用するようになり、リンク利用率が IPv4 から IPv6 に移る可能性があります。
- ディストリビューション レイヤ — 考慮事項はアクセス レイヤと同様です。
- コア レイヤ — HME1 を使用する場合、コア レイヤ スイッチへの影響が予測されます。HME1 では、何百もの ISATAP トンネルがコア レイヤ スイッチで終端する可能性があります。既存のコア レイヤ スイッチで、設計上必要とされるトンネル数に対応できるかどうかを、パートナーおよびシスコのアカウント チームとともに検証する必要があります。アクセス レイヤから着信するトンネル数をコア レイヤ スイッチがサポートできそうもない場合には、DSM に移行するか、または HME1 の代わりに SBM を使用して、DSM がサポートされるまで、トンネル終端および管理に専用のスイッチを使用することを検討しなければなりません。コア レイヤに関するスケーラビリティとパフォーマンスの重要な要素は、次の 3 つです。

- ISATAP トンネル インターフェイスの管理によるコントロール プレーンへの影響。VLAN 数と ISATAP トンネル数の間に 1 対 1 のマッピングが存在する場合は、これが問題になる可能性があります。大規模なネットワークでは、このマッピングによって、膨大な数のトンネルを CPU が追跡しなければなりません。仮想インターフェイスのコントロール プレーン管理は、CPU が処理します。
- ISATAP トンネル関連のプレフィクスに起因する、ルート テーブルの管理によるコントロール プレーンへの影響。
- リンク利用率 — ディストリビューション レイヤ（トンネル トラフィック）からのリンク利用率の増加と、コア レイヤからデータセンターのアグリゲーション レイヤへのリンクに IPv6（デュアルスタック）を追加することによるリンク利用率の増加が考えられます。

HME2 におけるスケーラビリティとパフォーマンスに関する考慮事項は次のとおりです。

- アクセス レイヤ — 考慮事項は、DSM のアクセス レイヤと同様です。
- ディストリビューション レイヤ — HME2 では、アクセス レイヤにはデュアルスタックを使用し、コアの伝送とデータセンター アグリゲーション レイヤでの終端には、手動設定トンネルを使用します。アクセス レイヤに関するスケーラビリティとパフォーマンスの考慮事項は、DSM のディストリビューション レイヤと同様です。手動設定トンネルに関する考慮事項は、HME1 のコア レイヤの場合と同様です。ただし、トンネルが存在するのは、ディストリビューション ペアと、データセンターの各アグリゲーション レイヤ スイッチの間だけです。状況によっては、ディストリビューション スイッチごとに 2 つという、少ないトンネル数になる場合もあります。また、何百ものトンネルが存在する場合があります。いずれにせよ、使用する Catalyst プラットフォームが IPv6 トンネリングをハードウェアでサポートしていれば、何百のトンネルがあっても、パフォーマンスまたはスケーラビリティの問題が生じることはありません。
- コア レイヤ — HME2 の場合、コア レイヤは IPv4 だけなので、スケーラビリティまたはパフォーマンスに関して特筆すべき点はありません。

SBM におけるスケーラビリティとパフォーマンスに関する考慮事項は次のとおりです。

- アクセス レイヤ — SBM の場合、アクセス レイヤは IPv4 だけなので、スケールまたはパフォーマンスに関して特に考慮すべき点はありません。
- ディストリビューション レイヤ — SBM の場合、ディストリビューション レイヤは IPv4 だけなので、スケールまたはパフォーマンスに関して特に考慮すべき点はありません。
- コア レイヤ — SBM の場合、コア レイヤは IPv4 だけなので、スケールまたはパフォーマンスに関して特に考慮すべき点はありません。
- サービス ブロック — HME1 のコア レイヤに見られる考慮事項の多くが、サービス ブロック スイッチに当てはまります。唯一の相違点は、サービス ブロックは ISATAP トンネルと手動設定トンネルの両方を同じスイッチ ペアで終端することです。SBM の利点は、スイッチ ペアがトンネル終端のみに使用され、トンネルが増えた場合にはサービス ブロックにスイッチを追加して対応できるため、大規模なトンネルベースの構成が可能になる点です。スイッチの増設によるスケールの拡大は、コア レイヤ（HME1）では困難です。各種のネットワーク ブロック（アクセス、データセンター、WAN など）を接続するという、コアの中心的な役割があるからです。

デュアルスタック モデル — 実装

ここでは、DSM の設定について説明します。設定は、VLAN、ルーティング、HA など、特定の分野ごとに行います。VLAN、物理インターフェイスなど、多くの設定は IPv6 特有ではありません。DSM における VLAN の設定は、IPv4 と IPv6 で共通ですが、完全を期するために両方とも示しています。設定例は、2 つのスイッチ（通常、同じレイヤ内のペア、または相互に接続するペ

ア）についてのみ、そのセクションで説明する部分（例：ルーティング、HA など）に限って掲載します。キャンパス ネットワーク内の各スイッチの設定全体の内容は、「付録 — 設定リスト」（p.66）を参照してください。

各セクションで説明するコマンドは、すべて**大文字**で示します。

ネットワーク トポロジ

次に、すべての DSM 設定例の基準としている図を示します。図 11 は、この DSM で使用する物理ポートのレイアウトを示しています。

図 11　　DSM ネットワーク トポロジ — 物理ポート

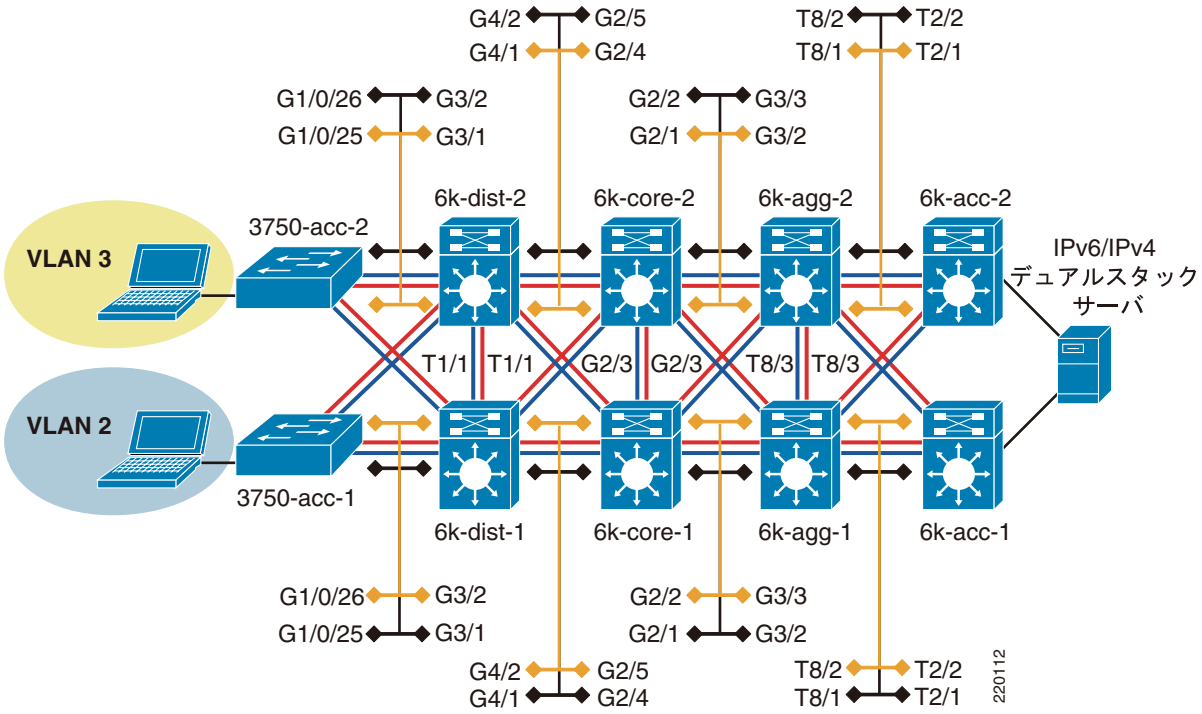
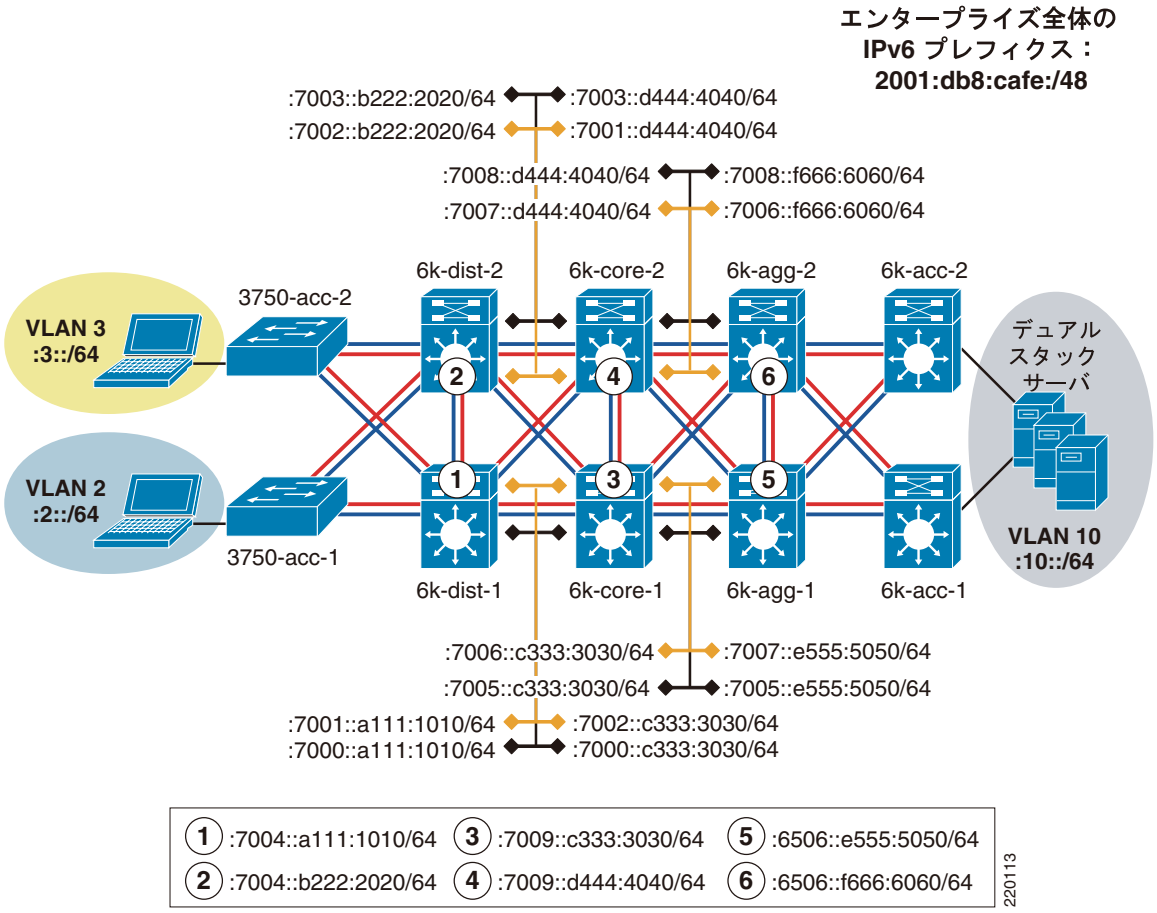


図 12 に、この DSM 環境の IPv6 アドレッシング プランを示します。図を見やすくするために、ネットワークの /48 プレフィクス部分を削除しています。このマニュアルで説明するすべてのモデルで使用している IPv6 /48 プレフィクスは、「2001:db8:cafe::/48」です。

図 12　DSM ネットワーク トポロジ — IPv6 アドレッシング



物理インターフェイスに加えて、ループバック インターフェイスおよび VLAN インターフェイスにも IPv6 アドレスが割り当てられています。表 6 に、スイッチ、インターフェイス、およびインターフェイスの IPv6 アドレスを示します。

表 6　スイッチ、インターフェイス、および IPv6 アドレス

スイッチ	インターフェイス	IPv6 アドレス
3750-acc-1	VLAN2	2001:db8:cafe:2::cac1:3750/64
3750-acc-2	VLAN3	2001:db8:cafe:3::cac2:3750/64
6k-dist-1	Loopback0	2001:db8:cafe:6507::a111:1010/128
	VLAN2	2001:db8:cafe:2::a111:1010/64
	VLAN3	2001:db8:cafe:3::a111:1010/64
6k-dist-2	Loopback0	2001:db8:cafe:6507::b222:2020/128
	VLAN2	2001:db8:cafe:2::b222:2020/64
	VLAN3	2001:db8:cafe:3::b222:2020/64
6k-core-1	Loopback0	2001:db8:cafe:6507::c333:3030/128
6k-core-2	Loopback0	2001:db8:cafe:6507::d444:4040/128
6k-agg-1	Loopback0	2001:db8:cafe:6507::e555:5050/128

表 6　スイッチ、インターフェイス、および IPv6 アドレス（続き）

スイッチ	インターフェイス	IPv6 アドレス
	VLAN10	2001:db8:cafe:10::e555:5050/64
6k-agg-2	Loopback0	2001:db8:cafe:6507::f666:6060/128
	VLAN10	2001:db8:cafe:10::f666:6060/64
6k-acc-1	VLAN10	2001:db8:cafe:10::dca1:6506/64
6k-acc-2	VLAN10	2001:db8:cafe:10::dca2:6506/64

物理 /VLAN の設定

物理 p2p リンクの設定は、IPv4 の場合とほぼ同様です。次の例は、6k-dist-1 と 6k-core-1 の間のリンクに関する p2p インターフェイスの設定です。

- 6k-dist-1:

```
ipv6 unicast-routing                    #Globally enable IPv6 unicast routing
ip cef distributed                      #Ensure IP CEF is enabled (req. for
                                        #IPv6 CEF to run).
ipv6 cef distributed                    #Globally enable IPv6 CEF.
!
interface GigabitEthernet4/1
 description to 6k-core-1
 dampening
 load-interval 30
 carrier-delay msec 0
 ipv6 address 2001:DB8:CAFE:7000::A111:1010/64     #Assign IPv6 address
 no ipv6 redirects                                 #Disable IPv6 redirects
 ipv6 nd suppress-ra                               #Disable RAs on this interface
 ipv6 cef                                          #Enable IPv6 CEF for this intf.
```

- 6k-core-1:

```
ipv6 unicast-routing
ip cef distributed
ipv6 cef distributed
!
interface GigabitEthernet2/4
 description to 6k-dist-1
 dampening
 load-interval 30
 carrier-delay msec 0
 ipv6 address 2001:DB8:CAFE:7000::C333:3030/64
 no ipv6 redirects
 ipv6 nd suppress-ra
 ipv6 cef
```

必須ではありませんが、p2p リンクでは RA の送信をディセーブルにしておくとよいでしょう。静的に定義される p2p リンクでは、RA は不要です。また、プラットフォームとコード バージョンによっては、**ipv6 cef** をインターフェイスごとにイネーブルにしなくてもよい場合がある点に注意してください。この例では、インターフェイス上で IPv6 CEF を確実にイネーブルにするための安全策として、このコマンドを使用しています。ただし、新しいコード バージョンでは、IPv6 ユニキャスト ルーティングがグローバルにイネーブル化され、インターフェイス上で IPv6 がイネーブルであれば、自動的にこの処理が実行されます。

Catalyst 3750 および 3560 スイッチでは、Ternary Content Addressable Memory（TCAM; Ternary CAM）を別の目的に使用できるようにするために、適切な Switch Database Management（SDM）テンプレートをイネーブルにする必要があります。3750-acc-1 および 3750-acc-2 では、**sdm prefer dual-ipv4-and-ipv6 default** コマンドを使用して、「dual-ipv4-and-ipv6」SDM テンプレートを設定し

ています。**sdm prefer** コマンドと関連するテンプレートについての詳細は、次の URL を参照してください。
http://www.cisco.com/univercd/cc/td/doc/product/lan/cat3750/12225see/scg/swsdm.htm#

アクセス レイヤはスイッチごとに 1 つの VLAN を使用しています。音声 VLAN については説明しません。これらの VLAN は複数のアクセス レイヤ スイッチにまたがることはなく、ディストリビューション レイヤで終端されています。次の例は、3750-acc-1 および 6k-dist-1 の VLAN2 設定です。

- 3750-acc-1:

```
vtp domain ese-dc
vtp mode transparent
!                                                  #VTP and STP configurations
!                                                  #shown for completeness, but not
!                                                  #specific to IPv6
spanning-tree mode rapid-pvst
spanning-tree loopguard default
spanning-tree portfast bpduguard default
no spanning-tree optimize bpdu transmission
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
vlan 2                                                 #VLAN2 - Data VLAN for 3750-acc-1
 name ACCESS-DATA-2
!
interface GigabitEthernet1/0/25                        #Physical intf. to 6k-dist-1
 description TRUNK TO 6k-dist-1
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 2
 switchport mode trunk
 switchport nonegotiate
 load-interval 30
!
interface Vlan2                                    #VLAN2 with IPv6 address used for mgmt.
 ipv6 address 2001:DB8:CAFE:2::CAC1:3750/64
 no ipv6 redirects
```

- 6k-dist-1:

```
vtp domain ese-dc
vtp mode transparent
!
spanning-tree mode rapid-pvst
spanning-tree loopguard default
no spanning-tree optimize bpdu transmission
spanning-tree extend system-id
spanning-tree vlan 2-3 priority 24576                  #6k-dist-1 is the STP root for
                                                       #VLAN2,3
!
vlan internal allocation policy descending
vlan dot1q tag native
vlan access-log ratelimit 2000
!
vlan 2                                                 #VLAN2 defined for 3750-acc-1
 name ACCESS-DATA-2
!
vlan 3                                                 #VLAN3 defined for 3750-acc-2
 name ACCESS-DATA-3
!
interface GigabitEthernet3/1                           #Physical intf. to 3750-acc-1
 description to 3750-acc-1
 switchport
 switchport trunk encapsulation dot1q
```

```
 switchport trunk allowed vlan 2
 switchport mode trunk
 switchport nonegotiate
 no ip address
 load-interval 30
 spanning-tree guard root
!
interface Vlan2                                    #VLAN2 intf is VLAN termination
                                                   #point for trunked VLAN from 3750-acc-1
 description ACCESS-DATA-2
 ipv6 address 2001:DB8:CAFE:2::A111:1010/64        #IPv6 address and prefix used for
                                                   #Stateless autoconfiguration for VLAN2
 no ipv6 redirects
```

ここで説明するモデルはいずれもスタックを使用していませんが、アクセス レイヤの Catalyst 3750 および 3560 ではスタックがよく使用されます。スイッチ スタックを使用する場合、IPv6 は IPv4 とほぼ同様にサポートされます。スイッチ スタックを使用する場合の IPv6 についての詳細は、次の URL を参照してください。
http://www.cisco.com/univercd/cc/td/doc/product/lan/cat3750/12225see/scg/swipv6.htm#wp1090623

ルーティングの設定

前述したように、DSM でのルーティングは、EIGRP for IPv4 および OSPFv3 for IPv6 を使用して設定します。OSPFv3 の設定は、シスコが推奨するキャンパス設計に可能な限り従っています。OSPFv2 で使用可能な機能で、OSPFv3 に統合中のものがあります。主に高速コンバージェンスと認証を目的とする機能です。6k-dist-1 および 6k-core-1 スイッチでの OSPFv3 の設定を示します。

- 6k-dist-1:

```
interface Loopback0
ip address 10.122.10.9 255.255.255.255                  #Address used for RID on OSPFv3
ipv6 address 2001:DB8:CAFE:6507::A111:1010/128
ipv6 ospf 1 area 0                                      #Part of area 0
!
interface TenGigabitEthernet1/1
 description to 6k-dist-2
 ipv6 address 2001:DB8:CAFE:7004::A111:1010/64
 ipv6 cef
 ipv6 ospf network point-to-point          #Defining network type as p2p
 ipv6 ospf hello-interval 1                #Lower hello/dead intervals as a fail-safe
                                           #for lower convergence times. p2p links do
                                           #not use hello/dead as the primary
                                           #detector of link/node failures.
 ipv6 ospf dead-interval 3
 ipv6 ospf 1 area 2
!
interface GigabitEthernet4/1
 description to 6k-core-1
 ipv6 address 2001:DB8:CAFE:7000::A111:1010/64
 ipv6 cef
 ipv6 ospf network point-to-point
 ipv6 ospf hello-interval 1
 ipv6 ospf dead-interval 3
 ipv6 ospf 1 area 0
!
interface GigabitEthernet4/2
 description to 6k-core-2
 ipv6 address 2001:DB8:CAFE:7001::A111:1010/64
 ipv6 cef
 ipv6 ospf network point-to-point
 ipv6 ospf hello-interval 1
 ipv6 ospf dead-interval 3
```

```
 ipv6 ospf 1 area 0
!
interface Vlan2
 description ACCESS-DATA-2
 ipv6 address 2001:DB8:CAFE:2::1/64 anycast        #One way to provide gateway
                                                   #redundancy for the mgmt interface
                                                   #on the 3750-dist-1. This anycast
                                                   #address is used on both
                                                   #distribution layer switches
 ipv6 address 2001:DB8:CAFE:2::A111:1010/64
 ipv6 nd reachable-time 5000                  #Lower the NUD-reachable time to provide
                                              #basic first-hop redundancy for the hosts
                                              #in VLAN2. This command is used on both
                                              #distribution layer switches' VLAN
                                              #interfaces.
 ipv6 cef
 ipv6 ospf 1 area 2                           #Per the campus best practices - Access
                                              #VLAN is not in area 0
!
ipv6 router ospf 1
 router-id 10.122.10.9                          #RID using Loopback0
 log-adjacency-changes
 auto-cost reference-bandwidth 10000
 area 2 range 2001:DB8:CAFE:2::/64 cost 10      #Summarize the /64 prefix for
                                                #VLAN2/3 into area 0
 area 2 range 2001:DB8:CAFE:3::/64 cost 10
 passive-interface Vlan2                        #Do not establish adjacency over
                                                #VLAN2/3 with 6k-dist-2
 passive-interface Vlan3
 passive-interface Loopback0
 timers spf 1 5                             #Lower the SPF throttling timer for
                                            #convergence time improvement. In campus
                                            #networks these values have been tested as
                                            #low as 1 and 1 without issue. Adjusting
                                            #these values should be well understood
                                            #and consistent #between all switches in
                                            #the campus
```

- 6k-core-1:

```
interface Loopback0
 ip address 10.122.10.3 255.255.255.255
 ipv6 address 2001:DB8:CAFE:6507::C333:3030/128
 ipv6 ospf 1 area 0
!
interface GigabitEthernet2/1
 description to 6k-agg-1
 ipv6 address 2001:DB8:CAFE:7005::C333:3030/64
 ipv6 cef
 ipv6 ospf network point-to-point
 ipv6 ospf hello-interval 1
 ipv6 ospf dead-interval 3
 ipv6 ospf 1 area 0
!
interface GigabitEthernet2/4
 description to 6k-dist-1
 ipv6 address 2001:DB8:CAFE:7000::C333:3030/64
 ipv6 cef
 ipv6 ospf network point-to-point
 ipv6 ospf hello-interval 1
 ipv6 ospf dead-interval 3
 ipv6 ospf 1 area 0
!
ipv6 router ospf 1
```

```
router-id 10.122.10.3
log-adjacency-changes
auto-cost reference-bandwidth 10000
passive-interface Loopback0
timers spf 1 5
```

各種の IGP タイマーを変更する場合の影響について理解しておくことが重要です。キャンパス ネットワークは、できるだけ速くコンバージするように設計する必要があります。また、キャンパス ネットワークは、ブランチまたは WAN 環境と比べて、より厳密にチューニングした IGP タイマーで動作できます。このルーティング設定例は、シスコのキャンパスに関する推奨事項に基づいています。実際のネットワークに導入する前に、各コマンドのコンテキストと、タイマー値の選択について理解しておく必要があります。シスコのキャンパス設計に関するベスト プラクティス ドキュメントについては、「その他の関連資料」（p.64）を参照してください。

ハイ アベイラビリティの設定

DSM における HA 設計の要素は、各スイッチ（ディストリビューション、コア、およびデータセンター アグリゲーション レイヤに適用）を 2 つずつ稼働させることと、IPv4 および IPv6 ルーティング設定をチューニングし完全にフォールトトレラントにすることです。このモデルが必要な場合は、シングルシャーシ、デュアルスーパーバイザを導入し実行した場合の影響について確認する必要があります。Non-Stop Forwarding（NSF）、Stateful Switchover（SSO）など、一部の HA 機能では、Catalyst プラットフォームにおける IPv6 がサポートされていない場合があります。検討中のプラットフォームとソフトウェアで、NSF/SSO と IPv6 を併用できるかどうかを確認してください。

QoS の設定

DSM における QoS の設定は、IPv4 の場合と同様です。分類、マーキング、キューイング、およびポリシングのためのポリシーは、カスタマー サービスの要件によって大きく異なります。キューイングのタイプおよびサポートされるキュー数も、プラットフォーム、またはラインカードによって異なります。6k-dist-1 での基本的な設定を示しますが、これはあくまで参考用です。簡潔にするため、一部のインターフェイスを省略しています。

- 6k-dist-1

```
mls qos
!
interface TenGigabitEthernet1/1
 description to 6k-dist-2
 wrr-queue bandwidth 5 25 70
 wrr-queue queue-limit 5 25 40
 wrr-queue random-detect min-threshold 1 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 3 50 60 70 80 90 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 2 100 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 3 60 70 80 90 100 100 100 100
 wrr-queue cos-map 1 1 1
 wrr-queue cos-map 2 1 0
 wrr-queue cos-map 3 1 4
 wrr-queue cos-map 3 2 2
 wrr-queue cos-map 3 3 3
 wrr-queue cos-map 3 4 6
 wrr-queue cos-map 3 5 7
 mls qos trust dscp
!
interface GigabitEthernet3/1
 description to 3750-acc-1
 wrr-queue bandwidth 5 25 70
```

```
 wrr-queue queue-limit 5 25 40
 wrr-queue random-detect min-threshold 1 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 3 50 60 70 80 90 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 2 100 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 3 60 70 80 90 100 100 100 100
 wrr-queue cos-map 1 1 1
 wrr-queue cos-map 2 1 0
 wrr-queue cos-map 3 1 4
 wrr-queue cos-map 3 2 2
 wrr-queue cos-map 3 3 3
 wrr-queue cos-map 3 4 6
 wrr-queue cos-map 3 5 7
 mls qos trust dscp
!
interface GigabitEthernet4/1
 description to 6k-core-1
 wrr-queue bandwidth 30 70
 wrr-queue queue-limit 40 30
 wrr-queue random-detect min-threshold 1 40 80
 wrr-queue random-detect min-threshold 2 70 80
 wrr-queue random-detect max-threshold 1 80 100
 wrr-queue random-detect max-threshold 2 80 100
 wrr-queue cos-map 1 1 1
 wrr-queue cos-map 1 2 0
 wrr-queue cos-map 2 1 2 3 4
 wrr-queue cos-map 2 2 6 7
 mls qos trust dscp
```

マルチキャストの設定

DSM では、IPv6 マルチキャストが完全にサポートされます。IPv6 マルチキャスト設計はこのマニュアルでは説明しませんが、3750-acc-1、6k-dist-1、6k-core-1、および 6k-agg-1（RP として動作）スイッチでの IPv6 マルチキャスト設定を示します。ほとんどの設定例は小さなものですが、動作上の一貫性を確保するために、アクセス レイヤからアグリゲーション レイヤまで示しています。

- 3750-acc-1

```
ipv6 mld snooping                       #Globally enable MLD snooping (see note below)
```

- 6k-dist-1

```
ipv6 multicast-routing                  #Globally enable IPv6 multicast routing
```

- 6k-core-1

```
ipv6 multicast-routing
```

- 6k-agg-1

```
ipv6 multicast-routing
!
ipv6 pim rp-address 2001:DB8:CAFE:10::e555:5050 ERP      #Embedded-RP is being used
                                                         #which requires the local
                                                         #definition of the RP.
                                                         #This command line states
                                                         #that this switch (v6 address
                                                         #on VLAN10) is the RP for any
                                                         #group permitted in the ACL
                                                         #ERP
!
```

```
ipv6 access-list ERP                                  #ACL to permit Embedded-RP group range
                                                      #FF7E:140:2001:DB8:CAFE:10::/96
 permit ipv6 any FF7E:140:2001:DB8:CAFE:10::/96 log-input
```

最初に理解すべきことは、PIM-SSM または Embedded-RP を使用する場合、IPv6 マルチキャストをイネーブルにするための CLI 入力は不要であるという点です。PIM-SSM のみを使用する場合、「ipv6 multicast-routing」をグローバルにイネーブル化するだけで、すべての IPv6 対応インターフェイスで自動的に PIM がイネーブルになります。これは、IPv4 マルチキャストの要件との大きな相違点です。

上記の例では、レイヤ 2 スイッチ（3750-acc-1）には IPv6 マルチキャストの認識能力が必要です。マルチキャストをアクティブにリッスンしているポートにのみ、マルチキャスト トラフィックを配信するためです。これは MLD スヌーピングをイネーブルにすることによって達成されます。3750-acc-1 スイッチで MLD スヌーピングをイネーブルに設定し、6k-dist-1（および 6k-dist-2）で IPv6 マルチキャスト ルーティングをイネーブルに設定することにより、3750-acc-1 は、両方のディストリビューション レイヤ スイッチを、ローカルに接続されたマルチキャスト ルータとして認識できるようになります。

```
3750-acc-1#sh ipv6 mld snooping mrouter
Vlan    ports
----    -----
   2    Gi1/0/25(dynamic), Gi1/0/26(dynamic)
```

アクセス レイヤ スイッチでグループがアクティブな場合、そのグループに関する情報を表示できます。

```
3750-acc-1#show ipv6 mld snooping address
Vlan      Group          Type        Version     Port List
------------------------------------------------------------
2         FF35::1111     mld         v2          Gi1/0/25, Gi1/0/26
```

6k-dist-1 では、PIM、マルチキャスト ルート、RPF、およびグループに関する情報を、IPv4 の場合と同じように表示できます。PIM-SSM (FF35::1111) を使用しているアクティブ グループの出力は次のとおりです。このストリームは 6k-core-1 スイッチから着信し、VLAN2（3750-acc-1）インターフェイスから発信されます。

```
6k-dist-1#show ipv6 mroute                      #"show ipv6 pim topology" can also be used
Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group,
       C - Connected, L - Local, I - Received Source Specific Host Report,
       P - Pruned, R - RP-bit set, F - Register flag, T - SPT-bit set,
       J - Join SPT
Timers: Uptime/Expires
Interface state: Interface, State

(2001:DB8:CAFE:11:2E0:81FF:FE2C:9332, FF35::1111), 19:58:58/never, flags: sTI
  Incoming interface: GigabitEthernet4/1
  RPF nbr: FE80::215:C7FF:FE24:7440
  Immediate Outgoing interface list:
    Vlan2, Forward, 19:58:58/never
```

ルーテッド アクセスの設定

ルーテッド アクセス設計を使用する場合、キャンパス実装に対する主な変更は、アクセス レイヤおよびディストリビューション レイヤの設定に適用されます。従来の設計ではアクセス レイヤがレイヤ 2 だけのコンポーネントであり、最初のレイヤ 3 コンポーネントはディストリビューション レイヤに存在していたのに対し、ルーテッド アクセス設計を使用すると、アクセス レイヤがルーティングを実行します。ルーテッド アクセス設計の利点と欠点については、このマニュアルでは説明しません。ただし、フェールオーバー パフォーマンスが向上する点と、スパニング ツリーがアクティブ コンポーネントではないという重要な事実から、この設計は多くのカスタ

マーにとって魅力的です。ルーテッド アクセス設計に対するカスタマーからの需要、パフォーマンス、運用上の利点を考慮して、このマニュアルでは、この設計における IPv6 の実装について説明します。

DSM をルーテッド アクセス設計にする拡張は、非常に簡単です。冗長なファーストホップ プロトコルへの依存が取り除かれることも、アクセス レイヤの主な改良点の 1 つです。基本的に、アクセス レイヤ スイッチは IPv6 ルーティングを有効にし、トランク リンクをルーテッド リンクに変更します。そしてディストリビューション スイッチは、アクセス レイヤのためにトランクと VLAN を削除します。

図 13 に、ルーテッド アクセス コンポーネントを含む、更新後の DSM トポロジを示します。ディストリビューション レイヤのアップストリームでは何も変更しないので、この図には変更されたアクセス レイヤとディストリビューション レイヤだけを示します。

図 13　　DSM トポロジ — ルーテッド アクセス設計

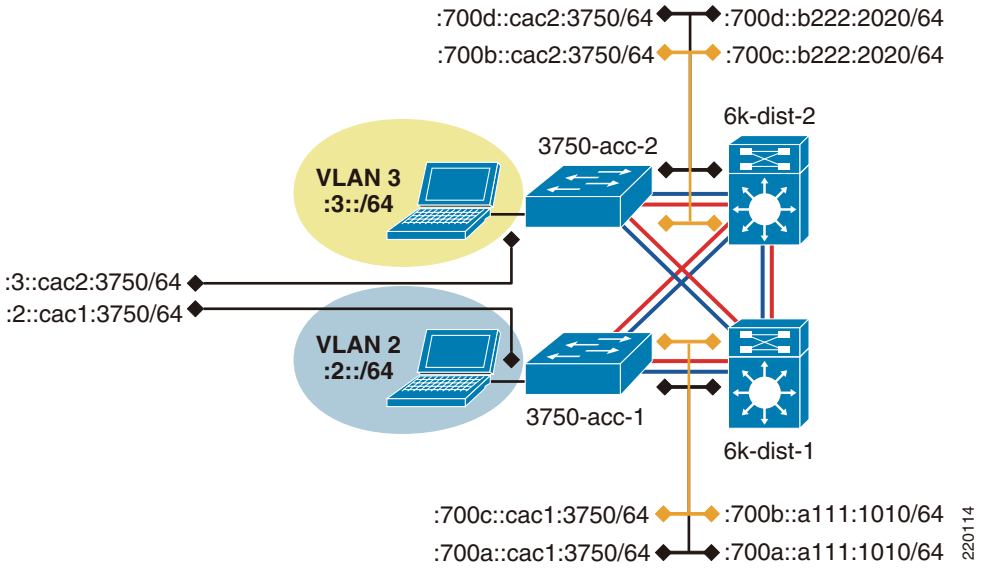


図 13 では、アクセス レイヤとディストリビューション レイヤの間のリンクが、トランキングされたレイヤ 2 リンクではなく、ルーテッド リンクになっています。この新しいリンクには IPv6 アドレッシングとルーティングが設定されており、VLAN 内のホストは、アクセス スイッチの VLAN インターフェイスの IPv6 アドレスを、デフォルト ゲートウェイとして使用します。次の設定例は、3750-acc-1 および 6k-dist-1 スイッチに関連する設定を示しています。

- 3750-acc-1

```
ipv6 unicast-routing                          #Globally enable IPv6 unicast routing
!
interface GigabitEthernet1/0/25
 description To 6k-dist-1
 load-interval 30
 carrier-delay msec 0
 srr-queue bandwidth share 1 70 25 5
 srr-queue bandwidth shape  3  0  0  0
 priority-queue out
 ipv6 address 2001:DB8:CAFE:700A::CAC1:3750/64              #Link is now a routed link
 ipv6 nd suppress-ra
 ipv6 ospf network point-to-point                  #OSPFv3 is configured in order to
                                                   #establish a peer relationship with
                                                   #6k-dist-1
 ipv6 ospf hello-interval 1
 ipv6 ospf dead-interval 3
```

```
 ipv6 ospf 1 area 2                                  #Link is in area 2
 no ipv6 redirects
 mls qos trust dscp
!
interface Vlan2
 load-interval 30
 ipv6 address 2001:DB8:CAFE:2::CAC1:3750/64          #VLAN2 on this switch becomes the
                                                     #first layer 3 point for the hosts
                                                     #in VLAN2 - the link-local address
                                                     #on VLAN 2 will be the default
                                                     #gateway for the hosts
 ipv6 ospf 1 area 2                                  #VLAN2 is in area 2
 no ipv6 redirects
!
ipv6 router ospf 1
 router-id 10.120.2.1
 log-adjacency-changes
 auto-cost reference-bandwidth 10000
 area 2 stub no-summary                        #Per the Routed Access Design guide - the
                                               #area (area 2) for the access layer
                                               #prefix is a totally stubby area
 passive-interface Vlan2
 timers spf 1 5
```

- 6k-dist-1

```
interface GigabitEthernet3/1
 description to 3750-acc-1
 dampening
 load-interval 30
 carrier-delay msec 0
 ipv6 address 2001:DB8:CAFE:700A::A111:1010/64        #Link is now a routed link
 no ipv6 redirects
 ipv6 nd suppress-ra
 ipv6 cef
 ipv6 ospf network point-to-point
 ipv6 ospf hello-interval 1
 ipv6 ospf dead-interval 3
 ipv6 ospf 1 area 2                                    #Link is in area 2
 wrr-queue bandwidth 5 25 70
 wrr-queue queue-limit 5 25 40
 wrr-queue random-detect min-threshold 1 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 3 50 60 70 80 90 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 2 100 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 3 60 70 80 90 100 100 100 100
 wrr-queue cos-map 1 1 1
 wrr-queue cos-map 2 1 0
 wrr-queue cos-map 3 1 4
 wrr-queue cos-map 3 2 2
 wrr-queue cos-map 3 3 3
 wrr-queue cos-map 3 4 6
 wrr-queue cos-map 3 5 7
 mls qos trust dscp
!
ipv6 router ospf 1
 router-id 10.122.10.9
 log-adjacency-changes
 auto-cost reference-bandwidth 10000
 area 2 stub no-summary                        #Per the Routed Access Design guide - the
                                               #area (area 2) for the access layer
                                               #prefix is a totally stubby area
 area 2 range 2001:DB8:CAFE:2::/64 cost 10     #Send a summary into area 0 for
```

```
                                                    #prefix "2" in area 2
     area 2 range 2001:DB8:CAFE:3::/64 cost 10
     area 2 range 2001:DB8:CAFE:7004::/64 cost 10
     area 2 range 2001:DB8:CAFE:700A::/64 cost 10
     area 2 range 2001:DB8:CAFE:700B::/64 cost 10
     passive-interface Loopback0
     timers spf 1 5
```

3750-acc-1 の「show ipv6 route」出力は、2 つのディストリビューション レイヤ スイッチから着信するデフォルト ルートを示しています（このデフォルトは、インターネット エッジがコア レイヤに接続するアップストリーム スイッチによってインジェクトされます）。

```
3750-acc-1#show ipv6 route
IPv6 Routing Table - 13 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
OI   ::/0 [110/11]
     via FE80::213:5FFF:FE1F:F840, GigabitEthernet1/0/26              #6k-dist-2
     via FE80::215:C7FF:FE25:9580, GigabitEthernet1/0/25              #6k-dist-1
C    2001:DB8:CAFE:2::/64 [0/0]
     via ::, Vlan2
L    2001:DB8:CAFE:2::CAC1:3750/128 [0/0]
     via ::, Vlan2
```

（注） この出力は、あくまで抜粋に過ぎません。

DSM でルーテッド アクセス設計を使用する場合、もう 1 つ変更する点は、IPv6 マルチキャストの設定です。アクセス レイヤ スイッチがルーティングを実行するので、ネットワークの他の部分で使用されている様々な PIM をスイッチがサポートするように設定する必要があります。前出の 6k-dist-1 のマルチキャスト設定では、汎用的な PIM-SSM または PIM-SM と Embedded-RP の組み合わせが使用できます。どのアクセス レイヤ プラットフォームが IPv6 マルチキャスト ルーティングをサポートするか、どのコードバージョンであるかを確認することが重要です。

シスコのルーテッド アクセス設計についての詳細は、次の URL を参照してください。

- 『*Campus SRNDs—Routed Access and High Availability*』— http://www.cisco.com/en/US/netsol/ns656/networking_solutions_design_guidances_list.html#anchor2
- 『*Routed Access Q&A*』— http://www.cisco.com/en/US/netsol/ns340/ns394/ns147/ns17/netqa0900aecd8045965a.html
- 『*Routing in the Wiring Closet*』white paper — http://www.cisco.com/en/US/netsol/ns340/ns394/ns147/ns17/networking_solutions_white_paper0900aecd804c6e73.shtml

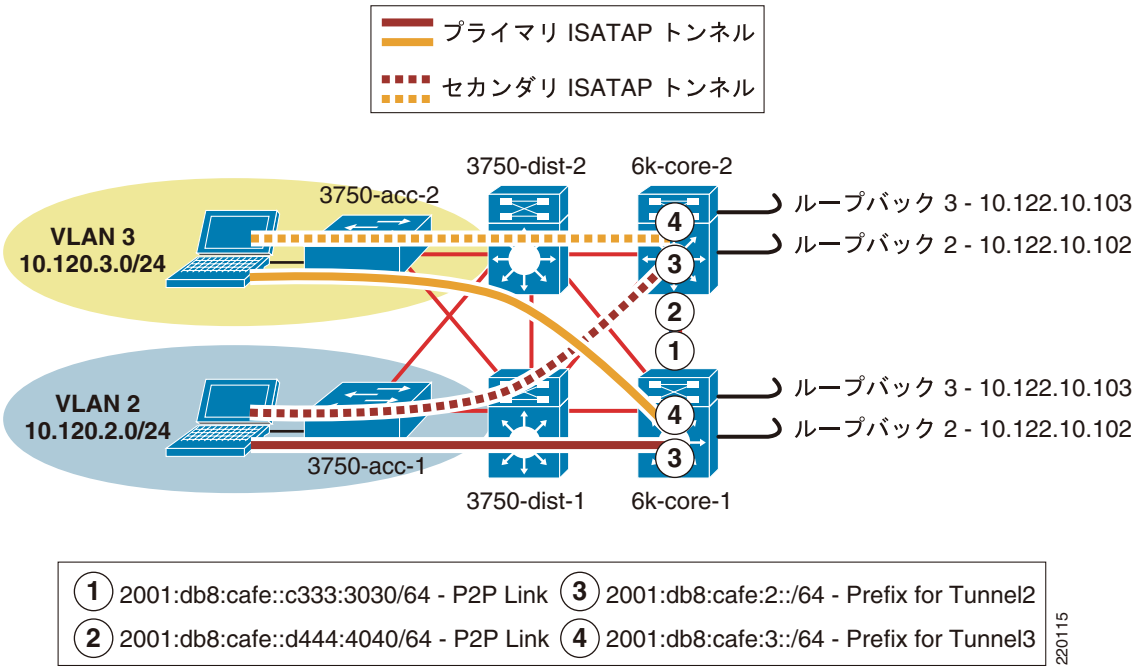
ハイブリッド モデル — 例 1 の実装

HME1 のキャンパス ネットワークは、大部分が IPv4 のみです。キャンパス ネットワークの IPv6 部分は、コア レイヤで始まります。ここでは、コア レイヤの設定のほかに、ホストの基本的な ISATAP 設定も示します。前述したように、HME1 ではコア レイヤからデータセンターまでデュアルスタックを使用します。これらの設定は DSM での設定と同じなので、HME1 モデルに固有ではありません。DSM の実装セクションと同様、ここでも導入の各側面について部分的な設定例を示します。設定全体については「付録 — 設定リスト」（p.66）を参照してください。

ネットワーク トポロジ

HME1 トポロジの相違点の 1 つは、ディストリビューション レイヤで Catalyst 6500 ではなく Catalyst 3750 スイッチのペアを使用している点です。これはテスト ラボの構成がこのようになっていたからに過ぎず、何か問題があるわけでも、これが推奨事項というわけでもありません。図 14 に HME1 のネットワーク トポロジを示します。

図 14　　HME1 のネットワーク トポロジ



このトポロジは、アクセス レイヤでの IPv4 アドレッシング（ホストが ISATAP トンネルの確立に使用）、コア レイヤでの IPv4 アドレッシング（ホストが ISATAP の終端ポイントとして使用）、およびコア レイヤで p2p リンクと ISATAP トンネル プレフィクスの両方に使用される IPv6 アドレッシングを中心としています。この設定では、両方のコア スイッチ間で同じ IPv4 アドレスを共有する冗長に設定されたループバック インターフェイスを使用して、ISATAP アクセスのハイアベイラビリティを達成していることがわかります。アクセス レイヤの各 ISATAP ホストでプレフィクスの一貫性を保つために、プライマリおよびバックアップの両方の ISATAP トンネルに同じプレフィクスを使用しています。

物理設定

両方のコア レイヤ スイッチの設定を示します。これらの設定には、ディストリビューション レイヤとコア レイヤ側のインターフェイスだけが含まれています。ディストリビューション レイヤとアクセス レイヤにおける IPv4 部分の設定は、既存のキャンパス設計に関するベスト プラクティスに基づいており、ここでは説明しません。IPv4 の設定値を含む設定全体は「付録 — 設定リスト」（p.66）を参照してください。

- 6k-core-1

```
interface GigabitEthernet1/1
 description to 3750-dist-1
 dampening
 ip address 10.122.0.41 255.255.255.252
 no ip redirects
 no ip proxy-arp
```

```
 ip hello-interval eigrp 10 1
 ip hold-time eigrp 10 3
 load-interval 30
 carrier-delay msec 0
 mls qos trust dscp
!
interface GigabitEthernet1/2
 description to 3750-dist-2
 dampening
 ip address 10.122.0.45 255.255.255.252
 no ip redirects
 no ip proxy-arp
 ip hello-interval eigrp 10 1
 ip hold-time eigrp 10 3
 load-interval 30
 carrier-delay msec 0
 mls qos trust dscp
!
interface GigabitEthernet2/3
 description to 6k-core-2
 dampening
 ip address 10.122.0.21 255.255.255.252
 ip hello-interval eigrp 10 1
 ip hold-time eigrp 10 3
 load-interval 30
 carrier-delay msec 0
 ipv6 address 2001:DB8:CAFE::c333:3030/64              #p2p link between core switches
 ipv6 ospf network point-to-point
 ipv6 ospf hello-interval 1
 ipv6 ospf dead-interval 3
 ipv6 ospf 1 area 0
 mls qos trust dscp
```

- 6k-core-2

```
interface GigabitEthernet1/1
 description to 3750-dist-1
 dampening
 ip address 10.122.0.49 255.255.255.252
 no ip redirects
 no ip proxy-arp
 ip hello-interval eigrp 10 1
 ip hold-time eigrp 10 3
 load-interval 30
 carrier-delay msec 0
 mls qos trust dscp
!
interface GigabitEthernet1/2
 description to 3750-dist-2
 dampening
 ip address 10.122.0.53 255.255.255.252
 no ip redirects
 no ip proxy-arp
 ip hello-interval eigrp 10 1
 ip hold-time eigrp 10 3
 load-interval 30
 carrier-delay msec 0
 mls qos trust dscp
!
interface GigabitEthernet2/3
 description to 6k-core-1
 dampening
 ip address 10.122.0.22 255.255.255.252
 ip hello-interval eigrp 10 1
```

```
ip hold-time eigrp 10 3
load-interval 30
carrier-delay msec 0
ipv6 address 2001:DB8:CAFE::d444:4040/64
ipv6 ospf network point-to-point
ipv6 ospf hello-interval 1
ipv6 ospf dead-interval 3
ipv6 ospf 1 area 0
mls qos trust dscp
```

トンネルの設定

トンネル レベルでの ISATAP 設定は比較的分かりやすいですが、ISATAP トンネルのハイ アベイラビリティ設計に関連する部分は、少々複雑かもしれません。ホストでの ISATAP の基本的な設定は、IPv6 をイネーブルにすることと、ISATAP ルータ名または IPv4 アドレスを設定することです。デフォルトでは、Microsoft Windows XP および Vista は、「isatap.domain.com」の DNS クエリーを実行します（「domain.com」はローカル ドメイン名）。「isatap」に対応する DNS「A」レコードが設定されている場合、ホストはそのアドレスへの ISATAP トンネルの確立を開始します。このデフォルト設定は、ISATAP ルータ、またはそのルータへのパスに何かが起こらないかぎり、問題なく動作します。このマニュアルで説明するすべての設定には、IPv6 サービスにできるだけ最適な耐障害性を提供する機能が含まれています。

HME1 環境では ISATAP のハイ アベイラビリティを確保することが不可欠です。いくつかの方式で ISATAP ルータの冗長性を提供できます。このマニュアルで説明する方式では、2 つのコア レイヤ スイッチを使用して、ISATAP トンネルの非常に高速なフェールオーバーを提供します。一般的に使用する別の方式は、DNS に依存します。DNS 方式は迅速に実装できますが、全体的な IPv6 キャンパス設計から見ると制約が多く、フェールオーバーは最も低速です。

（ホストの観点からの）トンネル デスティネーションを両方のコア スイッチで冗長にすることと、IPv4 および IPv6 ルーティングの両方を正しく設定することが重要です。

（注） このマニュアルの作成時点では、複数の tunnel source コマンドに対して 1 つのループバックを使用する Catalyst 6500 は、トンネル トラフィックをソフトウェアで処理します。このような場合、システムからユーザに警告メッセージが発行されます。HME1 設計では、この問題による支障はありません。各トンネルがコントロールとスケールを目的にそれぞれ個別のループバックを使用するからです。

よく聞かれる質問の 1 つに、「ディストリビューション レイヤ（IPv4）から 1 つの ISATAP ルータまで、決定論的ルーティングを使用すべきか、それとも何らかのロード バランシングの値を使用すべきか？」という問題があります。次の考慮事項が当てはまります。

- ISATAP トンネルの発信ロード バランシングをサポートする唯一のホスト OS は Microsoft Windows Vista であり、これには設定が必要です。
- カスタマーの導入事例と詳細なテストの結果、ISATAP ルータに対する ISATAP ホストのロード バランシングには、ほとんどメリットがないことが判明しています。テストによると、ISATAP トンネルに冗長な IPv6 プレフィクスを使用する場合、ホスト側からのロード バランシングは、ルーティング機能に問題を引き起こすことが判明しています。この設定例では、コア レイヤ スイッチが、この設計のすべての ISATAP トンネルの負荷を処理できるようになっています。プライマリのコア レイヤ スイッチに障害が発生すると、セカンダリがすべてのトンネルを問題なく引き継ぐことができます。この設計にロード バランシングを使用しても、パフォーマンス、負荷、またはアベイラビリティが改善されないばかりか、ISATAP のトラフィック フローのトラブルシューティングがさらに難しくなるため、オペレータによる管理作業が複雑になります。ISATAP に決定論的な設計を実装すれば、トラフィック管理とトラブルシューティングの負担が軽減され、リターン ルーティングの問題も排除されます。

コア レイヤ スイッチに障害が発生した場合に ISATAP トンネルのコンバージェンス時間を短く保つには、両方のコア スイッチに冗長で重複したトンネル アドレスを提供することが重要です。そうすれば、ホストに必要なのは 1 つの ISATAP ルータ アドレスまたは名前だけであり、DNS ラウンドロビンは不要です。このプロセスを次に説明します。

1. 両方のコア レイヤ スイッチに、同じループバック アドレス（例：10.122.10.102）を設定します。ループバック インターフェイスは安定した状態を保ち、トンネル終端に最適です。
2. 両方のコア レイヤ スイッチに、ループバックをソースとして使用する 1 つの ISATAP トンネルを設定します（例：Loopback2 — 10.122.10.102）。ISATAP IPv6 プレフィクスは両方のスイッチで同じなので、ホストはどちらのスイッチで終端しても、同じプレフィクスを接続に使用します。
3. 両方のコア レイヤ スイッチが、IPv4 IGP を介してループバック アドレスをアドバタイズするように設定します。プライマリ スイッチ（6k-core-1）は、ループバック アドレスのデフォルトの IGP メトリックを使用します。セカンダリ スイッチ（6k-core-2）は、このスイッチのループバック アドレスの優先度を低くするために、IGP メトリック（EIGRP の delay 値）を変更します。繰り返しになりますが、同じプレフィクスを使用するトンネル間でのロード バランシングは望ましくないため、トンネルには決定論的なフローを使用することを推奨します。
4. 両方のコア レイヤ スイッチが、IPv6 IGP を介して ISATAP IPv6 プレフィクスをアドバタイズするように設定します。プライマリ スイッチ（6k-core-1）は、ISATAP トンネルの IPv6 プレフィクスにデフォルトの IGP メトリックを使用します。セカンダリ スイッチ（6k-core-2）は、このスイッチの ISATAP プレフィクスの優先度を低くするために、IGP メトリック（OSPFv3 の cost 値）を変更します。この設定は任意です。このマニュアルでは、IPv4（ステップ 3 を参照）と IPv6 の両方に決定論的なフローが望ましいことを説明するために使用しています。
5. ホストに、手動で定義された ISATAP ルータのアドレスまたは名前（DNS「A」レコードと相関関係がある）を設定します。

ISATAP トンネル、HA、およびルーティングの設定をわかりやすくするために、これらを一括して示します。

簡潔さを保つために、VLAN2 のトンネル設定のみを記載します。VLAN3 のトンネルは、アドレッシングを除いて同じです。

上記の 5 つのステップを具体的に示した設定は、次のとおりです。

- 6k-core-1

```
interface Loopback2
 description Tunnel source for ISATAP-VLAN2
 ip address 10.122.10.102 255.255.255.255            #Address that will be used as the
                                                      #ISATAP tunnel2 source
!
interface Tunnel2
 description ISATAP VLAN2
 no ip address
 no ip redirects
 ipv6 address 2001:DB8:CAFE:2::/64 eui-64            #Tunnel prefix used for ISATAP
                                                     #hosts connecting to this tunnel.
                                                      #Interface-ID address for this
                                                      #switch will be generated using
                                                      #EUI-64
 no ipv6 nd suppress-ra                               #Tunnels interfaces disable the
                                                      #sending of RA's. This command
                                                      #re-enables RA's on this
                                                      #interface.
 ipv6 cef
 ipv6 ospf 1 area 2                                    #Just like the VLAN in the DSM,
                                                       #this interface is not part of
                                                       #area 0
 tunnel source Loopback2                               #Tunnel2 uses loopback2 as the
```

```
                                                                  #source
 tunnel mode ipv6ip isatap                                        #Define the tunnel as ISATAP
!
router eigrp 10
 passive-interface Loopback0
 passive-interface Loopback1
 passive-interface Loopback2
 passive-interface Loopback3
 network 10.0.0.0                                          #Covers Loopback2 interface and ensures
                                                            #that the 10.122.10.102 address is
                                                            #advertised to the rest of the network
 no auto-summary
 eigrp router-id 10.122.10.9
!
ipv6 router ospf 1
 router-id 10.122.10.9
 log-adjacency-changes
 auto-cost reference-bandwidth 10000
 area 2 range 2001:DB8:CAFE:2::/64 cost 10      #Advertise a summary for the prefix on
                                                #Tunnel2 - just like a VLAN prefix
                                                #would be sent in the DSM
 area 2 range 2001:DB8:CAFE:3::/64 cost 10
 passive-interface Loopback0
 passive-interface Loopback2
 passive-interface Loopback3
 passive-interface Tunnel2
 passive-interface Tunnel3
 timers spf 1 5
```

- 6k-core-2

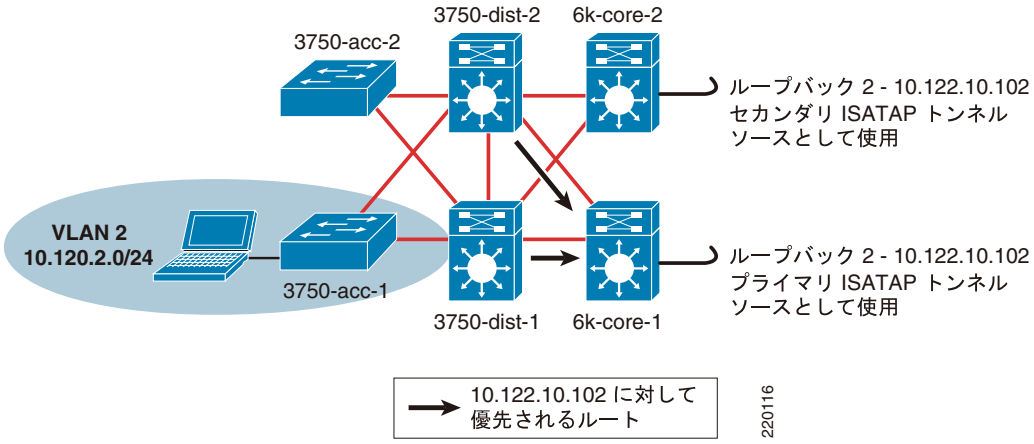
```
interface Loopback2
 description Tunnel source for ISATAP-VLAN2
 ip address 10.122.10.102 255.255.255.255
 delay 1000                                    #Delay adjusted for EIGRP (IPv4)
                                               #in order to adjust preference
                                               #for the 10.122.10.102 host
                                               #route. This ensures that
                                               #6k-core-2 is SECONDARY to 6k-core-1
!
interface Tunnel2
 description ISATAP VLAN2
 no ip address
 no ip redirects
 ipv6 address 2001:DB8:CAFE:2::/64 eui-64
 no ipv6 nd suppress-ra
 ipv6 cef
 ipv6 ospf 1 area 2
 tunnel source Loopback2
 tunnel mode ipv6ip isatap
!
router eigrp 10
 passive-interface Loopback0
 passive-interface Loopback1
 passive-interface Loopback2
 passive-interface Loopback3
 network 10.0.0.0
 no auto-summary
 eigrp router-id 10.122.10.10
!
ipv6 router ospf 1
 router-id 10.122.10.10
 log-adjacency-changes
 auto-cost reference-bandwidth 10000
```

```
area 2 range 2001:DB8:CAFE:2::/64 cost 20          #Cost for prefix adjusted so that
                                                    #the route from 6k-core-2 is not
                                                    #preferred or equal to 6k-core-1
                                                    #Not required.
area 2 range 2001:DB8:CAFE:3::/64 cost 20
passive-interface Loopback0
passive-interface Loopback2
passive-interface Loopback3

passive-interface Tunnel2
passive-interface Tunnel3
timers spf 1 5
```

図 15 に、ディストリビューション レイヤ スイッチから ISATAP トンネル インターフェイス（コア スイッチのループバック）への IPv4 ルーティングを示します。6k-core-1 の Loopback2 は、ホストのプライマリ ISATAP ルータ アドレスとして設定されています。前出の IPv4 IGP 設定で示したように、6k-core-2 のホスト ルートは 10.122.10.102 に設定され、遅延が大きいため優先されません。ISATAP ルータ（10.122.10.102）の VLAN2 のホストからパケットが着信すると、ディストリビューション スイッチで 10.122.10.102 のルックアップが実行され、そのアドレスのネクスト ホップは 6k-core-1 です。

図 15　　HME1 — 優先される 6k-core-1 へのルート



ディストリビューション レイヤ スイッチのルーティング テーブル 10.122.10.102 は、次のとおりです。

- 3750-dist-1（ルート出力の抜粋）

```
3750-dist-1#show ip route | b 10.122.10.102/32
D       10.122.10.102/32
[90/130816] via 10.122.0.41, 00:09:23, GigabitEthernet1/0/27          #3750-dist-1
                                                                      #has only one
                                                                      #route for
                                                                      #10.122.10.102
                                                                      #which is via
                                                                      #10.122.0.41
                                                                      #6k-core-1)
```

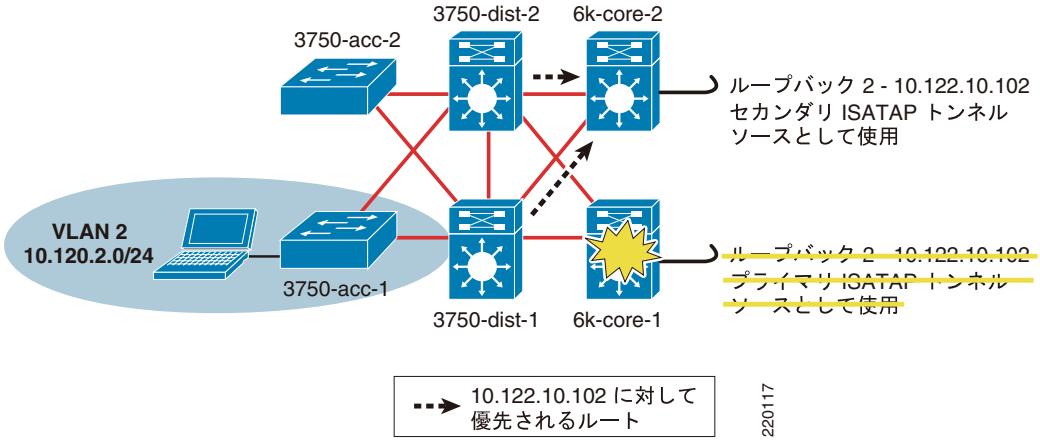
- 3750-dist-2

```
3750-dist-1#show ip route | b 10.122.10.102/32
D       10.122.10.102/32
[90/130816] via 10.122.0.45, 00:10:03, GigabitEthernet1/0/27          #3750-dist-2
                                                                      #has only one
                                                                      #route for
                                                                      #10.122.10.102
```

```
#which is via
#10.122.0.45
#6k-core-1)
```

図 16 は、6k-core-1 に障害が発生したため、loopback2（10.122.10.102）へのルートが使用できなくなった場合を示しています。6k-core-1 ルートが削除されると、10.122.10.102 への新しいルートが使用され、パケットは 6k-core-2 に転送されます。

図 16　　HME1 — 6k-core-1 が故障した場合に優先される 6k-core-2 へのルート



ディストリビューション レイヤ スイッチで、10.122.10.102 に対応する更新後のルーティング テーブル エントリは、次のとおりです。

- 3750-dist-1（ルート出力の抜粋）

```
3750-dist-1#show ip route | b 10.122.10.102/32
D       10.122.10.102/32
      [90/258816] via 10.122.0.49, 00:00:08, GigabitEthernet1/0/28
```

- 3750-dist-2

```
3750-dist-1#show ip route | b 10.122.10.102/32
D       10.122.10.102/32
[90/258816] via 10.122.0.53, 00:00:08, GigabitEthernet1/0/28
```

HME1 環境でホストの ISATAP 通信をイネーブルにするには、次の 2 つの方法があります。

- ISATAP IPv4 ルータ アドレスを手動で定義
- ISATAP IPv4 DNS 名を手動で定義（DNS レコード エントリが必要）

ISATAP IPv4 ルータ アドレス方式の使用は複雑ではありませんが、何らかのスクリプトまたはホスト管理ツールがないと、スケールが難しくなります。前述したように、Windows Scripting Host、Microsoft SMS Server など各種のツールを使用して、ログイン時、または所定のタイミングにおいてホスト上でローカルにコマンドを実行できます。

VLAN2 内の Microsoft Windows XP または Windows Vista ホストでは、ISATAP がイネーブルに設定され、IPv4 ISATAP ルータ アドレスが定義されます（ホストでは IPv6 がすでにイネーブルです）。前述したように、HME1 設計では VLAN/ サブネット内のホストが特定の ISATAP ルータ アドレスにマッピングされます。次の例では、ホストは VLAN 2 に存在します。これは 10.120.**2**.0/24 サブネットに存在するので 10.122.10.10**2** の ISATAP ルータを使用するように設定されています（ここで「10**2**」の「**2**」は、VLAN またはサブネット **2** を表します）。VLAN **3** または 10.120.**3**.0/24 でも同様です（この場合は ISATAP ルータは 10.122.10.10**3**）。

```
C:\>netsh interface ipv6 isatap set router 10.122.10.102 enabled
Ok.
```

このアドレスが受け入れられたかどうかは、次のコマンドで確認できます。

```
C:\>netsh interface ipv6 isatap show router
Router Name            : 10.122.10.102
Use Relay              : enabled
Resolution Interval    : default
```

ホストはプライマリのコア レイヤ スイッチ（6k-core-1）への ISATAP 接続を正常に確立し、有効なプレフィクス（2001:db8:cafe:2:0:5efe:10.120.2.101）を受信しました。ISATAP は、ホストの IPv4 アドレスを、64 ビット インターフェイス ID の右端の 32 ビット部分として使用し、左端の 32 ビットを「0000:5efe」で「パディング」します。IPv4 アドレス（10.120.2.101）がトンネルのホスト側でトンネル ソースとして使用され、コア レイヤ スイッチの loopback2（10.122.10.102）がホストのトンネル デスティネーション（前に定義した ISATAP ルータ アドレス）として使用されます。

トンネル アタプタの自動トンネリング疑似インターフェイスは次のとおりです。

```
Connection-specific DNS Suffix  . :
IP Address. . . . . . . . . . . . : 2001:db8:cafe:2:0:5efe:10.120.2.101
IP Address. . . . . . . . . . . . : fe80::5efe:10.120.2.101%2
Default Gateway . . . . . . . . . : fe80::5efe:10.122.10.102%2
```

ISATAP IPv4 ルータ名を使用する方式も難しくありませんが、この場合は DNS エントリが必要です。この場合も、何らかのスクリプトまたはホスト管理ツールがないと、スケールが難しくなります。前述したように、Windows Scripting Host、Microsoft SMS Server など各種のツールを使用して、ログイン時、または所定のタイミングにおいてホスト上でローカルにコマンドを実行できます。

この例では、ISATAP IPv4 アドレスの代わりに ISATAP ルータの名前を使用しています。ISATAP が解決を試みるデフォルトの DNS 名は、「isatap」にドメイン サフィックスが付いたものです。たとえば、このホストがドメイン「cisco.com」に存在する場合、ホストは「isatap.cisco.com」の解決を試みます。ユーザはアドレス選択を変更する場合と同じように、この名前を変更することができます。

```
C:\>netsh interface ipv6 isatap set router vlan2-isatap enabled
Ok.

C:\>netsh interface ipv6 isatap show router
Router Name            : vlan2-isatap
Use Relay              : enabled
Resolution Interval    : default
```

DNS サーバでは、このマニュアルに示す 2 つの VLAN に対応する次のエントリがあります。

- vlan2-isatap — ホスト（A）10.122.10.102
- vlan3-isatap — ホスト（A）10.122.10.103

QoS の設定

HME1 の QoS ポリシーは、既存の IPv4 ポリシーと一致している必要があります。前述したように、HME1 モデルでは、IPv6 パケットの分類とマーキングを実行する場所に関する問題があります。IPv6 パケットは、アクセス レイヤのホストからコア レイヤまでの ISATAP トンネル全体を通じてカプセル化され、IPv6 QoS ポリシーはトンネル内のパケットを認識できません。IPv6 パケットにポリシーを適用できる最初のポイントは、コア レイヤ スイッチの出力インターフェイスです。次に示す設定は単純な例に過ぎず、シスコのキャンパス QoS に関する推奨事項に基づくものではありません。このポリシーでは、クラス マップを使用して表 7 の IPv6 アクセス リストを照合します。

表 7　IPv6 QoS — クラス マップ、照合用 ACL、および DSCP 設定値

アプリケーション	アクセス グループ名	DSCP 設定値
FTP	BULK-APPS	AF11
Telnet	TRANSACTIONAL-APPS	AF21
SSH	TRANSACTIONAL-APPS	AF21
その他	N/A	0（デフォルト）

ポリシーは出力インターフェイス（アクセス レイヤのアップストリーム）で適用されます。アップストリーム スイッチはこれらの DSCP 設定値を信用することができ、必要に応じてキューイングとポリシングを適用します（「デュアルスタック モデル — 実装」[p.33] を参照）。

- 6k-core-1

```
mls qos
!
class-map match-all CAMPUS-BULK-DATA
  match access-group name BULK-APPS
class-map match-all CAMPUS-TRANSACTIONAL-DATA
  match access-group name TRANSACTIONAL-APPS
!
policy-map IPv6-ISATAP-MARK
  class CAMPUS-BULK-DATA
   set dscp af11
  class CAMPUS-TRANSACTIONAL-DATA
   set dscp af21
  class class-default
   set dscp default
!
ipv6 access-list BULK-APPS
 permit tcp any any eq ftp
 permit tcp any any eq ftp-data
!
ipv6 access-list TRANSACTIONAL-APPS
 permit tcp any any eq telnet
 permit tcp any any eq 22
!
interface GigabitEthernet2/1
 description to 6k-agg-1
 mls qos trust dscp
 service-policy output IPv6-ISATAP-MARK
!
interface GigabitEthernet2/2
 description to 6k-agg-2
 mls qos trust dscp
 service-policy output IPv6-ISATAP-MARK
!
interface GigabitEthernet2/3
 description to 6k-core-1
 mls qos trust dscp
 service-policy output IPv6-ISATAP-MARK
```

インフラストラクチャ セキュリティの設定

「アドレッシング」（p.18）で説明したセキュリティ設定に加えて、アクセス レイヤで ISATAP トンネルに関する IPv6 アクセス制御をさらに強化することができます。アクセス レイヤでは、ホスト ポートまたはアップリンク / トランク ポートでアクセス リストを適用できます。各ホスト ポートに ACL を設定するよりも、アップリンクで ACL を管理する方が簡単です。

使用できるアクセス リストの 1 つは、アクセス スイッチ上のホストから、その VLAN の ISATAP ルータ アドレスまでのトンネルを許可する ACL です。たとえば、次の ACL は、宛先が 10.122.10.102（前に設定した ISATAP ルータ アドレス）である場合にのみ、ISATAP トンネルを（プロトコル 41 で）許可します。前述したように、この ACL は、特定のホスト ポートで入力時（**ip access-group 100 in**）に適用することも、アップリンク トランクまたはルーテッド ポート（**ip access-group 100 out**）に適用することもできます。

```
access-list 100 remark Permit approved IPv6-Tunnels
access-list 100 permit 41 any host 10.122.10.102
access-list 100 deny   41 any any log-input
access-list 100 permit ip any any
```

サービス ブロック モデル — 実装

SBM における ISATAP の導入は、HME1 の場合とほぼ同様です。どちらのモデルでも、スイッチの冗長ペアを使用して、アクセス レイヤのホストから着信する ISATAP トンネルのフォールトトレラントな終端を提供します。SBM と HME1 の唯一の違いは、SBM の場合、接続（ISATAP、設定されたトンネル、またはデュアルスタック）を終端するために新しいスイッチの集合を専用で使用するのに対し、HME1 では既存のコア レイヤ スイッチを終端に使用する点です。

ここでは、サービス ブロック スイッチのインターフェイス（物理および論理）設定のほか、完全を期するため、データセンターのアグリゲーション レイヤ トンネル インターフェイスの設定を示します。全体的な IPv4 ネットワークは、HME1 の設定で説明したものと同じです。

また、この例でも ISATAP ルータ アドレスを再利用する必要があるため、SBM でのホスト設定も HME1 の場合と同じです。HME1 の設定セクションと同様に、ループバック、トンネル、ルーティング、およびハイ アベイラビリティの設定をすべて示します。

ネットワーク トポロジ

図をわかりやすくするために、このトポロジを 2 つの部分（ISATAP トポロジと手動設定トンネルのトポロジ）に分割しています。

図 17 は、SBM の ISATAP トポロジを示しています。このトポロジは、アクセス レイヤでの IPv4 アドレッシング（ホストが ISATAP トンネルの確立に使用）、サービス ブロックでの IPv4 アドレッシング（ホストが ISATAP トンネルの終端ポイントとして使用）、およびサービス ブロックで p2p リンクと ISATAP トンネル プレフィクスの両方に使用される IPv6 アドレッシングを中心としています。この設定では、両方の SBM スイッチ間で同じ IPv4 アドレスを共有するループバック インターフェイスを使用して、ISATAP アベイラビリティを達成していることがわかります。アクセス レイヤの各 ISATAP ホストでプレフィクスの一貫性を保つために、プライマリおよびバックアップの両方の ISATAP トンネルに同じプレフィクスを使用しています。

図 17　SBM における ISATAP ネットワークのトポロジ

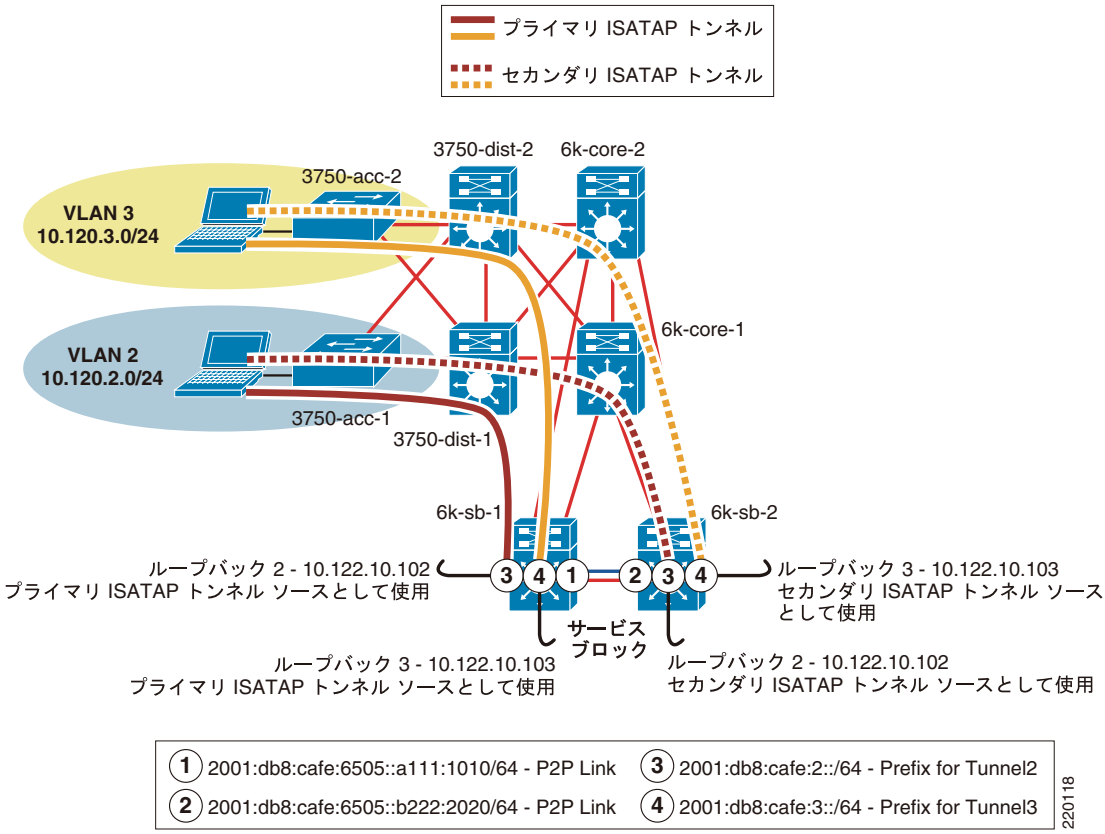
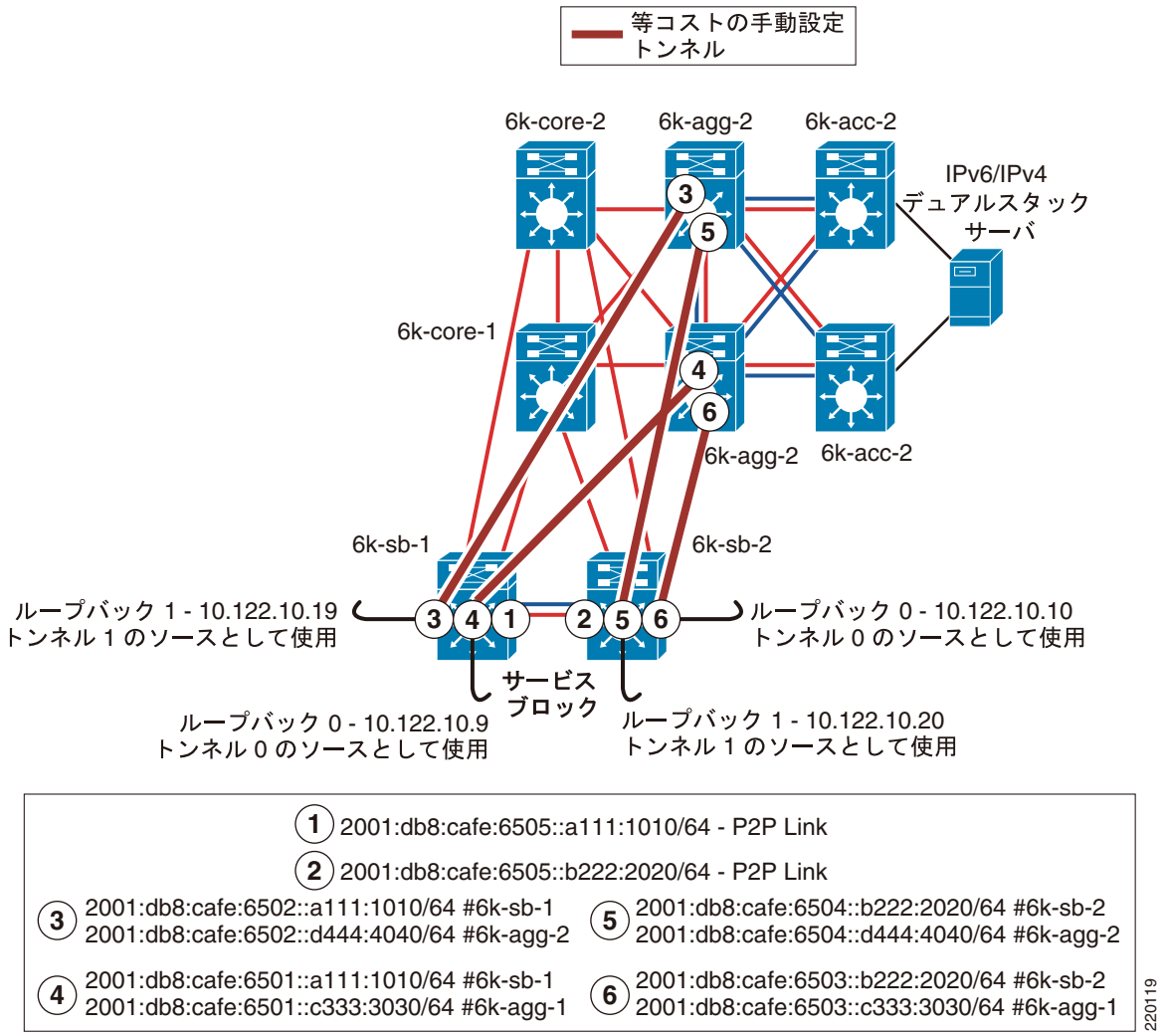


図 18 は、SBM の手動設定トンネル トポロジを示しています。このトポロジ図では、サービス ブロック スイッチのループバック アドレス（設定されたトンネルのトンネル ソースとして使用）と、手動設定トンネルのインターフェイスで使用する IPv6 アドレッシングが示されています。

図 18　SBM における手動設定トンネルのトポロジ



物理設定

両方のサービス ブロック スイッチの設定を、コア レイヤ側のインターフェイスも含めて示します。上記トポロジの IPv4 部分の設定は、サービス ブロック スイッチについてのみ示します。それ以外の IPv4 設定はいずれも、キャンパス設計に関する既存のベスト プラクティスに基づいており、ここでは説明しません。IPv4 のセットアップを含む設定全体は「付録 — 設定リスト」（p.66）を参照してください。

- 6k-sb-1

```
interface GigabitEthernet4/1
 description to 6k-core-1
 dampening
 ip address 10.122.0.78 255.255.255.252
 no ip redirects
 no ip proxy-arp
 ip hello-interval eigrp 10 1
 ip hold-time eigrp 10 3
 ip authentication mode eigrp 10 md5
 ip authentication key-chain eigrp 10 eigrp
```

```
 load-interval 30
 carrier-delay msec 0
 mls qos trust dscp
!
interface GigabitEthernet4/2
 description to 6k-core-2
 dampening
 ip address 10.122.0.86 255.255.255.252
 no ip redirects
 no ip proxy-arp
 ip hello-interval eigrp 10 1
 ip hold-time eigrp 10 3
 ip authentication mode eigrp 10 md5
 ip authentication key-chain eigrp 10 eigrp
 load-interval 30
 carrier-delay msec 0
 mls qos trust dscp
!
interface TenGigabitEthernet1/1
 description to 6k-sb-2
 dampening
 ip address 10.122.0.93 255.255.255.252
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ip hello-interval eigrp 10 1
 ip hold-time eigrp 10 3
 ip authentication mode eigrp 10 md5
 ip authentication key-chain eigrp 10 eigrp
 load-interval 30
 carrier-delay msec 0
 ipv6 address 2001:DB8:CAFE:6505::A111:1010/64            #p2p link between SBM
                                                          #switches
 no ipv6 redirects
 ipv6 nd suppress-ra
 ipv6 cef
 ipv6 ospf network point-to-point
 ipv6 ospf hello-interval 1
 ipv6 ospf dead-interval 3
 ipv6 ospf 1 area 0
 mls qos trust dscp
```

- 6k-sb-2

```
interface GigabitEthernet4/1
 description to 6k-core-1
 dampening
 ip address 10.122.0.82 255.255.255.252
 no ip redirects
 no ip proxy-arp
 ip hello-interval eigrp 10 1
 ip hold-time eigrp 10 3
 ip authentication mode eigrp 10 md5
 ip authentication key-chain eigrp 10 eigrp
 load-interval 30
 carrier-delay msec 0
 mls qos trust dscp
!
interface GigabitEthernet4/2
 description to 6k-core-2
 dampening
 ip address 10.122.0.90 255.255.255.252
 no ip redirects
 no ip proxy-arp
```

```
 ip hello-interval eigrp 10 1
 ip hold-time eigrp 10 3
 ip authentication mode eigrp 10 md5
 ip authentication key-chain eigrp 10 eigrp
 load-interval 30
 carrier-delay msec 0
 mls qos trust dscp
!
interface TenGigabitEthernet1/1
 description to 6k-sb-1
 dampening
 ip address 10.122.0.94 255.255.255.252
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ip hello-interval eigrp 10 1
 ip hold-time eigrp 10 3
 ip authentication mode eigrp 10 md5
 ip authentication key-chain eigrp 10 eigrp
 load-interval 30
 carrier-delay msec 0
 ipv6 address 2001:DB8:CAFE:6505::B222:2020/64            #p2p link between SBM
                                                          #switches
 no ipv6 redirects
 ipv6 nd suppress-ra
 ipv6 cef
 ipv6 ospf network point-to-point
 ipv6 ospf hello-interval 1
 ipv6 ospf dead-interval 3
 ipv6 ospf 1 area 0
 mls qos trust dscp
```

トンネルの設定

ISATAP のトンネルおよびルーティング設定は、HME1 の場合とまったく同じです。次に設定を示しますが、前のセクションで示した情報の繰り返しを避けるために、ISATAP トンネリングおよびルーティングについての説明は省略します（HME1 の例の説明を参照してください）。

手動設定トンネルの設定は、サービス ブロック スイッチについてのみ示します。データセンター アグリゲーション スイッチ（6k-agg-1/6k-agg-2）におけるトンネル設定は、個々のアドレスを除いてサービス ブロックと同様です。

- 6k-sb-1

```
interface Loopback0
 description Tunnel source for 6k-agg-1
 ip address 10.122.10.9 255.255.255.255
!
interface Loopback1
 description Tunnel source for 6k-agg-2
 ip address 10.122.10.19 255.255.255.255
!
interface Loopback2
 description Tunnel source for ISATAP-VLAN2
 ip address 10.122.10.102 255.255.255.255
!
interface Loopback3
 description Tunnel source for ISATAP-VLAN3
 ip address 10.122.10.103 255.255.255.255
!
interface Tunnel0
 description tunnel to 6k-agg-1
```

```
 no ip address
 ipv6 address 2001:DB8:CAFE:6501::A111:1010/64
 no ipv6 redirects
 ipv6 cef
 ipv6 ospf network point-to-point
 ipv6 ospf hello-interval 1
 ipv6 ospf dead-interval 3
 ipv6 ospf 1 area 0
 tunnel source Loopback0
 tunnel destination 10.122.10.1                #10.122.10.1 is loopback0 on 6k-agg-1
 tunnel mode ipv6ip
!
interface Tunnel1
 description tunnel to 6k-agg-2
 no ip address
 ipv6 address 2001:DB8:CAFE:6502::A111:1010/64
 no ipv6 redirects
 ipv6 nd reachable-time 5000
 ipv6 cef
 ipv6 ospf network point-to-point
 ipv6 ospf hello-interval 1
 ipv6 ospf dead-interval 3
 ipv6 ospf 1 area 0
 tunnel source Loopback1
 tunnel destination 10.122.10.2                #10.122.10.2 is loopback0 on 6k-agg-2
 tunnel mode ipv6ip
!
interface Tunnel2
 description ISATAP VLAN2
 no ip address
 no ip redirects
 ipv6 address 2001:DB8:CAFE:2::/64 eui-64
 no ipv6 redirects
 no ipv6 nd suppress-ra
 ipv6 cef
 ipv6 ospf 1 area 2
 tunnel source Loopback2
 tunnel mode ipv6ip isatap
!
interface Tunnel3
 description ISATAP VLAN3
 no ip address
 no ip redirects
 ipv6 address 2001:DB8:CAFE:3::/64 eui-64
 no ipv6 redirects
 no ipv6 nd suppress-ra
 ipv6 cef
 ipv6 ospf 1 area 2
 tunnel source Loopback3
 tunnel mode ipv6ip isatap
!
ipv6 router ospf 1
 router-id 10.122.10.9
 log-adjacency-changes
 auto-cost reference-bandwidth 10000
 area 2 range 2001:DB8:CAFE:2::/64 cost 10
 area 2 range 2001:DB8:CAFE:3::/64 cost 10
 passive-interface Loopback0
 passive-interface Loopback1
 passive-interface Loopback2
 passive-interface Loopback3
 passive-interface Tunnel2
 passive-interface Tunnel3
 timers spf 1 5
```

- 6k-sb-2

```
interface Loopback0
 description Tunnel source for 6k-agg-1
 ip address 10.122.10.10 255.255.255.255
!
interface Loopback1
 description Tunnel source for 6k-agg-2
 ip address 10.122.10.20 255.255.255.255
!
interface Loopback2
 description Tunnel source for ISATAP-VLAN2
 ip address 10.122.10.102 255.255.255.255
 delay 1000
!
interface Loopback3
 description Tunnel source for ISATAP-VLAN3
 ip address 10.122.10.103 255.255.255.255
 delay 1000
!
interface Tunnel0
 description tunnel to 6k-agg-1
 no ip address
 load-interval 30
 ipv6 address 2001:DB8:CAFE:6503::B222:2020/64
 no ipv6 redirects
 ipv6 cef
 ipv6 ospf network point-to-point
 ipv6 ospf hello-interval 1
 ipv6 ospf dead-interval 3
 ipv6 ospf priority 255
 ipv6 ospf 1 area 0
 tunnel source Loopback0
 tunnel destination 10.122.10.11
 tunnel mode ipv6ip
!
interface Tunnel1
 description tunnel to 6k-agg-2
 no ip address
 load-interval 30
 ipv6 address 2001:DB8:CAFE:6504::B222:2020/64
 no ipv6 redirects
 ipv6 cef
 ipv6 ospf network point-to-point
 ipv6 ospf hello-interval 1
 ipv6 ospf dead-interval 3
 ipv6 ospf 1 area 0
 tunnel source Loopback1
 tunnel destination 10.122.10.12
 tunnel mode ipv6ip
!
interface Tunnel2
 description ISATAP VLAN2
 no ip address
 ip access-group 100 in
 no ip redirects
 load-interval 30
 ipv6 address 2001:DB8:CAFE:2::/64 eui-64
 no ipv6 redirects
 no ipv6 nd suppress-ra
 ipv6 cef
 ipv6 ospf 1 area 2
 tunnel source Loopback2
```

```
 tunnel mode ipv6ip isatap
!
interface Tunnel3
 description ISATAP VLAN3
 no ip address
 no ip redirects
 load-interval 30
 ipv6 address 2001:DB8:CAFE:3::/64 eui-64
 no ipv6 redirects
 no ipv6 nd suppress-ra
 ipv6 cef
 ipv6 ospf 1 area 2
 tunnel source Loopback3
 tunnel mode ipv6ip isatap
!
ipv6 router ospf 1
 router-id 10.122.10.10
 log-adjacency-changes
 auto-cost reference-bandwidth 10000
 area 2 range 2001:DB8:CAFE:2::/64 cost 20
 area 2 range 2001:DB8:CAFE:3::/64 cost 20
 passive-interface Loopback0
 passive-interface Loopback1
 passive-interface Loopback2
 passive-interface Loopback3
 passive-interface Tunnel2
 passive-interface Tunnel3
 timers spf 1 5
```

QoS の設定

SBM には、「デュアルスタック モデル — 実装」（p.33）および「まとめ」（p.63）に記載されている QoS 設定と説明が適用されます。HME1 のケースで示した設定例から唯一の変更点は、分類とマーキングのポリシーを適用するインターフェイスに関するものです。SBM では、6k-agg-1 および 6k-agg-2 への手動設定トンネルの出力側でサービス ポリシーを適用します。

6k-sb-1 を例にすると、サービス ポリシーは Tunnel0 および Tunnel1 に適用します。

```
interface Tunnel0
 description tunnel to 6k-agg-1
 service-policy output IPv6-ISATAP-MARK
!
interface Tunnel1
 description tunnel to 6k-agg-2
 service-policy output IPv6-ISATAP-MARK
```

インフラストラクチャ セキュリティの設定

SBM には、「デュアルスタック モデル — 実装」（p.33）および「インフラストラクチャ セキュリティの設定」（p.55）に記載されているセキュリティの考慮事項と設定がそのまま適用されます。

まとめ

このマニュアルでは、キャンパス ネットワークで IPv6 サービスを提供するための各種アーキテクチャを分析しました。説明した各モデルは、この環境に IPv6 を導入するための唯一の方法というわけではなく、環境、導入スケジュール、および目標とするサービスの条件に合わせて利用できる選択肢です。

表 8 に、このマニュアルで説明した各モデルの利点と懸念点を要約します。

表 8　　各モデルの利点と懸念点

モデル	利点	懸念点
デュアルスタック モデル（DSM）	トンネリングが不要 IPv4 に依存しない（ルーティング、QoS、HA、マルチキャスト、セキュリティ、および管理が個別） IPv6 ユニキャストおよびマルチキャストにおける優れたパフォーマンスと最高のアベイラビリティ スケーラブル	ハードウェアで IPv6 対応のキャンパス スイッチング機器が必要 デュアル プロトコルのサポートに関連する運用上の課題 ― トレーニングや管理ツール
ハイブリッド モデル例 1（HME1）	IPv4 のみに対応する既存のキャンパス機器の大部分を使用可能（アクセスおよびディストリビューション レイヤ） IPv6 サービスの配信をユーザ単位またはアプリケーション単位で制御 ISATAP トンネル上での IPv6 アクセスにハイアベイラビリティを提供	トンネリングが必要なため、運用と管理の負担が増加 スケール ファクタが不明： • 使用できる ISATAP トンネルは何個までか？ • ISATAP トンネルごとのホスト数は？ • ホスト / サービスのアクセスにおけるパフォーマンスの低下は？ IPv6 マルチキャストがサポートされない コア レイヤが IPv6 トンネル用のアクセス レイヤになる IPv6 対応のホストと ISATAP 設定が必要

表 8　　各モデルの利点と懸念点（続き）

モデル	利点	懸念点
ハイブリッド モデル例 2（HME2）	コア レイヤをデュアルスタックにする必要がない コアをアップグレード中の場合、または IPv6 ハードウェアのサポートが限られている場合の一時的なソリューション IPv6 マルチキャストをサポート（DSM ほどのパフォーマンスとスケーラビリティはない） 設定されたトンネル上での IPv6 接続にハイアベイラビリティを提供	トンネリングが必要なため、運用と管理の負担が増加 大規模なネットワークで、p2p の手動設定トンネルを大量に使用すると、スケールと管理に問題が生じる可能性がある IPv6 対応のホストが必要
サービス ブロック モデル（SBM）	IPv6 対応サービスを非常に迅速に展開可能 既存のキャンパス インフラストラクチャの変更が不要 IPv6 サービスの配信をユーザ単位またはアプリケーション単位で制御 ISATAP トンネル上での IPv6 アクセスにハイ アベイラビリティを提供 設定されたトンネル上での IPv6 接続にハイ アベイラビリティを提供	ハードウェアで IPv6 対応の新しいキャンパス スイッチが必要 トンネリングが（広範囲で）必要なため、運用と管理の負担が増加 多くのスケール ファクタが不明（HME1 を参照） ISATAP トンネルで IPv6 マルチキャストがサポートされない IPv6 対応のホストと ISATAP 設定が必要

今後の作業

このマニュアルは、エンタープライズ カスタマー向けに IPv6 の基本的な実装ガイダンスを提供することを目的とした一連の資料の 1 つです。ブランチ、WAN、データセンター、およびエンタープライズ エッジでの IPv6 導入について分析した、同様のマニュアルも発行が予定されています。

このマニュアルは「進行型のマニュアル」であり、機能の完成度に応じて変更される予定です。ただし、最終目標はすべてのエンタープライズ アーキテクチャ設計ガイドに、IPv6 を 1 つのベースライン コンポーネントとして完全に統合することです。そうすれば、さまざまなテクノロジーや設計について個別の資料を参照するのではなく、エンタープライズのあらゆる分野に関する最新の設計ベスト プラクティスを、1 つの資料で学習できるようになります。一連のエンタープライズ アーキテクチャ設計ガイドは、次の URL を参照してください。
http://www.cisco.com/go/srnd

その他の関連資料

このマニュアルでは、IPv6 のテクノロジーやプロトコルのさまざまな側面をよく理解する必要があることを随所で指摘しています。IPv6 の実装には、セキュリティ、QoS、アベイラビリティ、管理、IT トレーニング、アプリケーション サポートなど、設計に関する多くの考慮事項があります。

IPv6、設計に関するシスコの推奨事項、製品とソリューション、および業界の活動について詳しく記載された多くの資料のうち一部分を次に示します。

- シスコ独自のリンク
  - 『*Deploying IPv6 Networks*』Ciprian P. Popoviciu、Eric Levy-Abegnoli、Patrick Grossetete 著（ISBN-10:1-58705-210-5、ISBN-13:978-1-58705-210-1）— http://www.ciscopress.com/bookstore/product.asp?isbn=1587052105&rl=1
  - Cisco IPv6 CCO ホームページ — http://www.cisco.com/ipv6
  - 『*Cisco Solution Reference Network Design (SRND) Guides*』— http://www.cisco.com/go/srnd
  - 『*Cisco Solution Reference Network Design (SRND) Campus Guides*』— http://www.cisco.com/en/US/netsol/ns656/networking_solutions_design_guidances_list.html#anchor2
  - 『*Enterprise QoS SRND*』— http://www.cisco.com/application/pdf/en/us/guest/netsol/ns432/c649/ccmigration_09186a008049b062.pdf
  - 『*Cisco IOS IPv6 Configuration Guide, Release 12.4*』— http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124cg/hipv6_c/index.htm
  - 『*Catalyst 6500 Series Cisco IOS Software Configuration Guide, 12.2SX*』— http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/swcg/index.htm
  - 『*Catalyst 3750 Switch Software Configuration Guide, 12.2(25)SEE*』— http://www.cisco.com/univercd/cc/td/doc/product/lan/cat3750/12225see/scg/index.htm
  - 『*Cisco Network Virtualization*』— http://www.cisco.com/en/US/netsol/ns658/networking_solutions_package.html
  - 『*Cisco IOS IPv6 Traffic Filter Configurations*』— http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/ipv6_c/v6_tffw.htm
  - 『*Securing Cisco Routers Online Training and Documentation*』— http://www.cisco.com/web/about/security/security_services/ciag/workforce_development/securing_cisco_routers.html
- Microsoft の IPv6 リンク
  - Microsoft IPv6 ホーム — http://www.microsoft.com/technet/itsolutions/network/ipv6/default.mspx
  - Microsoft–『*Cisco ISATAP White Paper*』— http://www.microsoft.com/downloads/details.aspx?FamilyId=B8F50E07-17BF-4B5C-A1F9-5A09E2AF698B&displaylang=en
  - Microsoft TechNet–『*Teredo Overview*』— http://www.microsoft.com/technet/prodtechnol/winxppro/maintain/teredo.mspx
- IPv6 に関する業界のリンク
  - National Security Agency–『*Security for IPv6 on Cisco Routers*』— http://www.nsa.gov/notices/notic00004.cfm?Address=/snac/routers/I33-002R-06.pdf
  - IETF IPv6 オペレーションズ ワーキング グループ — http://www.ietf.org/html.charters/v6ops-charter.html
  - go6 IPv6 ポータル –IPv6 ナレッジ センター — http://wiki.go6.net/index.php?title=Main_Page
  - 6NET– 大規模な国際的 IPv6 パイロット ネットワーク — http://www.6net.org/
  - IETF IPv6 ワーキング グループ — http://www.ietf.org/html.charters/ipv6-charter.html
  - IETF IPv6 オペレーションズ ワーキング グループ — http://www.ietf.org/html.charters/v6ops-charter.html
  - 『*Internet Protocol, Version 6 (IPv6) Specification*』— http://www.ietf.org/rfc/rfc2460.txt
  - 『*Neighbor Discovery for IPv6*』— http://www.ietf.org/rfc/rfc2461.txt

- 『*IPv6 Stateless Address Autoconfiguration*』— http://www.ietf.org/rfc/rfc2462.txt
- 『*Transmission of IPv6 Packets over Ethernet Networks*』— http://www.ietf.org/rfc/rfc2464.txt
- 『*Transition Mechanisms for IPv6 Hosts and Routers*』— http://www.ietf.org/rfc/rfc2893.txt
- 『*Privacy Extensions for Stateless Address Autoconfiguration in IPv6*』— http://www.ietf.org/rfc/rfc3041.txt
- 『*Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)*』— http://www.ietf.org/rfc/rfc4214.txt
- 『*IPv6 Addressing Architecture*』— http://www.ietf.org/rfc/rfc4291.txt
- 『*Internet Control Message Protocol (ICMPv6) for Internet Protocol Version 6 (IPv6) Specification*』— http://www.ietf.org/rfc/rfc4443.txt
- North American IPv6 Task Force–『*IPv6 Security Technology Paper*』— http://www.ipv6forum.org/dl/white/NAv6TF_Security_Report.pdf

付録 — 設定リスト

ここでは、このマニュアルで説明されている 3 つのモデル（DSM、HME1、および SBM）の設定全体を示します。一部のスイッチ設定は、このマニュアルで説明されているすべてのモデルに共通であるため、1 回しか示しません。

簡潔さを保つために、使用しないインターフェイスやシャットダウンされたインターフェイスは、設定では省略しています。

デュアルスタック モデル（DSM）

3750-acc-1

```
version 12.2
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service password-encryption
service sequence-numbers
!
hostname 3750-acc-1
!
logging count
logging buffered 8192 debugging
logging rate-limit 5
no logging console
enable secret 5 $1$RPWW$KR0qkU1kW0a7Pd1svvhgB.
!
username cisco privilege 15 secret 5 $1$KNSF$3XavijOuoVCq68RASxTYD1
no aaa new-model
clock timezone mst -7
switch 1 provision ws-c3750g-24ts
vtp domain ese-dc
vtp mode transparent
udld enable

udld message time 7

ip subnet-zero
```

```
no ip source-route
ip icmp rate-limit unreachable 2000
ip telnet source-interface Vlan2
no ip domain-lookup
ip domain-name cisco.com
ip dhcp smart-relay
!
ip dhcp snooping vlan 2
ip dhcp snooping database flash:dhcp.txt
ip dhcp snooping database timeout 10
ip dhcp snooping
ip ftp source-interface Vlan2
ip ftp username cisco
ip ftp password 7 120B0419150E1E
ip tftp source-interface Vlan2
ip ssh time-out 60
ip ssh authentication-retries 2
ip ssh source-interface Vlan2
ip ssh version 2
ip arp inspection vlan 2
ip arp inspection validate src-mac
ip arp inspection log-buffer entries 100
ip arp inspection log-buffer logs 20 interval 120
login block-for 30 attempts 3 within 200
login delay 2
ipv6 mld snooping
!
mls qos map policed-dscp  0 10 18 24 25 34 to 8
mls qos map cos-dscp 0 8 16 24 32 46 48 56
mls qos srr-queue output cos-map queue 1 threshold 3  5
mls qos srr-queue output cos-map queue 2 threshold 1  2 4
mls qos srr-queue output cos-map queue 2 threshold 2  3
mls qos srr-queue output cos-map queue 2 threshold 3  6 7
mls qos srr-queue output cos-map queue 3 threshold 3  0
mls qos srr-queue output cos-map queue 4 threshold 3  1
mls qos srr-queue output dscp-map queue 1 threshold 3  46
mls qos srr-queue output dscp-map queue 2 threshold 1  16 18 20 22 25 32 34 36
mls qos srr-queue output dscp-map queue 2 threshold 1  38
mls qos srr-queue output dscp-map queue 2 threshold 2  24 26
mls qos srr-queue output dscp-map queue 2 threshold 3  48 56
mls qos srr-queue output dscp-map queue 3 threshold 3  0
mls qos srr-queue output dscp-map queue 4 threshold 1  8
mls qos srr-queue output dscp-map queue 4 threshold 3  10 12 14
mls qos queue-set output 1 threshold 2 70 80 100 100
mls qos queue-set output 1 threshold 4 40 100 100 100
mls qos
!
crypto pki trustpoint TP-self-signed-3669881984
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-3669881984
 revocation-check none
 rsakeypair TP-self-signed-3669881984
!
!
 crypto ca certificate chain TP-self-signed-3669881984
  certificate self-signed 01
   30820299 30820202 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
   57312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274
   69666963 6174652D 33363639 38383139 38343124 30220609 2A864886 F70D0109
   02161533 3735302D 65646765 2D312E63 6973636F 2E636F6D 301E170D 39333033
   30313030 30313533 5A170D32 30303130 31303030 3030305A 3057312F 302D0603
   55040313 26494F53 2D53656C 662D5369 676E6564 2D436572 74696669 63617465
   2D333636 39383831 39383431 24302206 092A8648 86F70D01 09021615 33373530
   2D656467 652D312E 63697363 6F2E636F 6D30819F 300D0609 2A864886 F70D0101
```

```
   01050003 818D0030 81890281 8100BF7D E793E21B 6C1F75C2 16AAFF9F C110D038
   2D6D1DC9 04758DB8 7B3AD4C9 9F36A3B1 54983BEC 10FEA2D4 151D2783 5765C58A
   A95E6364 CCBCF7F9 F4750437 AB8C00BF EFD54E88 6F650A5C 9563A309 247C6070
   DC38A870 DEC5D4DA 765AD7A4 274B7649 36D876CA E28CF66C 77335F90 949DF258
   E3E019BD 5E6801EC 9E15F980 C13D0203 010001A3 75307330 0F060355 1D130101
   FF040530 030101FF 30200603 551D1104 19301782 15333735 302D6564 67652D31
   2E636973 636F2E63 6F6D301F 0603551D 23041830 168014E0 18682CE1 D6A3EF2C
   32A7C8D5 4DAFB9AA F11A0030 1D060355 1D0E0416 0414E018 682CE1D6 A3EF2C32
   A7C8D54D AFB9AAF1 1A00300D 06092A86 4886F70D 01010405 00038181 00755909
   C99DEB7F E05FC2A3 482558FA 33C292AE 7E4543E3 5BD6F32F 1D671B97 BC45B73B
   85E954ED 7FC58F90 23A38132 24216CDB C978B3DD 9BCBC48E 519D01BF F4CEBB82
   07834C2D D82CA163 8E638214 5B5C277D 5E7DD52E 56172675 BD563769 590E4DC6
   39AD9BF8 CDBBA241 E5E2C666 5CAE912E 40DC2150 A1CE39B4 D8101D33 A8
   quit
!
!
errdisable recovery cause link-flap
errdisable recovery interval 60
no file verify auto
!
spanning-tree mode rapid-pvst
spanning-tree loopguard default
spanning-tree portfast bpduguard default
no spanning-tree optimize bpdu transmission
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
vlan 2
 name ACCESS-DATA-2
!
class-map match-all DVLAN-PC-VIDEO
  match access-group name DVLAN-PC-VIDEO
class-map match-all DVLAN-Transactional-Data
  match access-group name DVLAN-Transactional-Data
class-map match-all DVLAN-Mission-Critical-Data
  match access-group name DVLAN-Mission-Critical-Data
class-map match-all DVLAN-Bulk-Data
  match access-group name DVLAN-Bulk-Data
!
!
policy-map DATA
  class DVLAN-PC-VIDEO
   set dscp af41
    police 48000 8000 exceed-action policed-dscp-transmit
  class DVLAN-Mission-Critical-Data
   set dscp 25
    police 5000000 8000 exceed-action policed-dscp-transmit
  class DVLAN-Transactional-Data
   set dscp af21
    police 5000000 8000 exceed-action policed-dscp-transmit
  class DVLAN-Bulk-Data
   set dscp af11
    police 5000000 8000 exceed-action policed-dscp-transmit
!
!
!
interface Null0
 no ip unreachables
!
interface GigabitEthernet1/0/5
 description to PC-DATA-ONLY
 switchport access vlan 2
 switchport mode access
```

```
 switchport port-security maximum 3
 switchport port-security
 switchport port-security aging time 2
 switchport port-security violation restrict
 switchport port-security aging type inactivity
 ip arp inspection limit rate 100
 service-policy input DATA
 load-interval 30
 srr-queue bandwidth share 1 70 25 5
 srr-queue bandwidth shape  3  0  0  0
 priority-queue out
 spanning-tree portfast
 spanning-tree bpduguard enable
 ip verify source
 ip dhcp snooping limit rate 100
!
interface GigabitEthernet1/0/25
 description TRUNK TO 6k-dist-1
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 2
 switchport mode trunk
 switchport nonegotiate
 switchport port-security aging time 10
 ip arp inspection trust
 load-interval 30
 srr-queue bandwidth share 1 70 25 5
 srr-queue bandwidth shape  3  0  0  0
 priority-queue out
 no cdp enable
 ip dhcp snooping limit rate 10
 ip dhcp snooping trust
!
interface GigabitEthernet1/0/26
 description TRUNK TO 6k-dist-2
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 2
 switchport mode trunk
 switchport nonegotiate
 switchport port-security aging time 10
 ip arp inspection trust
 load-interval 30
 srr-queue bandwidth share 1 70 25 5
 srr-queue bandwidth shape  3  0  0  0
 priority-queue out
 no cdp enable
 ip dhcp snooping limit rate 10
 ip dhcp snooping trust
!
interface Vlan2
 ip address 10.120.2.4 255.255.255.0
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 no ip route-cache
 no ip mroute-cache
 ipv6 address 2001:DB8:CAFE:2::CAC1:3750/64
 no ipv6 redirects
!
ip default-gateway 10.120.2.1
ip classless
no ip http server
no ip http secure-server
!
!
```

```
ip access-list extended DVLAN-Bulk-Data
 permit tcp any any eq 143
 permit tcp any any eq 220
ip access-list extended DVLAN-Mission-Critical-Data
 permit tcp any any range 3200 3203
 permit tcp any any eq 3600
 permit tcp any any range 2000 2002
ip access-list extended DVLAN-PC-VIDEO
 permit udp any any range 16384 32767
ip access-list extended DVLAN-Transactional-Data
 permit tcp any any eq 1352
ip access-list extended MGMT-IN-v4
 permit tcp 10.120.0.0 0.0.255.255 any log-input
 permit tcp 10.121.0.0 0.0.255.255 any log-input
 permit tcp 10.122.0.0 0.0.255.255 any log-input
 deny   ip any any log-input
!
logging source-interface Vlan2
logging 10.121.11.9
no cdp run
ipv6 route ::/0 2001:DB8:CAFE:2::1
!
snmp-server contact John Doe - ipv6rocks@cisco.com
snmp-server group IPv6-ADMIN v3 auth write v1default
!
ipv6 access-list MGMT-IN
 remark Permit MGMT only to VLAN2
 permit tcp 2001:DB8:CAFE::/48 host 2001:DB8:CAFE:2::CAC1:3750 log-input
 deny ipv6 any any log-input
!
control-plane
!
banner login ^C
Unauthorized access to this device and/or network is prohibited.
^C
!
line con 0
 session-timeout 3
 password 7 06140E2F4B4B1B
 logging synchronous
 login local
 transport output telnet ssh
line vty 0 4
 session-timeout 3
 password 7 06140E2F4B4B1B
 ipv6 access-class MGMT-IN in
 logging synchronous
 login local
 exec prompt timestamp
 transport input telnet ssh
line vty 5 15
 session-timeout 3
 password 7 0101070A5C0E14
 ipv6 access-class MGMT-IN in
 logging synchronous
 login local
 exec prompt timestamp
 transport input telnet ssh
!
!
end
```

3750-acc-2

```
version 12.2
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service password-encryption
service sequence-numbers
!
hostname 3750-acc-2
!
logging count
logging buffered 8192 debugging
logging rate-limit 5
no logging console
enable secret 5 $1$2Nvb$4.Zz3eHzz2KgCFzc12pLh.
!
username cisco privilege 15 secret 5 $1$/S8z$0ek0VBA.QWuKR8R6U1.Ly0
no aaa new-model
clock timezone mst -7
switch 1 provision ws-c3750g-24ts
vtp domain ese-dc
vtp mode transparent
udld enable

udld message time 7

ip subnet-zero
no ip source-route
ip icmp rate-limit unreachable 2000
ip telnet source-interface Vlan3
no ip domain-lookup
ip domain-name cisco.com
ip dhcp smart-relay
!
ip dhcp snooping vlan 3
ip dhcp snooping database flash:dhcp.txt
ip dhcp snooping database timeout 10
ip dhcp snooping
ip ftp source-interface Vlan3
ip ftp username cisco
ip ftp password 7 111B180B101719
ip tftp source-interface Vlan3
ip ssh time-out 60
ip ssh authentication-retries 2
ip ssh source-interface Vlan3
ip ssh version 2
ip arp inspection vlan 3
ip arp inspection validate src-mac
ip arp inspection log-buffer entries 100
ip arp inspection log-buffer logs 20 interval 120
login block-for 30 attempts 3 within 200
login delay 2
ipv6 mld snooping
!
mls qos map policed-dscp  0 10 18 24 25 34 to 8
mls qos map cos-dscp 0 8 16 24 32 46 48 56
mls qos srr-queue output cos-map queue 1 threshold 3  5
mls qos srr-queue output cos-map queue 2 threshold 1  2 4
mls qos srr-queue output cos-map queue 2 threshold 2  3
mls qos srr-queue output cos-map queue 2 threshold 3  6 7
```

```
mls qos srr-queue output cos-map queue 3 threshold 3  0
mls qos srr-queue output cos-map queue 4 threshold 3  1
mls qos srr-queue output dscp-map queue 1 threshold 3  46
mls qos srr-queue output dscp-map queue 2 threshold 1  16 18 20 22 25 32 34 36
mls qos srr-queue output dscp-map queue 2 threshold 1  38
mls qos srr-queue output dscp-map queue 2 threshold 2  24 26
mls qos srr-queue output dscp-map queue 2 threshold 3  48 56
mls qos srr-queue output dscp-map queue 3 threshold 3  0
mls qos srr-queue output dscp-map queue 4 threshold 1  8
mls qos srr-queue output dscp-map queue 4 threshold 3  10 12 14
mls qos queue-set output 1 threshold 2 70 80 100 100
mls qos queue-set output 1 threshold 4 40 100 100 100
mls qos
!
errdisable recovery cause link-flap
errdisable recovery interval 60
no file verify auto
!
spanning-tree mode rapid-pvst
spanning-tree loopguard default
spanning-tree portfast bpduguard default
no spanning-tree optimize bpdu transmission
spanning-tree extend system-id
!
vlan internal allocation policy ascending
vlan dot1q tag native
!
vlan 3
 name ACCESS-DATA-3
!
class-map match-all DVLAN-PC-VIDEO
  match access-group name DVLAN-PC-VIDEO
class-map match-all DVLAN-Transactional-Data
  match access-group name DVLAN-Transactional-Data
class-map match-all DVLAN-Mission-Critical-Data
  match access-group name DVLAN-Mission-Critical-Data
class-map match-all DVLAN-Bulk-Data
  match access-group name DVLAN-Bulk-Data
!
!
policy-map DATA
  class DVLAN-PC-VIDEO
   set dscp af41
    police 48000 8000 exceed-action policed-dscp-transmit
  class DVLAN-Mission-Critical-Data
   set dscp 25
    police 5000000 8000 exceed-action policed-dscp-transmit
  class DVLAN-Transactional-Data
   set dscp af21
    police 5000000 8000 exceed-action policed-dscp-transmit
  class DVLAN-Bulk-Data
   set dscp af11
    police 5000000 8000 exceed-action policed-dscp-transmit
!
interface Null0
 no ip unreachables
!
interface GigabitEthernet1/0/5
 description to PC-DATA-ONLY
 switchport access vlan 3
 switchport mode access
 switchport port-security maximum 3
 switchport port-security
 switchport port-security aging time 2
```

```
 switchport port-security violation restrict
 switchport port-security aging type inactivity
 ip arp inspection limit rate 100
 service-policy input DATA
 load-interval 30
 srr-queue bandwidth share 1 70 25 5
 srr-queue bandwidth shape  3  0  0  0
 priority-queue out
 spanning-tree portfast
 spanning-tree bpduguard enable
 ip verify source
 ip dhcp snooping limit rate 100
!
interface GigabitEthernet1/0/25
 description TRUNK TO 6k-dist-1
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 3
 switchport mode trunk
 switchport nonegotiate
 switchport port-security aging time 10
 ip arp inspection trust
 load-interval 30
 srr-queue bandwidth share 1 70 25 5
 srr-queue bandwidth shape  3  0  0  0
 priority-queue out
 no cdp enable
 spanning-tree guard loop
 ip dhcp snooping limit rate 10
 ip dhcp snooping trust
!
interface GigabitEthernet1/0/26
 description TRUNK TO 6k-dist-2
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 3
 switchport mode trunk
 switchport nonegotiate
 switchport port-security aging time 10
 ip arp inspection trust
 load-interval 30
 srr-queue bandwidth share 1 70 25 5
 srr-queue bandwidth shape  3  0  0  0
 priority-queue out
 no cdp enable
 spanning-tree guard loop
 ip dhcp snooping limit rate 10
 ip dhcp snooping trust
!
interface Vlan3
 ip address 10.120.3.4 255.255.255.0
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 no ip route-cache
 no ip mroute-cache
 ipv6 address 2001:DB8:CAFE:3::CAC2:3750/64
 no ipv6 redirects
!
ip default-gateway 10.120.3.1
ip classless
no ip http server
no ip http secure-server
!
ip access-list extended DVLAN-Bulk-Data
 permit tcp any any eq 143
```

```
 permit tcp any any eq 220
ip access-list extended DVLAN-Mission-Critical-Data
 permit tcp any any range 3200 3203
 permit tcp any any eq 3600
 permit tcp any any range 2000 2002
ip access-list extended DVLAN-PC-VIDEO
 permit udp any any range 16384 32767
ip access-list extended DVLAN-Transactional-Data
 permit tcp any any eq 1352
ip access-list extended MGMT-IN-v4
 permit tcp 10.120.0.0 0.0.255.255 any log-input
 permit tcp 10.121.0.0 0.0.255.255 any log-input
 permit tcp 10.122.0.0 0.0.255.255 any log-input
 deny   ip any any log-input
!
logging source-interface Vlan3
logging 10.121.11.9
no cdp run
ipv6 route ::/0 2001:DB8:CAFE:3::1
!
snmp-server contact John Doe - ipv6rocks@cisco.com
snmp-server group IPv6-ADMIN v3 auth write v1default
!
ipv6 access-list MGMT-IN
 remark Permit MGMT only to VLAN2
 permit tcp 2001:DB8:CAFE::/48 host 2001:DB8:CAFE:3::CAC2:3750 log-input
 deny ipv6 any any log-input
!
control-plane
!
banner login ^C
Unauthorized access to this device and/or network is prohibited.
^C
!
line con 0
 session-timeout 3
 password 7 00161208035E19
 logging synchronous
 login local
 transport output telnet ssh
line vty 0 4
 session-timeout 3
 password 7 0519070126495C
 ipv6 access-class MGMT-IN in
 logging synchronous
 login local
 exec prompt timestamp
 transport input telnet ssh
line vty 5 15
 session-timeout 3
 password 7 071D2042490C0B
 ipv6 access-class MGMT-IN in
 logging synchronous
 login local
 exec prompt timestamp
 transport input telnet ssh
!
end
```

6k-dist-1

```
upgrade fpd auto
```

```
version 12.2
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service password-encryption
service sequence-numbers
service counters max age 5
!
hostname 6k-dist-1
!
boot system flash sup-bootdisk:s3223-adventerprisek9_wan-mz.122-18.SXF5.bin
logging buffered 64000 debugging
logging rate-limit 5
no logging console
enable secret 5 $1$EZB7$nbqNvH9QH4qo3zpGsZog6/
!
username cisco privilege 15 secret 5 $1$VwbR$aXCTEAusOPhpmcfg7nOn01
no aaa new-model
clock timezone mst -7
ip subnet-zero
no ip source-route
ip icmp rate-limit unreachable 2000
!
!
!
ip ftp source-interface Loopback0
ip ftp username cisco
ip ftp password 7 121A0C041104
ip tftp source-interface Loopback0
no ip bootp server
ip telnet source-interface Loopback0
ip ssh time-out 30
ip ssh authentication-retries 2
ip ssh source-interface Loopback0
ip ssh version 2
no ip domain-lookup
ip domain-name cisco.com
ipv6 unicast-routing
ipv6 mfib hardware-switching replication-mode ingress
ipv6 multicast-routing
udld enable

udld message time 7

vtp domain ese-dc
vtp mode transparent
mls ip cef load-sharing full
mls ip multicast flow-stat-timer 9
no mls flow ip
no mls flow ipv6
mls qos
mls rate-limit unicast ip icmp unreachable acl-drop 0
no mls acl tcam share-global
mls cef error action freeze
!
key chain eigrp
 key 100
  key-string 7 1111
!
redundancy
 mode sso
 main-cpu
```

```
  auto-sync running-config
!
spanning-tree mode rapid-pvst
spanning-tree loopguard default
no spanning-tree optimize bpdu transmission
spanning-tree extend system-id
spanning-tree vlan 2-3 priority 24576
environment temperature-controlled
system flowcontrol bus auto
diagnostic cns publish cisco.cns.device.diag_results
diagnostic cns subscribe cisco.cns.device.diag_commands
!
vlan internal allocation policy descending
vlan dot1q tag native
vlan access-log ratelimit 2000
!
vlan 2
 name ACCESS-DATA-2
!
vlan 3
 name ACCESS-DATA-3
!
interface Loopback0
 ip address 10.122.10.9 255.255.255.255
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ipv6 address 2001:DB8:CAFE:6507::A111:1010/128
 no ipv6 redirects
 ipv6 ospf 1 area 0
!
interface Null0
 no ip unreachables
!
interface TenGigabitEthernet1/1
 description to 6k-dist-2
 dampening
 ip address 10.122.0.93 255.255.255.252
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ip hello-interval eigrp 10 1
 ip hold-time eigrp 10 3
 ip authentication mode eigrp 10 md5
 ip authentication key-chain eigrp 10 eigrp
 load-interval 30
 carrier-delay msec 0
 ipv6 address 2001:DB8:CAFE:7004::A111:1010/64
 no ipv6 redirects
 ipv6 nd suppress-ra
 ipv6 cef
 ipv6 ospf network point-to-point
 ipv6 ospf hello-interval 1
 ipv6 ospf dead-interval 3
 ipv6 ospf 1 area 2
 wrr-queue bandwidth 5 25 70
 wrr-queue queue-limit 5 25 40
 wrr-queue random-detect min-threshold 1 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 3 50 60 70 80 90 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 2 100 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 3 60 70 80 90 100 100 100 100
 wrr-queue cos-map 1 1 1
```

```
 wrr-queue cos-map 2 1 0
 wrr-queue cos-map 3 1 4
 wrr-queue cos-map 3 2 2
 wrr-queue cos-map 3 3 3
 wrr-queue cos-map 3 4 6
 wrr-queue cos-map 3 5 7
 mls qos trust dscp
!
interface GigabitEthernet3/1
 description to 3750-acc-1
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 2
 switchport mode trunk
 switchport nonegotiate
 no ip address
 load-interval 30
 wrr-queue bandwidth 5 25 70
 wrr-queue queue-limit 5 25 40
 wrr-queue random-detect min-threshold 1 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 3 50 60 70 80 90 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 2 100 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 3 60 70 80 90 100 100 100 100
 wrr-queue cos-map 1 1 1
 wrr-queue cos-map 2 1 0
 wrr-queue cos-map 3 1 4
 wrr-queue cos-map 3 2 2
 wrr-queue cos-map 3 3 3
 wrr-queue cos-map 3 4 6
 wrr-queue cos-map 3 5 7
 mls qos trust dscp
 no cdp enable
 spanning-tree guard root
!
interface GigabitEthernet3/2
 description to 3750-acc-2
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 3
 switchport mode trunk
 switchport nonegotiate
 no ip address
 load-interval 30
 wrr-queue bandwidth 5 25 70
 wrr-queue queue-limit 5 25 40
 wrr-queue random-detect min-threshold 1 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 3 50 60 70 80 90 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 2 100 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 3 60 70 80 90 100 100 100 100
 wrr-queue cos-map 1 1 1
 wrr-queue cos-map 2 1 0
 wrr-queue cos-map 3 1 4
 wrr-queue cos-map 3 2 2
 wrr-queue cos-map 3 3 3
 wrr-queue cos-map 3 4 6
 wrr-queue cos-map 3 5 7
 mls qos trust dscp
 no cdp enable
 spanning-tree guard root
!
```

```
interface GigabitEthernet4/1
 description to 6k-core-1
 dampening
 ip address 10.122.0.78 255.255.255.252
 no ip redirects
 no ip proxy-arp
 ip hello-interval eigrp 10 1
 ip hold-time eigrp 10 3
 ip authentication mode eigrp 10 md5
 ip authentication key-chain eigrp 10 eigrp
 ip summary-address eigrp 10 10.120.0.0 255.255.0.0 5
 load-interval 30
 carrier-delay msec 0
 ipv6 address 2001:DB8:CAFE:7000::A111:1010/64
 no ipv6 redirects
 ipv6 nd suppress-ra
 ipv6 cef
 ipv6 ospf network point-to-point
 ipv6 ospf hello-interval 1
 ipv6 ospf dead-interval 3
 ipv6 ospf 1 area 0
 wrr-queue bandwidth 30 70
 wrr-queue queue-limit 40 30
 wrr-queue random-detect min-threshold 1 40 80
 wrr-queue random-detect min-threshold 2 70 80
 wrr-queue random-detect max-threshold 1 80 100
 wrr-queue random-detect max-threshold 2 80 100
 wrr-queue cos-map 1 1 1
 wrr-queue cos-map 1 2 0
 wrr-queue cos-map 2 1 2 3 4
 wrr-queue cos-map 2 2 6 7
 mls qos trust dscp
!
interface GigabitEthernet4/2
 description to 6k-core-2
 dampening
 ip address 10.122.0.86 255.255.255.252
 no ip redirects
 no ip proxy-arp
 ip hello-interval eigrp 10 1
 ip hold-time eigrp 10 3
 ip authentication mode eigrp 10 md5
 ip authentication key-chain eigrp 10 eigrp
 ip summary-address eigrp 10 10.120.0.0 255.255.0.0 5
 load-interval 30
 carrier-delay msec 0
 ipv6 address 2001:DB8:CAFE:7001::A111:1010/64
 no ipv6 redirects
 ipv6 nd suppress-ra
 ipv6 cef
 ipv6 ospf network point-to-point
 ipv6 ospf hello-interval 1
 ipv6 ospf dead-interval 3
 ipv6 ospf 1 area 0
 wrr-queue bandwidth 30 70
 wrr-queue queue-limit 40 30
 wrr-queue random-detect min-threshold 1 40 80
 wrr-queue random-detect min-threshold 2 70 80
 wrr-queue random-detect max-threshold 1 80 100
 wrr-queue random-detect max-threshold 2 80 100
 wrr-queue cos-map 1 1 1
 wrr-queue cos-map 1 2 0
 wrr-queue cos-map 2 1 2 3 4
 wrr-queue cos-map 2 2 6 7
```

```
 mls qos trust dscp
!
interface Vlan2
 description ACCESS-DATA-2
 ip address 10.120.2.2 255.255.255.0
 ip helper-address 10.121.10.7
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ipv6 address 2001:DB8:CAFE:2::1/64 anycast
 ipv6 address 2001:DB8:CAFE:2::A111:1010/64
 ipv6 traffic-filter VLAN2-v6-INGRESS in
 no ipv6 redirects
 ipv6 nd reachable-time 5000
 ipv6 cef
 ipv6 ospf 1 area 2
 arp timeout 200
 standby 1 ip 10.120.2.1
 standby 1 timers msec 250 msec 800
 standby 1 priority 110
 standby 1 preempt delay minimum 180
 standby 1 authentication ese
!
interface Vlan3
 description ACCESS-DATA-3
 ip address 10.120.3.2 255.255.255.0
 ip helper-address 10.121.10.7
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ipv6 address 2001:DB8:CAFE:3::1/64 anycast
 ipv6 address 2001:DB8:CAFE:3::A111:1010/64
 ipv6 traffic-filter VLAN3-v6-INGRESS in
 no ipv6 redirects
 ipv6 nd reachable-time 5000
 ipv6 cef
 ipv6 ospf 1 area 2
 arp timeout 200
 standby 1 ip 10.120.3.1
 standby 1 timers msec 250 msec 800
 standby 1 priority 110
 standby 1 preempt delay minimum 180
 standby 1 authentication ese
!
router eigrp 10
 passive-interface Vlan2
 passive-interface Vlan3
 passive-interface Loopback0
 network 10.0.0.0
 no auto-summary
 eigrp router-id 10.122.10.9
!
ip classless
!
no ip http server
!
ip access-list extended MGMT-IN-v4
 remark Permit v4MGMT only to Lo0
 permit tcp 10.120.0.0 0.0.255.255 any log-input
 permit tcp 10.121.0.0 0.0.255.255 any log-input
 permit tcp 10.122.0.0 0.0.255.255 any log-input
 deny   ip any any log-input
!
logging source-interface Loopback0
```

```
logging 10.121.11.9
ipv6 router ospf 1
 router-id 10.122.10.9
 log-adjacency-changes
 auto-cost reference-bandwidth 10000
 area 2 range 2001:DB8:CAFE:2::/64 cost 10
 area 2 range 2001:DB8:CAFE:3::/64 cost 10
 passive-interface Vlan2
 passive-interface Vlan3
 passive-interface Loopback0
 timers spf 1 5
!
snmp-server contact John Doe - ipv6rocks@cisco.com
snmp-server group IPv6-ADMIN v3 auth write v1default
!
ipv6 access-list MGMT-IN
 remark Permit MGMT only to Loopback0
 permit tcp 2001:DB8:CAFE::/48 host 2001:DB8:CAFE:6507::A111:1010 log-input
 deny ipv6 any any log-input
!
ipv6 access-list VLAN2-v6-INGRESS
 remark PERMIT ICMPv6 PACKETS FROM HOSTS WITH PREFIX CAFE:2::/64
 permit icmp 2001:DB8:CAFE:2::/64 any
 remark PERMIT IPv6 PACKETS FROM HOSTS WITH PREFIX CAFE:2::64
 permit ipv6 2001:DB8:CAFE:2::/64 any
 remark PERMIT ALL ICMPv6 PACKETS SOURCED BY HOSTS USING THE LINK-LOCAL PREFIX
 permit icmp FE80::/10 any
 remark DENY ALL OTHER IPv6 PACKETS AND LOG
 deny ipv6 any any log-input
!
ipv6 access-list VLAN3-v6-INGRESS
 remark PERMIT ICMPv6 PACKETS FROM HOSTS WITH PREFIX CAFE:3::/64
 permit icmp 2001:DB8:CAFE:3::/64 any
 remark PERMIT IPv6 PACKETS FROM HOSTS WITH PREFIX CAFE:3::64
 permit ipv6 2001:DB8:CAFE:3::/64 any
 remark PERMIT ALL ICMPv6 PACKETS SOURCED BY HOSTS USING THE LINK-LOCAL PREFIX
 permit icmp FE80::/10 any
 remark DENY ALL OTHER IPv6 PACKETS AND LOG
 deny ipv6 any any log-input
!
control-plane
!
dial-peer cor custom
!
banner login ^C
Unauthorized access to this device and/or network is prohibited!
^C
!
line con 0
 session-timeout 3
 password 7 06140E2F4B4B1B
 logging synchronous
 login local
 transport output none
line vty 0 4
 session-timeout 3
 access-class MGMT-IN-v4 in
 password 7 08334D400E1C17
 ipv6 access-class MGMT-IN in
 logging synchronous
 login local
 exec prompt timestamp
 transport input telnet ssh
!
```

```
no cns aaa enable
end
```

6k-dist-2

```
upgrade fpd auto
version 12.2
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service password-encryption
service internal
service sequence-numbers
service counters max age 5
!
hostname 6k-dist-2
!
boot system flash sup-bootdisk:s3223-adventerprisek9_wan-mz.122-18.SXF5.bin
logging buffered 64000 debugging
logging rate-limit 5
no logging console
enable secret 5 $1$0UKB$YN.zu/IQt0ivlkqLsdxtY0
!
username cisco privilege 15 secret 5 $1$SUYV$ShOXyooFT..fL/4tyOnAN1
no aaa new-model
clock timezone mst -7
ip subnet-zero
no ip source-route
ip icmp rate-limit unreachable 2000
!
ip ftp source-interface Loopback0
ip ftp username cisco
ip ftp password 7 01100F175804
ip tftp source-interface Loopback0
no ip bootp server
ip telnet source-interface Loopback0
ip ssh time-out 30
ip ssh authentication-retries 2
ip ssh source-interface Loopback0
ip ssh version 2
no ip domain-lookup
ip domain-name cisco.com
ipv6 unicast-routing
ipv6 mfib hardware-switching replication-mode ingress
ipv6 multicast-routing
udld enable

udld message time 7

vtp domain ese-dc
vtp mode transparent
mls ip cef load-sharing full
mls ip multicast flow-stat-timer 9
no mls flow ip
no mls flow ipv6
mls qos
mls rate-limit unicast ip icmp unreachable acl-drop 0
no mls acl tcam share-global
mls cef error action freeze
!
```

```
key chain eigrp
 key 100
  key-string 7 1111
!
redundancy
 mode sso
 main-cpu
  auto-sync running-config
!
spanning-tree mode rapid-pvst
spanning-tree loopguard default
no spanning-tree optimize bpdu transmission
spanning-tree extend system-id
spanning-tree vlan 2-3 priority 28672
environment temperature-controlled
system flowcontrol bus auto
diagnostic cns publish cisco.cns.device.diag_results
diagnostic cns subscribe cisco.cns.device.diag_commands
!
vlan internal allocation policy descending
vlan dot1q tag native
vlan access-log ratelimit 2000
!
vlan 2
 name ACCESS-DATA-2
!
vlan 3
 name ACCESS-DATA-3
!
!
interface Loopback0
 ip address 10.122.10.10 255.255.255.255
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ipv6 address 2001:DB8:CAFE:6507::B222:2020/128
 no ipv6 redirects
 ipv6 ospf 1 area 0
!
interface Null0
 no ip unreachables
!
interface TenGigabitEthernet1/1
 description to 6k-dist-1
 dampening
 ip address 10.122.0.94 255.255.255.252
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ip hello-interval eigrp 10 1
 ip hold-time eigrp 10 3
 ip authentication mode eigrp 10 md5
 ip authentication key-chain eigrp 10 eigrp
 load-interval 30
 carrier-delay msec 0
 ipv6 address 2001:DB8:CAFE:7004::B222:2020/64
 no ipv6 redirects
 ipv6 nd suppress-ra
 ipv6 cef
 ipv6 ospf network point-to-point
 ipv6 ospf hello-interval 1
 ipv6 ospf dead-interval 3
 ipv6 ospf 1 area 2
 wrr-queue bandwidth 5 25 70
```

```
 wrr-queue queue-limit 5 25 40
 wrr-queue random-detect min-threshold 1 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 3 50 60 70 80 90 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 2 100 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 3 60 70 80 90 100 100 100 100
 wrr-queue cos-map 1 1 1
 wrr-queue cos-map 2 1 0
 wrr-queue cos-map 3 1 4
 wrr-queue cos-map 3 2 2
 wrr-queue cos-map 3 3 3
 wrr-queue cos-map 3 4 6
 wrr-queue cos-map 3 5 7
 mls qos trust dscp
!
interface GigabitEthernet3/1
 description to 3750-acc-1
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 2
 switchport mode trunk
 switchport nonegotiate
 no ip address
 load-interval 30
 wrr-queue bandwidth 5 25 70
 wrr-queue queue-limit 5 25 40
 wrr-queue random-detect min-threshold 1 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 3 50 60 70 80 90 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 2 100 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 3 60 70 80 90 100 100 100 100
 wrr-queue cos-map 1 1 1
 wrr-queue cos-map 2 1 0
 wrr-queue cos-map 3 1 4
 wrr-queue cos-map 3 2 2
 wrr-queue cos-map 3 3 3
 wrr-queue cos-map 3 4 6
 wrr-queue cos-map 3 5 7
 mls qos trust dscp
 no cdp enable
!
interface GigabitEthernet3/2
 description to 3750-acc-1
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 3
 switchport mode trunk
 switchport nonegotiate
 no ip address
 load-interval 30
 wrr-queue bandwidth 5 25 70
 wrr-queue queue-limit 5 25 40
 wrr-queue random-detect min-threshold 1 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 3 50 60 70 80 90 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 2 100 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 3 60 70 80 90 100 100 100 100
 wrr-queue cos-map 1 1 1
 wrr-queue cos-map 2 1 0
 wrr-queue cos-map 3 1 4
 wrr-queue cos-map 3 2 2
```

```
 wrr-queue cos-map 3 3 3
 wrr-queue cos-map 3 4 6
 wrr-queue cos-map 3 5 7
 mls qos trust dscp
 no cdp enable
!
interface GigabitEthernet4/1
 description to 6k-core-1
 dampening
 ip address 10.122.0.82 255.255.255.252
 no ip redirects
 no ip proxy-arp
 ip hello-interval eigrp 10 1
 ip hold-time eigrp 10 3
 ip authentication mode eigrp 10 md5
 ip authentication key-chain eigrp 10 eigrp
 ip summary-address eigrp 10 10.120.0.0 255.255.0.0 5
 load-interval 30
 carrier-delay msec 0
 ipv6 address 2001:DB8:CAFE:7002::B222:2020/64
 no ipv6 redirects
 ipv6 nd suppress-ra
 ipv6 cef
 ipv6 ospf network point-to-point
 ipv6 ospf hello-interval 1
 ipv6 ospf dead-interval 3
 ipv6 ospf 1 area 0
 wrr-queue bandwidth 30 70
 wrr-queue queue-limit 40 30
 wrr-queue random-detect min-threshold 1 40 80
 wrr-queue random-detect min-threshold 2 70 80
 wrr-queue random-detect max-threshold 1 80 100
 wrr-queue random-detect max-threshold 2 80 100
 wrr-queue cos-map 1 1 1
 wrr-queue cos-map 1 2 0
 wrr-queue cos-map 2 1 2 3 4
 wrr-queue cos-map 2 2 6 7
 mls qos trust dscp
!
interface GigabitEthernet4/2
 description to 6k-core-2
 dampening
 ip address 10.122.0.90 255.255.255.252
 no ip redirects
 no ip proxy-arp
 ip hello-interval eigrp 10 1
 ip hold-time eigrp 10 3
 ip authentication mode eigrp 10 md5
 ip authentication key-chain eigrp 10 eigrp
 ip summary-address eigrp 10 10.120.0.0 255.255.0.0 5
 load-interval 30
 carrier-delay msec 0
 ipv6 address 2001:DB8:CAFE:7003::B222:2020/64
 no ipv6 redirects
 ipv6 nd suppress-ra
 ipv6 cef
 ipv6 ospf network point-to-point
 ipv6 ospf hello-interval 1
 ipv6 ospf dead-interval 3
 ipv6 ospf 1 area 0
 wrr-queue bandwidth 30 70
 wrr-queue queue-limit 40 30
 wrr-queue random-detect min-threshold 1 40 80
 wrr-queue random-detect min-threshold 2 70 80
```

```
 wrr-queue random-detect max-threshold 1 80 100
 wrr-queue random-detect max-threshold 2 80 100
 wrr-queue cos-map 1 1 1
 wrr-queue cos-map 1 2 0
 wrr-queue cos-map 2 1 2 3 4
 wrr-queue cos-map 2 2 6 7
 mls qos trust dscp
!
interface Vlan2
 description ACCESS-DATA-2
 ip address 10.120.2.3 255.255.255.0
 ip helper-address 10.121.10.7
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ipv6 address 2001:DB8:CAFE:2::1/64 anycast
 ipv6 address 2001:DB8:CAFE:2::B222:2020/64
 ipv6 traffic-filter VLAN2-v6-INGRESS in
 no ipv6 redirects
 ipv6 nd reachable-time 5000
 ipv6 cef
 ipv6 ospf 1 area 2
 arp timeout 200
 standby 1 ip 10.120.2.1
 standby 1 timers msec 250 msec 800
 standby 1 priority 105
 standby 1 preempt delay minimum 180
 standby 1 authentication ese
!
interface Vlan3
 description ACCESS-DATA-3
 ip address 10.120.3.3 255.255.255.0
 ip helper-address 10.121.10.7
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ipv6 address 2001:DB8:CAFE:3::1/64 anycast
 ipv6 address 2001:DB8:CAFE:3::B222:2020/64
 ipv6 traffic-filter VLAN3-v6-INGRESS in
 no ipv6 redirects
 ipv6 nd reachable-time 5000
 ipv6 cef
 ipv6 ospf 1 area 2
 arp timeout 200
 standby 1 ip 10.120.3.1
 standby 1 timers msec 250 msec 800
 standby 1 priority 105
 standby 1 preempt delay minimum 180
 standby 1 authentication ese
!
router eigrp 10
 passive-interface Vlan2
 passive-interface Vlan3
 passive-interface Loopback0
 network 10.0.0.0
 no auto-summary
 eigrp router-id 10.122.10.10
!
ip classless
!
no ip http server
!
ip access-list extended MGMT-IN-v4
 remark Permit v4MGMT only to Lo0
```

```
 permit tcp 10.120.0.0 0.0.255.255 any log-input
 permit tcp 10.121.0.0 0.0.255.255 any log-input
 permit tcp 10.122.0.0 0.0.255.255 any log-input
 deny   ip any any log-input
!
logging source-interface Loopback0
logging 10.121.11.9
ipv6 router ospf 1
 router-id 10.122.10.10
 log-adjacency-changes
 auto-cost reference-bandwidth 10000
 area 2 range 2001:DB8:CAFE:2::/64 cost 10
 area 2 range 2001:DB8:CAFE:3::/64 cost 10
 passive-interface Vlan2
 passive-interface Vlan3
 passive-interface Loopback0
 timers spf 1 5
!
!
snmp-server group IPv6-ADMIN v3 auth write v1default
snmp-server contact John Doe - ipv6rocks@cisco.com
!
!
ipv6 access-list MGMT-IN
 remark Permit MGMT only to Loopback0
 permit tcp 2001:DB8:CAFE::/48 host 2001:DB8:CAFE:6507::B222:2020 log-input
 deny ipv6 any any log-input
!
ipv6 access-list VLAN2-v6-INGRESS
 remark PERMIT ICMPv6 PACKETS FROM HOSTS WITH PREFIX 2001:DB8:CAFE:2::/64
 permit icmp 2001:DB8:CAFE:2::/64 any
 remark PERMIT IPv6 PACKETS FROM HOSTS WITH PREFIX 2001:DB8:CAFE:2::64
 permit ipv6 2001:DB8:CAFE:2::/64 any
 remark PERMIT ALL ICMPv6 PACKETS SOURCED BY HOSTS USING THE LINK-LOCAL PREFIX
 permit icmp FE80::/10 any
 remark DENY ALL OTHER IPv6 PACKETS AND LOG
 deny ipv6 any any log-input
!
ipv6 access-list VLAN3-v6-INGRESS
 remark PERMIT ICMPv6 PACKETS FROM HOSTS WITH PREFIX 2001:DB8:CAFE:3::/64
 permit icmp 2001:DB8:CAFE:3::/64 any
 remark PERMIT IPv6 PACKETS FROM HOSTS WITH PREFIX 2001:DB8:CAFE:3::64
 permit ipv6 2001:DB8:CAFE:3::/64 any
 remark PERMIT ALL ICMPv6 PACKETS SOURCED BY HOSTS USING THE LINK-LOCAL PREFIX
 permit icmp FE80::/10 any
 remark DENY ALL OTHER IPv6 PACKETS AND LOG
 deny ipv6 any any log-input
!
control-plane
!
dial-peer cor custom
!
banner login ^C

Unauthorized access to this device and network is prohibited.

^C
!
line con 0
 session-timeout 3
 password 7 1317161C0C0916
 logging synchronous
 login local
 transport output none
```

```
line vty 0 4
 session-timeout 3
 access-class MGMT-IN-v4 in
 password 7 071D2042490C0B
 ipv6 access-class MGMT-IN in
 logging synchronous
 login local
 exec prompt timestamp
 transport input telnet ssh
!
no cns aaa enable
end
```

6k-core-1

```
upgrade fpd auto
version 12.2
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service password-encryption
service internal
service sequence-numbers
service counters max age 5
!
hostname 6k-core-1
!
boot system flash sup-bootdisk:s3223-adventerprisek9_wan-mz.122-18.SXF5.bin
logging buffered 64000 debugging
logging rate-limit 5
no logging console
enable secret 5 $1$hHvm$ln0YNSdCb7lzgHMmFz9Bi0
!
username cisco privilege 15 password 7 120B0419150E1E
no aaa new-model
clock timezone mst -7
ip subnet-zero
no ip source-route
ip icmp rate-limit unreachable 2000
!
ip ftp source-interface Loopback0
ip ftp username cisco
ip ftp password 7 071D2042490C0B
ip tftp source-interface Loopback0
no ip bootp server
ip telnet source-interface Loopback0
ip ssh time-out 30
ip ssh authentication-retries 2
ip ssh source-interface Loopback0
ip ssh version 2
no ip domain-lookup
ip domain-name cisco.com
ipv6 unicast-routing
ipv6 mfib hardware-switching replication-mode ingress
ipv6 multicast-routing
udld enable

udld message time 7

vtp domain ese-dc
```

```
vtp mode transparent
mls ip multicast flow-stat-timer 9
no mls flow ip
no mls flow ipv6
mls qos
mls rate-limit unicast ip icmp unreachable acl-drop 0
no mls acl tcam share-global
mls cef error action freeze
!
key chain eigrp
 key 100
  key-string 7 1111
!
redundancy
 mode sso
 main-cpu
  auto-sync running-config
!
spanning-tree mode rapid-pvst
spanning-tree loopguard default
no spanning-tree optimize bpdu transmission
spanning-tree extend system-id
environment temperature-controlled
system flowcontrol bus auto
diagnostic cns publish cisco.cns.device.diag_results
diagnostic cns subscribe cisco.cns.device.diag_commands
!
vlan internal allocation policy descending
vlan dot1q tag native
vlan access-log ratelimit 2000
!
interface Loopback0
 ip address 10.122.10.3 255.255.255.255
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ipv6 address 2001:DB8:CAFE:6507::C333:3030/128
 no ipv6 redirects
 ipv6 ospf 1 area 0
!
interface Null0
 no ip unreachables
!
interface GigabitEthernet2/1
 description to 6k-agg-1
 dampening
 ip address 10.122.0.26 255.255.255.252
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ip hello-interval eigrp 10 1
 ip hold-time eigrp 10 3
 ip authentication mode eigrp 10 md5
 ip authentication key-chain eigrp 10 eigrp
 load-interval 30
 carrier-delay msec 0
 ipv6 address 2001:DB8:CAFE:7005::C333:3030/64
 no ipv6 redirects
 ipv6 nd suppress-ra
 ipv6 cef
 ipv6 ospf network point-to-point
 ipv6 ospf hello-interval 1
 ipv6 ospf dead-interval 3
 ipv6 ospf 1 area 0
```

```
 wrr-queue bandwidth 30 70
 wrr-queue queue-limit 30 70
 wrr-queue threshold 1 40 100
 wrr-queue cos-map 1 1 1
 wrr-queue cos-map 1 2 0
 wrr-queue cos-map 2 1 2 3 4 6 7
 wrr-queue cos-map 2 2 5
 mls qos trust dscp
!
interface GigabitEthernet2/2
 description to 6k-agg-2
 dampening
 ip address 10.122.0.34 255.255.255.252
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ip hello-interval eigrp 10 1
 ip hold-time eigrp 10 3
 ip authentication mode eigrp 10 md5
 ip authentication key-chain eigrp 10 eigrp
 load-interval 30
 carrier-delay msec 0
 ipv6 address 2001:DB8:CAFE:7006::C333:3030/64
 no ipv6 redirects
 ipv6 nd suppress-ra
 ipv6 cef
 ipv6 ospf network point-to-point
 ipv6 ospf hello-interval 1
 ipv6 ospf dead-interval 3
 ipv6 ospf 1 area 0
 wrr-queue bandwidth 30 70
 wrr-queue queue-limit 30 70
 wrr-queue threshold 1 40 100
 wrr-queue cos-map 1 1 1
 wrr-queue cos-map 1 2 0
 wrr-queue cos-map 2 1 2 3 4 6 7
 wrr-queue cos-map 2 2 5
 mls qos trust dscp
!
interface GigabitEthernet2/3
 description to 6k-core-2
 dampening
 ip address 10.122.0.21 255.255.255.252
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ip hello-interval eigrp 10 1
 ip hold-time eigrp 10 3
 ip authentication mode eigrp 10 md5
 ip authentication key-chain eigrp 10 eigrp
 load-interval 30
 carrier-delay msec 0
 ipv6 address 2001:DB8:CAFE:7009::C333:3030/64
 no ipv6 redirects
 ipv6 nd suppress-ra
 ipv6 cef
 ipv6 ospf network point-to-point
 ipv6 ospf hello-interval 1
 ipv6 ospf dead-interval 3
 ipv6 ospf 1 area 0
 wrr-queue bandwidth 30 70
 wrr-queue queue-limit 30 70
 wrr-queue threshold 1 40 100
 wrr-queue cos-map 1 1 1
```

```
 wrr-queue cos-map 1 2 0
 wrr-queue cos-map 2 1 2 3 4 6 7
 wrr-queue cos-map 2 2 5
 mls qos trust dscp
!
interface GigabitEthernet2/4
 description to 6k-dist-1
 dampening
 ip address 10.122.0.77 255.255.255.252
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ip hello-interval eigrp 10 1
 ip hold-time eigrp 10 3
 ip authentication mode eigrp 10 md5
 ip authentication key-chain eigrp 10 eigrp
 load-interval 30
 carrier-delay msec 0
 ipv6 address 2001:DB8:CAFE:7000::C333:3030/64
 no ipv6 redirects
 ipv6 nd suppress-ra
 ipv6 cef
 ipv6 ospf network point-to-point
 ipv6 ospf hello-interval 1
 ipv6 ospf dead-interval 3
 ipv6 ospf 1 area 0
 wrr-queue bandwidth 30 70
 wrr-queue queue-limit 30 70
 wrr-queue threshold 1 40 100
 wrr-queue cos-map 1 1 1
 wrr-queue cos-map 1 2 0
 wrr-queue cos-map 2 1 2 3 4 6 7
 wrr-queue cos-map 2 2 5
 mls qos trust dscp
!
interface GigabitEthernet2/5
 description to 6k-dist-2
 dampening
 ip address 10.122.0.81 255.255.255.252
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ip hello-interval eigrp 10 1
 ip hold-time eigrp 10 3
 ip authentication mode eigrp 10 md5
 ip authentication key-chain eigrp 10 eigrp
 load-interval 30
 carrier-delay msec 0
 ipv6 address 2001:DB8:CAFE:7002::C333:3030/64
 no ipv6 redirects
 ipv6 nd suppress-ra
 ipv6 cef
 ipv6 ospf network point-to-point
 ipv6 ospf hello-interval 1
 ipv6 ospf dead-interval 3
 ipv6 ospf 1 area 0
 wrr-queue bandwidth 30 70
 wrr-queue queue-limit 30 70
 wrr-queue threshold 1 40 100
 wrr-queue cos-map 1 1 1
 wrr-queue cos-map 1 2 0
 wrr-queue cos-map 2 1 2 3 4 6 7
 wrr-queue cos-map 2 2 5
 mls qos trust dscp
```

```
!
router eigrp 10
 passive-interface Loopback0
 network 10.0.0.0
 no auto-summary
 eigrp router-id 10.122.10.3
!
ip classless
!
no ip http server
ip http path bootflash:
!
ip access-list extended MGMT-IN-v4
 remark Permit v4MGMT only to Lo0
 permit tcp 10.120.0.0 0.0.255.255 any log-input
 permit tcp 10.121.0.0 0.0.255.255 any log-input
 permit tcp 10.122.0.0 0.0.255.255 any log-input
 deny   ip any any log-input
!
logging source-interface Loopback0
logging 10.121.11.9
ipv6 router ospf 1
 router-id 10.122.10.3
 log-adjacency-changes
 auto-cost reference-bandwidth 10000
 passive-interface Loopback0
 timers spf 1 5
!
snmp-server group IPv6-ADMIN v3 auth write v1default
snmp-server contact John Doe - IPv6 ipv6rocks@cisco.com
!
ipv6 access-list MGMT-IN
 remark Permit MGMT only to Loopback0
 permit tcp 2001:DB8:CAFE::/48 host 2001:DB8:CAFE:6507::C333:3030 log-input
 deny ipv6 any any log-input
!
control-plane
!
dial-peer cor custom
!
banner login ^C
Unauthorized access to this device and/or network is prohibited.
^C
!
line con 0
 session-timeout 3
 exec-timeout 0 0
 password 7 095E4F071E0005
 logging synchronous
 login local
 transport output telnet ssh
line vty 0 4
 session-timeout 3
 access-class MGMT-IN-v4 in
 exec-timeout 30 0
 password 7 03165A05010A33
 ipv6 access-class MGMT-IN in
 logging synchronous
 login local
 exec prompt timestamp
 transport input telnet ssh
!
no cns aaa enable
end
```

```
6k-core-2
upgrade fpd auto
version 12.2
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service password-encryption
service internal
service sequence-numbers
service counters max age 5
!
hostname 6k-core-2
!
boot system flash sup-bootdisk:s3223-adventerprisek9_wan-mz.122-18.SXF5.bin
logging buffered 64000 debugging
logging rate-limit 5
no logging console
enable secret 5 $1$W031$3oHUmVfyHXW7fwdMWEBq01
!
username cisco privilege 15 secret 5 $1$vVK6$2OGixA1lDE.ufYBqWUrru/
no aaa new-model
clock timezone mst -7
ip subnet-zero
no ip source-route
ip icmp rate-limit unreachable 2000
!
ip ftp source-interface Loopback0
ip ftp username cisco
ip ftp password 7 111B180B101719
ip tftp source-interface Loopback0
no ip bootp server
ip telnet source-interface Loopback0
ip ssh time-out 30
ip ssh authentication-retries 2
ip ssh source-interface Loopback0
ip ssh version 2
no ip domain-lookup
ip domain-name cisco.com
ipv6 unicast-routing
ipv6 mfib hardware-switching replication-mode ingress
ipv6 multicast-routing
udld enable

udld message time 7

vtp domain ese-dc
vtp mode transparent
mls ip multicast flow-stat-timer 9
no mls flow ip
no mls flow ipv6
mls qos
mls rate-limit unicast ip icmp unreachable acl-drop 0
no mls acl tcam share-global
mls cef error action freeze
!
key chain eigrp
 key 100
  key-string 7 1111
!
redundancy
 mode sso
```

```
 main-cpu
  auto-sync running-config
!
spanning-tree mode rapid-pvst
spanning-tree loopguard default
no spanning-tree optimize bpdu transmission
spanning-tree extend system-id
environment temperature-controlled
system flowcontrol bus auto
diagnostic cns publish cisco.cns.device.diag_results
diagnostic cns subscribe cisco.cns.device.diag_commands
!
vlan internal allocation policy descending
vlan dot1q tag native
vlan access-log ratelimit 2000
!
interface Loopback0
 ip address 10.122.10.4 255.255.255.255
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ipv6 address 2001:DB8:CAFE:6507::D444:4040/64
 no ipv6 redirects
 ipv6 ospf 1 area 0
!
interface Null0
 no ip unreachables
!
interface GigabitEthernet2/1
 description to 6k-agg-1
 dampening
 ip address 10.122.0.30 255.255.255.252
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ip hello-interval eigrp 10 1
 ip hold-time eigrp 10 3
 ip authentication mode eigrp 10 md5
 ip authentication key-chain eigrp 10 eigrp
 load-interval 30
 carrier-delay msec 0
 ipv6 address 2001:DB8:CAFE:7007::D444:4040/64
 no ipv6 redirects
 ipv6 nd suppress-ra
 ipv6 cef
 ipv6 ospf network point-to-point
 ipv6 ospf hello-interval 1
 ipv6 ospf dead-interval 3
 ipv6 ospf 1 area 0
 wrr-queue bandwidth 30 70
 wrr-queue queue-limit 40 30
 wrr-queue random-detect min-threshold 1 40 80
 wrr-queue random-detect min-threshold 2 70 80
 wrr-queue random-detect max-threshold 1 80 100
 wrr-queue random-detect max-threshold 2 80 100
 wrr-queue cos-map 1 1 1
 wrr-queue cos-map 1 2 0
 wrr-queue cos-map 2 1 2 3 4
 wrr-queue cos-map 2 2 6 7
 mls qos trust dscp
!
interface GigabitEthernet2/2
 description to 6k-agg-2
 dampening
```

```
 ip address 10.122.0.38 255.255.255.252
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ip hello-interval eigrp 10 1
 ip hold-time eigrp 10 3
 ip authentication mode eigrp 10 md5
 ip authentication key-chain eigrp 10 eigrp
 load-interval 30
 carrier-delay msec 0
 ipv6 address 2001:DB8:CAFE:7008::D444:4040/64
 no ipv6 redirects
 ipv6 nd suppress-ra
 ipv6 cef
 ipv6 ospf network point-to-point
 ipv6 ospf hello-interval 1
 ipv6 ospf dead-interval 3
 ipv6 ospf 1 area 0
 wrr-queue bandwidth 30 70
 wrr-queue queue-limit 40 30
 wrr-queue random-detect min-threshold 1 40 80
 wrr-queue random-detect min-threshold 2 70 80
 wrr-queue random-detect max-threshold 1 80 100
 wrr-queue random-detect max-threshold 2 80 100
 wrr-queue cos-map 1 1 1
 wrr-queue cos-map 1 2 0
 wrr-queue cos-map 2 1 2 3 4
 wrr-queue cos-map 2 2 6 7
 mls qos trust dscp
!
interface GigabitEthernet2/3
 description to 6k-core-1
 dampening
 ip address 10.122.0.22 255.255.255.252
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ip hello-interval eigrp 10 1
 ip hold-time eigrp 10 3
 ip authentication mode eigrp 10 md5
 ip authentication key-chain eigrp 10 eigrp
 load-interval 30
 carrier-delay msec 0
 ipv6 address 2001:DB8:CAFE:7009::D444:4040/64
 no ipv6 redirects
 ipv6 nd suppress-ra
 ipv6 cef
 ipv6 ospf network point-to-point
 ipv6 ospf hello-interval 1
 ipv6 ospf dead-interval 3
 ipv6 ospf 1 area 0
 wrr-queue bandwidth 30 70
 wrr-queue queue-limit 40 30
 wrr-queue random-detect min-threshold 1 40 80
 wrr-queue random-detect min-threshold 2 70 80
 wrr-queue random-detect max-threshold 1 80 100
 wrr-queue random-detect max-threshold 2 80 100
 wrr-queue cos-map 1 1 1
 wrr-queue cos-map 1 2 0
 wrr-queue cos-map 2 1 2 3 4
 wrr-queue cos-map 2 2 6 7
 mls qos trust dscp
!
interface GigabitEthernet2/4
```

```
 description to 6k-dist-1
 dampening
 ip address 10.122.0.85 255.255.255.252
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ip hello-interval eigrp 10 1
 ip hold-time eigrp 10 3
 ip authentication mode eigrp 10 md5
 ip authentication key-chain eigrp 10 eigrp
 load-interval 30
 carrier-delay msec 0
 ipv6 address 2001:DB8:CAFE:7001::D444:4040/64
 no ipv6 redirects
 ipv6 nd suppress-ra
 ipv6 cef
 ipv6 ospf network point-to-point
 ipv6 ospf hello-interval 1
 ipv6 ospf dead-interval 3
 ipv6 ospf 1 area 0
 wrr-queue bandwidth 30 70
 wrr-queue queue-limit 40 30
 wrr-queue random-detect min-threshold 1 40 80
 wrr-queue random-detect min-threshold 2 70 80
 wrr-queue random-detect max-threshold 1 80 100
 wrr-queue random-detect max-threshold 2 80 100
 wrr-queue cos-map 1 1 1
 wrr-queue cos-map 1 2 0
 wrr-queue cos-map 2 1 2 3 4
 wrr-queue cos-map 2 2 6 7
 mls qos trust dscp
!
interface GigabitEthernet2/5
 description to 6k-dist-2
 dampening
 ip address 10.122.0.89 255.255.255.252
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ip hello-interval eigrp 10 1
 ip hold-time eigrp 10 3
 ip authentication mode eigrp 10 md5
 ip authentication key-chain eigrp 10 eigrp
 load-interval 30
 carrier-delay msec 0
 ipv6 address 2001:DB8:CAFE:7003::D444:4040/64
 no ipv6 redirects
 ipv6 nd suppress-ra
 ipv6 cef
 ipv6 ospf network point-to-point
 ipv6 ospf hello-interval 1
 ipv6 ospf dead-interval 3
 ipv6 ospf 1 area 0
 wrr-queue bandwidth 30 70
 wrr-queue queue-limit 40 30
 wrr-queue random-detect min-threshold 1 40 80
 wrr-queue random-detect min-threshold 2 70 80
 wrr-queue random-detect max-threshold 1 80 100
 wrr-queue random-detect max-threshold 2 80 100
 wrr-queue cos-map 1 1 1
 wrr-queue cos-map 1 2 0
 wrr-queue cos-map 2 1 2 3 4
 wrr-queue cos-map 2 2 6 7
 mls qos trust dscp
```

```
!
!
router eigrp 10
 passive-interface Loopback0
 network 10.0.0.0
 no auto-summary
 eigrp router-id 10.122.10.4
!
ip classless
!
no ip http server
!
ip access-list extended MGMT-IN-v4
 remark Permit v4MGMT only to Lo0
 permit tcp 10.120.0.0 0.0.255.255 any log-input
 permit tcp 10.121.0.0 0.0.255.255 any log-input
 permit tcp 10.122.0.0 0.0.255.255 any log-input
 deny   ip any any log-input
!
logging source-interface Loopback0
logging 10.121.11.9
ipv6 router ospf 1
 router-id 10.122.10.4
 log-adjacency-changes
 auto-cost reference-bandwidth 10000
 passive-interface Loopback0
 timers spf 1 5
!
!
snmp-server group IPv6-ADMIN v3 auth write v1default
snmp-server contact John Doe - IPv6 ipv6rocks@cisco.com
!
ipv6 access-list MGMT-IN
 remark Permit MGMT only to Loopback0
 permit tcp 2001:DB8:CAFE::/48 host 2001:DB8:CAFE:6507::D444:4040 log-input
 deny ipv6 any any log-input
!
control-plane
!
dial-peer cor custom
!
banner login ^C
Unauthorized access to this device and/or network is prohibited.
^C
!
line con 0
 session-timeout 3
 exec-timeout 0 0
 password 7 120B0419150E1E
 logging synchronous
 login local
 transport output telnet ssh
line vty 0 4
 session-timeout 3
 access-class MGMT-IN-v4 in
 exec-timeout 30 0
 password 7 105C0817021200
 ipv6 access-class MGMT-IN in
 logging synchronous
 login local
 exec prompt timestamp
 transport input telnet ssh
!
no cns aaa enable
```

```
end
```

デュアルスタック モデル（DSM）— ルーテッド アクセス

ここでは、アクセス レイヤ（3750-acc-1）およびディストリビューション レイヤ（6k-dist-1/6k-dist-2）についてのみ設定を示します。

3750-acc-1

```
version 12.2
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service password-encryption
service sequence-numbers
!
hostname 3750-acc-1
!
logging count
logging buffered 8192 debugging
logging rate-limit 5
no logging console
enable secret 5 $1$RPWW$KR0qkU1kW0a7Pd1svvhgB.
!
username cisco privilege 15 secret 5 $1$KNSF$3XavijOuoVCq68RASxTYD1
no aaa new-model
clock timezone mst -7
switch 1 provision ws-c3750g-24ts
vtp domain ese-dc
vtp mode transparent
udld enable

udld message time 7

ip subnet-zero
no ip source-route
ip routing
ip icmp rate-limit unreachable 2000
ip telnet source-interface Vlan2
no ip domain-lookup
ip domain-name cisco.com
ip dhcp smart-relay
!
ip dhcp snooping vlan 2
ip dhcp snooping database flash:dhcp.txt
ip dhcp snooping database timeout 10
ip dhcp snooping
ip ftp source-interface Vlan2
ip ftp username cisco
ip ftp password 7 120B0419150E1E
ip tftp source-interface Vlan2
ip ssh time-out 60
ip ssh authentication-retries 2
ip ssh source-interface Vlan2
ip ssh version 2
ip arp inspection vlan 2
ip arp inspection validate src-mac
ip arp inspection log-buffer entries 100
```

```
ip arp inspection log-buffer logs 20 interval 120
login block-for 30 attempts 3 within 200
login delay 2
ipv6 mld snooping
ipv6 unicast-routing
!
mls qos map policed-dscp  0 10 18 24 25 34 to 8
mls qos map cos-dscp 0 8 16 24 32 46 48 56
mls qos srr-queue output cos-map queue 1 threshold 3  5
mls qos srr-queue output cos-map queue 2 threshold 1  2 4
mls qos srr-queue output cos-map queue 2 threshold 2  3
mls qos srr-queue output cos-map queue 2 threshold 3  6 7
mls qos srr-queue output cos-map queue 3 threshold 3  0
mls qos srr-queue output cos-map queue 4 threshold 3  1
mls qos srr-queue output dscp-map queue 1 threshold 3  46
mls qos srr-queue output dscp-map queue 2 threshold 1  16 18 20 22 25 32 34 36
mls qos srr-queue output dscp-map queue 2 threshold 1  38
mls qos srr-queue output dscp-map queue 2 threshold 2  24 26
mls qos srr-queue output dscp-map queue 2 threshold 3  48 56
mls qos srr-queue output dscp-map queue 3 threshold 3  0
mls qos srr-queue output dscp-map queue 4 threshold 1  8
mls qos srr-queue output dscp-map queue 4 threshold 3  10 12 14
mls qos queue-set output 1 threshold 2 70 80 100 100
mls qos queue-set output 1 threshold 4 40 100 100 100
mls qos
!
key chain eigrp
 key 100
  key-string 7 1111
!
crypto pki trustpoint TP-self-signed-3669881984
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-3669881984
 revocation-check none
 rsakeypair TP-self-signed-3669881984
!
crypto ca certificate chain TP-self-signed-3669881984
 certificate self-signed 01
  30820299 30820202 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
  57312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274
  69666963 6174652D 33363639 38383139 38343124 30220609 2A864886 F70D0109
  02161533 3735302D 65646765 2D312E63 6973636F 2E636F6D 301E170D 39333033
  30313030 30313533 5A170D32 30303130 31303030 3030305A 3057312F 302D0603
  55040313 26494F53 2D53656C 662D5369 676E6564 2D436572 74696669 63617465
  2D333636 39383831 39383431 24302206 092A8648 86F70D01 09021615 33373530
  2D656467 652D312E 63697363 6F2E636F 6D30819F 300D0609 2A864886 F70D0101
  01050003 818D0030 81890281 8100BF7D E793E21B 6C1F75C2 16AAFF9F C110D038
  2D6D1DC9 04758DB8 7B3AD4C9 9F36A3B1 54983BEC 10FEA2D4 151D2783 5765C58A
  A95E6364 CCBCF7F9 F4750437 AB8C00BF EFD54E88 6F650A5C 9563A309 247C6070
  DC38A870 DEC5D4DA 765AD7A4 274B7649 36D876CA E28CF66C 77335F90 949DF258
  E3E019BD 5E6801EC 9E15F980 C13D0203 010001A3 75307330 0F060355 1D130101
  FF040530 030101FF 30200603 551D1104 19301782 15333735 302D6564 67652D31
  2E636973 636F2E63 6F6D301F 0603551D 23041830 168014E0 18682CE1 D6A3EF2C
  32A7C8D5 4DAFB9AA F11A0030 1D060355 1D0E0416 0414E018 682CE1D6 A3EF2C32
  A7C8D54D AFB9AAF1 1A00300D 06092A86 4886F70D 01010405 00038181 00755909
  C99DEB7F E05FC2A3 482558FA 33C292AE 7E4543E3 5BD6F32F 1D671B97 BC45B73B
  85E954ED 7FC58F90 23A38132 24216CDB C978B3DD 9BCBC48E 519D01BF F4CEBB82
  07834C2D D82CA163 8E638214 5B5C277D 5E7DD52E 56172675 BD563769 590E4DC6
  39AD9BF8 CDBBA241 E5E2C666 5CAE912E 40DC2150 A1CE39B4 D8101D33 A8
  quit
!
errdisable recovery cause link-flap
errdisable recovery interval 60
no file verify auto
```

```
!
spanning-tree mode rapid-pvst
spanning-tree loopguard default
spanning-tree portfast bpduguard default
no spanning-tree optimize bpdu transmission
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
vlan 2
 name ACCESS-DATA-2
!
class-map match-all DVLAN-PC-VIDEO
  match access-group name DVLAN-PC-VIDEO
class-map match-all DVLAN-Transactional-Data
  match access-group name DVLAN-Transactional-Data
class-map match-all DVLAN-Mission-Critical-Data
  match access-group name DVLAN-Mission-Critical-Data
class-map match-all DVLAN-Bulk-Data
  match access-group name DVLAN-Bulk-Data
!
!
policy-map DATA
  class DVLAN-PC-VIDEO
   set dscp af41
    police 48000 8000 exceed-action policed-dscp-transmit
  class DVLAN-Mission-Critical-Data
   set dscp 25
    police 5000000 8000 exceed-action policed-dscp-transmit
  class DVLAN-Transactional-Data
   set dscp af21
    police 5000000 8000 exceed-action policed-dscp-transmit
  class DVLAN-Bulk-Data
   set dscp af11
    police 5000000 8000 exceed-action policed-dscp-transmit
!
interface Null0
 no ip unreachables
!
interface GigabitEthernet1/0/5
 description to PC-DATA-ONLY
 switchport access vlan 2
 switchport mode access
 switchport port-security maximum 3
 switchport port-security
 switchport port-security aging time 2
 switchport port-security violation restrict
 switchport port-security aging type inactivity
 ip arp inspection limit rate 100
 service-policy input DATA
 load-interval 30
 srr-queue bandwidth share 1 70 25 5
 srr-queue bandwidth shape  3  0  0  0
 priority-queue out
 spanning-tree portfast
 spanning-tree bpduguard enable
 ip verify source
 ip dhcp snooping limit rate 100
!
interface GigabitEthernet1/0/25
 description To 6k-dist-1
 no switchport
 dampening
 ip address 10.120.0.2 255.255.255.252
```

```
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ip hello-interval eigrp 10 1
 ip hold-time eigrp 10 3
 ip authentication mode eigrp 10 md5
 ip authentication key-chain eigrp 10 eigrp
 load-interval 30
 carrier-delay msec 0
 srr-queue bandwidth share 1 70 25 5
 srr-queue bandwidth shape  3  0  0  0
 priority-queue out
 ipv6 address 2001:DB8:CAFE:700A::CAC1:3750/64
 ipv6 nd suppress-ra
 ipv6 ospf network point-to-point
 ipv6 ospf hello-interval 1
 ipv6 ospf dead-interval 3
 ipv6 ospf 1 area 2
 no ipv6 redirects
 mls qos trust dscp
 no cdp enable
!
interface GigabitEthernet1/0/26
 description To 6k-dist-2
 no switchport
 dampening
 ip address 10.120.0.10 255.255.255.252
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ip hello-interval eigrp 10 1
 ip hold-time eigrp 10 3
 ip authentication mode eigrp 10 md5
 ip authentication key-chain eigrp 10 eigrp
 load-interval 30
 carrier-delay msec 0
 srr-queue bandwidth share 1 70 25 5
 srr-queue bandwidth shape  3  0  0  0
 priority-queue out
 ipv6 address 2001:DB8:CAFE:700C::CAC1:3750/64
 ipv6 nd suppress-ra
 ipv6 ospf network point-to-point
 ipv6 ospf hello-interval 1
 ipv6 ospf dead-interval 3
 ipv6 ospf 1 area 2
 no ipv6 redirects
 mls qos trust dscp
 no cdp enable
!
interface Vlan2
 ip address 10.120.2.1 255.255.255.0
 ip helper-address 10.121.10.7
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 no ip mroute-cache
 load-interval 30
 ipv6 address 2001:DB8:CAFE:2::CAC1:3750/64
 ipv6 ospf 1 area 2
 no ipv6 redirects
!
router eigrp 10
 passive-interface Vlan2
 network 10.120.0.0 0.0.255.255
```

```
 no auto-summary
 eigrp router-id 10.120.2.1
 eigrp stub connected
!
ip classless
no ip http server
no ip http secure-server
!
ip access-list extended DVLAN-Bulk-Data
 permit tcp any any eq 143
 permit tcp any any eq 220
ip access-list extended DVLAN-Mission-Critical-Data
 permit tcp any any range 3200 3203
 permit tcp any any eq 3600
 permit tcp any any range 2000 2002
ip access-list extended DVLAN-PC-VIDEO
 permit udp any any range 16384 32767
ip access-list extended DVLAN-Transactional-Data
 permit tcp any any eq 1352
ip access-list extended MGMT-IN-v4
 permit tcp 10.120.0.0 0.0.255.255 any log-input
 permit tcp 10.121.0.0 0.0.255.255 any log-input
 permit tcp 10.122.0.0 0.0.255.255 any log-input
 deny   ip any any log-input
!
logging source-interface Vlan2
logging 10.121.11.9
no cdp run
!
ipv6 router ospf 1
 router-id 10.120.2.1
 log-adjacency-changes
 auto-cost reference-bandwidth 10000
 area 2 stub no-summary
 passive-interface Vlan2
 timers spf 1 5
!
snmp-server group IPv6-ADMIN v3 auth write v1default
snmp-server contact John Doe - IPv6 ipv6rocks@cisco.com
!
ipv6 access-list MGMT-IN
 remark Permit MGMT only to VLAN2
 permit tcp 2001:DB8:CAFE::/48 host 2001:DB8:CAFE:2::CAC1:3750 log-input
 deny ipv6 any any log-input
!
control-plane
!
banner login ^C
Unauthorized access to this device and/or network is prohibited.
^C
!
line con 0
 session-timeout 3
 exec-timeout 0 0
 password 7 06140E2F4B4B1B
 logging synchronous
 login local
 transport output telnet ssh
line vty 0 4
 session-timeout 3
 password 7 06140E2F4B4B1B
 ipv6 access-class MGMT-IN in
 logging synchronous
 login local
```

```
 exec prompt timestamp
 transport input telnet ssh
line vty 5 15
 session-timeout 3
 password 7 0101070A5C0E14
 ipv6 access-class MGMT-IN in
 logging synchronous
 login local
 exec prompt timestamp
 transport input telnet ssh
!
end
```

6k-dist-1

```
upgrade fpd auto
version 12.2
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service password-encryption
service sequence-numbers
service counters max age 5
!
hostname 6k-dist-1
!
boot system flash sup-bootdisk:s3223-adventerprisek9_wan-mz.122-18.SXF5.bin
logging buffered 64000 debugging
logging rate-limit 5
no logging console
enable secret 5 $1$EZB7$nbqNvH9QH4qo3zpGsZog6/
!
username cisco privilege 15 secret 5 $1$VwbR$aXCTEAusOPhpmcfg7nOn01
no aaa new-model
clock timezone mst -7
ip subnet-zero
no ip source-route
ip icmp rate-limit unreachable 2000
!
ip ftp source-interface Loopback0
ip ftp username cisco
ip ftp password 7 121A0C041104
ip tftp source-interface Loopback0
no ip bootp server
ip telnet source-interface Loopback0
ip ssh time-out 30
ip ssh authentication-retries 2
ip ssh source-interface Loopback0
ip ssh version 2
no ip domain-lookup
ip domain-name cisco.com
ipv6 unicast-routing
ipv6 mfib hardware-switching replication-mode ingress
ipv6 multicast-routing
udld enable

udld message time 7

vtp domain ese-dc
vtp mode transparent
```

```
mls ip cef load-sharing full
mls ip multicast flow-stat-timer 9
no mls flow ip
no mls flow ipv6
mls qos
mls rate-limit unicast ip icmp unreachable acl-drop 0
no mls acl tcam share-global
mls cef error action freeze
!
key chain eigrp
 key 100
  key-string 7 1111
!
redundancy
 mode sso
 main-cpu
  auto-sync running-config
!
spanning-tree mode rapid-pvst
spanning-tree loopguard default
no spanning-tree optimize bpdu transmission
spanning-tree extend system-id
spanning-tree vlan 2-3 priority 24576
environment temperature-controlled
system flowcontrol bus auto
diagnostic cns publish cisco.cns.device.diag_results
diagnostic cns subscribe cisco.cns.device.diag_commands
!
vlan internal allocation policy descending
vlan dot1q tag native
vlan access-log ratelimit 2000
!
interface Loopback0
 ip address 10.122.10.9 255.255.255.255
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ipv6 address 2001:DB8:CAFE:6507::A111:1010/128
 no ipv6 redirects
 ipv6 ospf 1 area 0
!
interface Null0
 no ip unreachables
!
interface TenGigabitEthernet1/1
 description to 6k-dist-2
 dampening
 ip address 10.120.0.13 255.255.255.252
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ip hello-interval eigrp 10 1
 ip hold-time eigrp 10 3
 ip authentication mode eigrp 10 md5
 ip authentication key-chain eigrp 10 eigrp
 load-interval 30
 carrier-delay msec 0
 ipv6 address 2001:DB8:CAFE:7004::A111:1010/64
 no ipv6 redirects
 ipv6 nd suppress-ra
 ipv6 cef
 ipv6 ospf network point-to-point
 ipv6 ospf hello-interval 1
 ipv6 ospf dead-interval 3
```

```
 ipv6 ospf 1 area 2
 wrr-queue bandwidth 5 25 70
 wrr-queue queue-limit 5 25 40
 wrr-queue random-detect min-threshold 1 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 3 50 60 70 80 90 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 2 100 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 3 60 70 80 90 100 100 100 100
 wrr-queue cos-map 1 1 1
 wrr-queue cos-map 2 1 0
 wrr-queue cos-map 3 1 4
 wrr-queue cos-map 3 2 2
 wrr-queue cos-map 3 3 3
 wrr-queue cos-map 3 4 6
 wrr-queue cos-map 3 5 7
 mls qos trust dscp
!
interface GigabitEthernet3/1
 description to 3750-acc-1
 dampening
 ip address 10.120.0.1 255.255.255.252
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ip hello-interval eigrp 10 1
 ip hold-time eigrp 10 3
 ip authentication mode eigrp 10 md5
 ip authentication key-chain eigrp 10 eigrp
 load-interval 30
 carrier-delay msec 0
 ipv6 address 2001:DB8:CAFE:700A::A111:1010/64
 no ipv6 redirects
 ipv6 nd suppress-ra
 ipv6 cef
 ipv6 ospf network point-to-point
 ipv6 ospf hello-interval 1
 ipv6 ospf dead-interval 3
 ipv6 ospf 1 area 2
 wrr-queue bandwidth 5 25 70
 wrr-queue queue-limit 5 25 40
 wrr-queue random-detect min-threshold 1 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 3 50 60 70 80 90 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 2 100 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 3 60 70 80 90 100 100 100 100
 wrr-queue cos-map 1 1 1
 wrr-queue cos-map 2 1 0
 wrr-queue cos-map 3 1 4
 wrr-queue cos-map 3 2 2
 wrr-queue cos-map 3 3 3
 wrr-queue cos-map 3 4 6
 wrr-queue cos-map 3 5 7
 mls qos trust dscp
 no cdp enable
 spanning-tree guard root
!
interface GigabitEthernet3/2
 description to 3750-acc-2
 dampening
 ip address 10.120.0.5 255.255.255.252
 no ip redirects
 no ip unreachables
```

```
 no ip proxy-arp
 ip hello-interval eigrp 10 1
 ip hold-time eigrp 10 3
 ip authentication mode eigrp 10 md5
 ip authentication key-chain eigrp 10 eigrp
 load-interval 30
 carrier-delay msec 0
 ipv6 address 2001:DB8:CAFE:700B::A111:1010/64
 no ipv6 redirects
 ipv6 nd suppress-ra
 ipv6 cef
 ipv6 ospf network point-to-point
 ipv6 ospf hello-interval 1
 ipv6 ospf dead-interval 3
 ipv6 ospf 1 area 2
 wrr-queue bandwidth 5 25 70
 wrr-queue queue-limit 5 25 40
 wrr-queue random-detect min-threshold 1 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 3 50 60 70 80 90 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 2 100 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 3 60 70 80 90 100 100 100 100
 wrr-queue cos-map 1 1 1
 wrr-queue cos-map 2 1 0
 wrr-queue cos-map 3 1 4
 wrr-queue cos-map 3 2 2
 wrr-queue cos-map 3 3 3
 wrr-queue cos-map 3 4 6
 wrr-queue cos-map 3 5 7
 mls qos trust dscp
 no cdp enable
 spanning-tree guard root
!
interface GigabitEthernet4/1
 description to 6k-core-1
 dampening
 ip address 10.122.0.78 255.255.255.252
 no ip redirects
 no ip proxy-arp
 ip hello-interval eigrp 10 1
 ip hold-time eigrp 10 3
 ip authentication mode eigrp 10 md5
 ip authentication key-chain eigrp 10 eigrp
 ip summary-address eigrp 10 10.120.0.0 255.255.0.0 5
 load-interval 30
 carrier-delay msec 0
 ipv6 address 2001:DB8:CAFE:7000::A111:1010/64
 no ipv6 redirects
 ipv6 nd suppress-ra
 ipv6 cef
 ipv6 ospf network point-to-point
 ipv6 ospf hello-interval 1
 ipv6 ospf dead-interval 3
 ipv6 ospf 1 area 0
 wrr-queue bandwidth 30 70
 wrr-queue queue-limit 40 30
 wrr-queue random-detect min-threshold 1 40 80
 wrr-queue random-detect min-threshold 2 70 80
 wrr-queue random-detect max-threshold 1 80 100
 wrr-queue random-detect max-threshold 2 80 100
 wrr-queue cos-map 1 1 1
 wrr-queue cos-map 1 2 0
 wrr-queue cos-map 2 1 2 3 4
```

```
 wrr-queue cos-map 2 2 6 7
 mls qos trust dscp
!
interface GigabitEthernet4/2
 description to 6k-core-2
 dampening
 ip address 10.122.0.86 255.255.255.252
 no ip redirects
 no ip proxy-arp
 ip hello-interval eigrp 10 1
 ip hold-time eigrp 10 3
 ip authentication mode eigrp 10 md5
 ip authentication key-chain eigrp 10 eigrp
 ip summary-address eigrp 10 10.120.0.0 255.255.0.0 5
 load-interval 30
 carrier-delay msec 0
 ipv6 address 2001:DB8:CAFE:7001::A111:1010/64
 no ipv6 redirects
 ipv6 nd suppress-ra
 ipv6 cef
 ipv6 ospf network point-to-point
 ipv6 ospf hello-interval 1
 ipv6 ospf dead-interval 3
 ipv6 ospf 1 area 0
 wrr-queue bandwidth 30 70
 wrr-queue queue-limit 40 30
 wrr-queue random-detect min-threshold 1 40 80
 wrr-queue random-detect min-threshold 2 70 80
 wrr-queue random-detect max-threshold 1 80 100
 wrr-queue random-detect max-threshold 2 80 100
 wrr-queue cos-map 1 1 1
 wrr-queue cos-map 1 2 0
 wrr-queue cos-map 2 1 2 3 4
 wrr-queue cos-map 2 2 6 7
 mls qos trust dscp
!
router eigrp 10
 passive-interface Loopback0
 network 10.120.0.0 0.0.255.255
 network 10.122.0.0 0.0.0.255
 distribute-list DEFAULT out GigabitEthernet3/1
 distribute-list DEFAULT out GigabitEthernet3/2
 no auto-summary
 eigrp router-id 10.122.10.9
!
ip classless
!
no ip http server
!
ip access-list standard DEFAULT
 permit 0.0.0.0
!
ip access-list extended MGMT-IN-v4
 remark Permit v4MGMT only to Lo0
 permit tcp 10.120.0.0 0.0.255.255 any log-input
 permit tcp 10.121.0.0 0.0.255.255 any log-input
 permit tcp 10.122.0.0 0.0.255.255 any log-input
 deny   ip any any log-input
!
logging source-interface Loopback0
logging 10.121.11.9
ipv6 router ospf 1
 router-id 10.122.10.9
 log-adjacency-changes
```

```
 auto-cost reference-bandwidth 10000
 area 2 stub no-summary
 area 2 range 2001:DB8:CAFE:2::/64 cost 10
 area 2 range 2001:DB8:CAFE:3::/64 cost 10
 area 2 range 2001:DB8:CAFE:7004::/64 cost 10
 area 2 range 2001:DB8:CAFE:700A::/64 cost 10
 area 2 range 2001:DB8:CAFE:700B::/64 cost 10
 passive-interface Loopback0
 timers spf 1 5
!
snmp-server group IPv6-ADMIN v3 auth write v1default
snmp-server contact John Doe - ipv6rocks@cisco.com
!
ipv6 access-list MGMT-IN
 remark Permit MGMT only to Loopback0
 permit tcp 2001:DB8:CAFE::/48 host 2001:DB8:CAFE:6507::A111:1010 log-input
 deny ipv6 any any log-input
!
control-plane
!
dial-peer cor custom
!
banner login ^C
Unauthorized access to this device and/or network is prohibited!
^C
!
line con 0
 session-timeout 3
 password 7 06140E2F4B4B1B
 logging synchronous
 login local
 transport output none
line vty 0 4
 session-timeout 3
 access-class MGMT-IN-v4 in
 password 7 08334D400E1C17
 ipv6 access-class MGMT-IN in
 logging synchronous
 login local
 exec prompt timestamp
 transport input telnet ssh
!
no cns aaa enable
end
```

6k-dist-2

```
upgrade fpd auto
version 12.2
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service password-encryption
service internal
service sequence-numbers
service counters max age 5
!
hostname 6k-dist-2
!
boot system flash sup-bootdisk:s3223-adventerprisek9_wan-mz.122-18.SXF5.bin
```

```
logging buffered 64000 debugging
logging rate-limit 5
no logging console
enable secret 5 $1$0UKB$YN.zu/IQt0ivlkqLsdxtY0
!
username cisco privilege 15 secret 5 $1$SUYV$ShOXyooFT..fL/4tyOnAN1
no aaa new-model
clock timezone mst -7
ip subnet-zero
no ip source-route
ip icmp rate-limit unreachable 2000
!
ip ftp source-interface Loopback0
ip ftp username cisco
ip ftp password 7 01100F175804
ip tftp source-interface Loopback0
no ip bootp server
ip telnet source-interface Loopback0
ip ssh time-out 30
ip ssh authentication-retries 2
ip ssh source-interface Loopback0
ip ssh version 2
no ip domain-lookup
ip domain-name cisco.com
ipv6 unicast-routing
ipv6 mfib hardware-switching replication-mode ingress
ipv6 multicast-routing
udld enable

udld message time 7

vtp domain ese-dc
vtp mode transparent
mls ip cef load-sharing full
mls ip multicast flow-stat-timer 9
no mls flow ip
no mls flow ipv6
mls qos
mls rate-limit unicast ip icmp unreachable acl-drop 0
no mls acl tcam share-global
mls cef error action freeze
!
key chain eigrp
 key 100
  key-string 7 1111
!
redundancy
 mode sso
 main-cpu
  auto-sync running-config
!
spanning-tree mode rapid-pvst
spanning-tree loopguard default
no spanning-tree optimize bpdu transmission
spanning-tree extend system-id
spanning-tree vlan 2-3 priority 28672
environment temperature-controlled
system flowcontrol bus auto
diagnostic cns publish cisco.cns.device.diag_results
diagnostic cns subscribe cisco.cns.device.diag_commands
!
vlan internal allocation policy descending
vlan dot1q tag native
vlan access-log ratelimit 2000
```

```
!
interface Loopback0
 ip address 10.122.10.10 255.255.255.255
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ipv6 address 2001:DB8:CAFE:6507::B222:2020/128
 no ipv6 redirects
 ipv6 ospf 1 area 0
!
interface Null0
 no ip unreachables
!
interface TenGigabitEthernet1/1
 description to 6k-dist-1
 dampening
 ip address 10.120.0.14 255.255.255.252
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ip hello-interval eigrp 10 1
 ip hold-time eigrp 10 3
 ip authentication mode eigrp 10 md5
 ip authentication key-chain eigrp 10 eigrp
 load-interval 30
 carrier-delay msec 0
 ipv6 address 2001:DB8:CAFE:7004::B222:2020/64
 no ipv6 redirects
 ipv6 nd suppress-ra
 ipv6 cef
 ipv6 ospf network point-to-point
 ipv6 ospf hello-interval 1
 ipv6 ospf dead-interval 3
 ipv6 ospf 1 area 2
 wrr-queue bandwidth 5 25 70
 wrr-queue queue-limit 5 25 40
 wrr-queue random-detect min-threshold 1 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 3 50 60 70 80 90 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 2 100 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 3 60 70 80 90 100 100 100 100
 wrr-queue cos-map 1 1 1
 wrr-queue cos-map 2 1 0
 wrr-queue cos-map 3 1 4
 wrr-queue cos-map 3 2 2
 wrr-queue cos-map 3 3 3
 wrr-queue cos-map 3 4 6
 wrr-queue cos-map 3 5 7
 mls qos trust dscp
!
interface GigabitEthernet3/1
 description to 3750-acc-1
 dampening
 ip address 10.120.0.9 255.255.255.252
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ip hello-interval eigrp 10 1
 ip hold-time eigrp 10 3
 ip authentication mode eigrp 10 md5
 ip authentication key-chain eigrp 10 eigrp
 load-interval 30
 carrier-delay msec 0
```

```
 ipv6 address 2001:DB8:CAFE:700C::B222:2020/64
 no ipv6 redirects
 ipv6 nd suppress-ra
 ipv6 cef
 ipv6 ospf network point-to-point
 ipv6 ospf hello-interval 1
 ipv6 ospf dead-interval 3
 ipv6 ospf 1 area 2
 wrr-queue bandwidth 5 25 70
 wrr-queue queue-limit 5 25 40
 wrr-queue random-detect min-threshold 1 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 3 50 60 70 80 90 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 2 100 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 3 60 70 80 90 100 100 100 100
 wrr-queue cos-map 1 1 1
 wrr-queue cos-map 2 1 0
 wrr-queue cos-map 3 1 4
 wrr-queue cos-map 3 2 2
 wrr-queue cos-map 3 3 3
 wrr-queue cos-map 3 4 6
 wrr-queue cos-map 3 5 7
 mls qos trust dscp
 no cdp enable
!
interface GigabitEthernet3/2
 description to 3750-acc-1
 dampening
 ip address 10.120.0.17 255.255.255.252
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ip hello-interval eigrp 10 1
 ip hold-time eigrp 10 3
 ip authentication mode eigrp 10 md5
 ip authentication key-chain eigrp 10 eigrp
 load-interval 30
 carrier-delay msec 0
 ipv6 address 2001:DB8:CAFE:700D::B222:2020/64
 no ipv6 redirects
 ipv6 nd suppress-ra
 ipv6 cef
 ipv6 ospf network point-to-point
 ipv6 ospf hello-interval 1
 ipv6 ospf dead-interval 3
 ipv6 ospf 1 area 2
 wrr-queue bandwidth 5 25 70
 wrr-queue queue-limit 5 25 40
 wrr-queue random-detect min-threshold 1 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 2 80 100 100 100 100 100 100 100
 wrr-queue random-detect min-threshold 3 50 60 70 80 90 100 100 100
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 2 100 100 100 100 100 100 100 100
 wrr-queue random-detect max-threshold 3 60 70 80 90 100 100 100 100
 wrr-queue cos-map 1 1 1
 wrr-queue cos-map 2 1 0
 wrr-queue cos-map 3 1 4
 wrr-queue cos-map 3 2 2
 wrr-queue cos-map 3 3 3
 wrr-queue cos-map 3 4 6
 wrr-queue cos-map 3 5 7
 mls qos trust dscp
 no cdp enable
```

```
!
interface GigabitEthernet4/1
 description to 6k-core-1
 dampening
 ip address 10.122.0.82 255.255.255.252
 no ip redirects
 no ip proxy-arp
 ip hello-interval eigrp 10 1
 ip hold-time eigrp 10 3
 ip authentication mode eigrp 10 md5
 ip authentication key-chain eigrp 10 eigrp
 load-interval 30
 carrier-delay msec 0
 ipv6 address 2001:DB8:CAFE:7002::B222:2020/64
 no ipv6 redirects
 ipv6 nd suppress-ra
 ipv6 cef
 ipv6 ospf network point-to-point
 ipv6 ospf hello-interval 1
 ipv6 ospf dead-interval 3
 ipv6 ospf 1 area 0
 wrr-queue bandwidth 30 70
 wrr-queue queue-limit 40 30
 wrr-queue random-detect min-threshold 1 40 80
 wrr-queue random-detect min-threshold 2 70 80
 wrr-queue random-detect max-threshold 1 80 100
 wrr-queue random-detect max-threshold 2 80 100
 wrr-queue cos-map 1 1 1
 wrr-queue cos-map 1 2 0
 wrr-queue cos-map 2 1 2 3 4
 wrr-queue cos-map 2 2 6 7
 mls qos trust dscp
!
interface GigabitEthernet4/2
 description to 6k-core-2
 dampening
 ip address 10.122.0.90 255.255.255.252
 no ip redirects
 no ip proxy-arp
 ip hello-interval eigrp 10 1
 ip hold-time eigrp 10 3
 ip authentication mode eigrp 10 md5
 ip authentication key-chain eigrp 10 eigrp
 load-interval 30
 carrier-delay msec 0
 ipv6 address 2001:DB8:CAFE:7003::B222:2020/64
 no ipv6 redirects
 ipv6 nd suppress-ra
 ipv6 cef
 ipv6 ospf network point-to-point
 ipv6 ospf hello-interval 1
 ipv6 ospf dead-interval 3
 ipv6 ospf 1 area 0
 wrr-queue bandwidth 30 70
 wrr-queue queue-limit 40 30
 wrr-queue random-detect min-threshold 1 40 80
 wrr-queue random-detect min-threshold 2 70 80
 wrr-queue random-detect max-threshold 1 80 100
 wrr-queue random-detect max-threshold 2 80 100
 wrr-queue cos-map 1 1 1
 wrr-queue cos-map 1 2 0
 wrr-queue cos-map 2 1 2 3 4
 wrr-queue cos-map 2 2 6 7
 mls qos trust dscp
```

```
!
router eigrp 10
 passive-interface Loopback0
 network 10.120.0.0 0.0.255.255
 network 10.122.0.0 0.0.0.255
 distribute-list DEFAULT out GigabitEthernet3/1
 distribute-list DEFAULT out GigabitEthernet3/2
 no auto-summary
 eigrp router-id 10.122.10.10
!
ip classless
!
no ip http server
!
ip access-list standard DEFAULT
 permit 0.0.0.0
!
ip access-list extended MGMT-IN-v4
 remark Permit v4MGMT only to Lo0
 permit tcp 10.120.0.0 0.0.255.255 any log-input
 permit tcp 10.121.0.0 0.0.255.255 any log-input
 permit tcp 10.122.0.0 0.0.255.255 any log-input
 deny   ip any any log-input
!
logging source-interface Loopback0
logging 10.121.11.9
ipv6 router ospf 1
 router-id 10.122.10.10
 log-adjacency-changes
 auto-cost reference-bandwidth 10000
 area 2 stub no-summary
 area 2 range 2001:DB8:CAFE:2::/64 cost 10
 area 2 range 2001:DB8:CAFE:3::/64 cost 10
 area 2 range 2001:DB8:CAFE:7004::/64 cost 10
 area 2 range 2001:DB8:CAFE:700A::/64 cost 10
 area 2 range 2001:DB8:CAFE:700B::/64 cost 10
 passive-interface Loopback0
 timers spf 1 5
!
snmp-server group IPv6-ADMIN v3 auth write v1default
snmp-server contact John Doe - ipv6rocks@cisco.com
!
ipv6 access-list MGMT-IN
 remark Permit MGMT only to Loopback0
 permit tcp 2001:DB8:CAFE::/48 host 2001:DB8:CAFE:6507::B222:2020 log-input
 deny ipv6 any any log-input
!
control-plane
!
dial-peer cor custom
!
banner login ^C

Unauthorized access to this device and network is prohibited.

^C
!
line con 0
 session-timeout 3
 password 7 1317161C0C0916
 logging synchronous
 login local
 transport output telnet ssh
line vty 0 4
```

```
 session-timeout 3
 access-class MGMT-IN-v4 in
 password 7 071D2042490C0B
 ipv6 access-class MGMT-IN in
 logging synchronous
 login local
 exec prompt timestamp
 transport input telnet ssh
!
no cns aaa enable
end
```

ハイブリッド モデル例 1（HME1）

ここではコア レイヤについてのみ設定を示します。その他のレイヤはすべて IPv4 のみであり、それらの設定は DSM での IPv4 設定と同じです（ディストリビューション レイヤに、少々アドレスの変更があります）。

6k-core-1

```
upgrade fpd auto
version 12.2
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service password-encryption
service internal
service sequence-numbers
service counters max age 5
!
hostname 6k-core-1
!
boot system flash sup-bootdisk:s3223-adventerprisek9_wan-mz.122-18.SXF5.bin
logging buffered 64000 debugging
logging rate-limit 5
no logging console
enable secret 5 $1$hHvm$ln0YNSdCb7lzgHMmFz9Bi0
!
username cisco privilege 15 password 7 120B0419150E1E
no aaa new-model
clock timezone mst -7
ip subnet-zero
no ip source-route
ip icmp rate-limit unreachable 2000
!
ip ftp source-interface Loopback0
ip ftp username cisco
ip ftp password 7 071D2042490C0B
ip tftp source-interface Loopback0
no ip bootp server
ip telnet source-interface Loopback0
ip ssh time-out 30
ip ssh authentication-retries 2
ip ssh source-interface Loopback0
ip ssh version 2
no ip domain-lookup
ip domain-name cisco.com
ipv6 unicast-routing
```

```
ipv6 mfib hardware-switching replication-mode ingress
ipv6 multicast-routing
udld enable

udld message time 7

vtp domain ese-dc
vtp mode transparent
mls ip multicast flow-stat-timer 9
no mls flow ip
no mls flow ipv6
mls qos
mls rate-limit unicast ip icmp unreachable acl-drop 0
no mls acl tcam share-global
mls cef error action freeze
!
key chain eigrp
 key 100
  key-string 7 1111
!
redundancy
 mode sso
 main-cpu
  auto-sync running-config
!
spanning-tree mode rapid-pvst
spanning-tree loopguard default
no spanning-tree optimize bpdu transmission
spanning-tree extend system-id
environment temperature-controlled
system flowcontrol bus auto
diagnostic cns publish cisco.cns.device.diag_results
diagnostic cns subscribe cisco.cns.device.diag_commands
!
vlan internal allocation policy descending
vlan dot1q tag native
vlan access-log ratelimit 2000
!
class-map match-all CAMPUS-BULK-DATA
  match access-group name BULK-APPS
class-map match-all CAMPUS-TRANSACTIONAL-DATA
  match access-group name TRANSACTIONAL-APPS
!
policy-map IPv6-ISATAP-MARK
  class CAMPUS-BULK-DATA
   set dscp af11
  class CAMPUS-TRANSACTIONAL-DATA
   set dscp af21
  class class-default
   set dscp default
!
interface Loopback0
 ip address 10.122.10.3 255.255.255.255
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ipv6 address 2001:DB8:CAFE:6507::C333:3030/128
 no ipv6 redirects
 ipv6 ospf 1 area 0
!
interface Loopback2
 description Tunnel source for ISATAP-VLAN2
 ip address 10.122.10.102 255.255.255.255
 no ip redirects
```

```
 no ip unreachables
 no ip proxy-arp
!
interface Loopback3
 description Tunnel source for ISATAP-VLAN3
 ip address 10.122.10.103 255.255.255.255
 no ip redirects
 no ip unreachables
 no ip proxy-arp
!
interface Tunnel2
 description ISATAP VLAN2
 no ip address
 no ip redirects
 ipv6 address 2001:DB8:CAFE:2::/64 eui-64
 ipv6 traffic-filter SOURCE-ISATAP-2 in
 no ipv6 redirects
 no ipv6 nd suppress-ra
 ipv6 cef
 ipv6 ospf 1 area 2
 tunnel source Loopback2
 tunnel mode ipv6ip isatap
!
interface Tunnel3
 description ISATAP VLAN3
 no ip address
 no ip redirects
 ipv6 address 2001:DB8:CAFE:3::/64 eui-64
 ipv6 traffic-filter SOURCE-ISATAP-3 in
 no ipv6 redirects
 no ipv6 nd suppress-ra
 ipv6 cef
 ipv6 ospf 1 area 2
 tunnel source Loopback3
 tunnel mode ipv6ip isatap
!
interface Null0
 no ip unreachables
!
interface GigabitEthernet1/1
 description to 3750-dist-1
 dampening
 ip address 10.122.0.41 255.255.255.252
 no ip redirects
 no ip proxy-arp
 ip hello-interval eigrp 10 1
 ip hold-time eigrp 10 3
 load-interval 30
 carrier-delay msec 0
 mls qos trust dscp
!
interface GigabitEthernet1/2
 description to 3750-dist-2
 dampening
 ip address 10.122.0.45 255.255.255.252
 no ip redirects
 no ip proxy-arp
 ip hello-interval eigrp 10 1
 ip hold-time eigrp 10 3
 load-interval 30
 carrier-delay msec 0
 mls qos trust dscp
!
interface GigabitEthernet2/1
```

```
 description to 6k-agg-1
 dampening
 ip address 10.122.0.26 255.255.255.252
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ip hello-interval eigrp 10 1
 ip hold-time eigrp 10 3
 ip authentication mode eigrp 10 md5
 ip authentication key-chain eigrp 10 eigrp
 load-interval 30
 carrier-delay msec 0
 ipv6 address 2001:DB8:CAFE:7005::C333:3030/64
 no ipv6 redirects
 ipv6 nd suppress-ra
 ipv6 cef
 ipv6 ospf network point-to-point
 ipv6 ospf hello-interval 1
 ipv6 ospf dead-interval 3
 ipv6 ospf 1 area 0
 wrr-queue bandwidth 30 70
 wrr-queue queue-limit 30 70
 wrr-queue threshold 1 40 100
 wrr-queue cos-map 1 1 1
 wrr-queue cos-map 1 2 0
 wrr-queue cos-map 2 1 2 3 4 6 7
 wrr-queue cos-map 2 2 5
 mls qos trust dscp
 service-policy output IPv6-ISATAP-MARK
!
interface GigabitEthernet2/2
 description to 6k-agg-2
 dampening
 ip address 10.122.0.34 255.255.255.252
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ip hello-interval eigrp 10 1
 ip hold-time eigrp 10 3
 ip authentication mode eigrp 10 md5
 ip authentication key-chain eigrp 10 eigrp
 load-interval 30
 carrier-delay msec 0
 ipv6 address 2001:DB8:CAFE:7006::C333:3030/64
 no ipv6 redirects
 ipv6 nd suppress-ra
 ipv6 cef
 ipv6 ospf network point-to-point
 ipv6 ospf hello-interval 1
 ipv6 ospf dead-interval 3
 ipv6 ospf 1 area 0
 wrr-queue bandwidth 30 70
 wrr-queue queue-limit 30 70
 wrr-queue threshold 1 40 100
 wrr-queue cos-map 1 1 1
 wrr-queue cos-map 1 2 0
 wrr-queue cos-map 2 1 2 3 4 6 7
 wrr-queue cos-map 2 2 5
 mls qos trust dscp
 service-policy output IPv6-ISATAP-MARK
!
interface GigabitEthernet2/3
 description to 6k-core-2
 dampening
```

```
 ip address 10.122.0.21 255.255.255.252
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ip hello-interval eigrp 10 1
 ip hold-time eigrp 10 3
 ip authentication mode eigrp 10 md5
 ip authentication key-chain eigrp 10 eigrp
 load-interval 30
 carrier-delay msec 0
 ipv6 address 2001:DB8:CAFE:7009::C333:3030/64
 no ipv6 redirects
 ipv6 nd suppress-ra
 ipv6 cef
 ipv6 ospf network point-to-point
 ipv6 ospf hello-interval 1
 ipv6 ospf dead-interval 3
 ipv6 ospf 1 area 0
 wrr-queue bandwidth 30 70
 wrr-queue queue-limit 30 70
 wrr-queue threshold 1 40 100
 wrr-queue cos-map 1 1 1
 wrr-queue cos-map 1 2 0
 wrr-queue cos-map 2 1 2 3 4 6 7
 wrr-queue cos-map 2 2 5
 mls qos trust dscp
!
router eigrp 10
 passive-interface Loopback0
 passive-interface Loopback2
 passive-interface Loopback3
 network 10.0.0.0
 no auto-summary
 eigrp router-id 10.122.10.3
!
ip classless
!
no ip http server
!
ip access-list extended MGMT-IN-v4
 remark Permit v4MGMT only to Lo0
 permit tcp 10.120.0.0 0.0.255.255 any log-input
 permit tcp 10.121.0.0 0.0.255.255 any log-input
 permit tcp 10.122.0.0 0.0.255.255 any log-input
 deny   ip any any log-input
!
logging source-interface Loopback0
logging 10.121.11.9
ipv6 router ospf 1
 router-id 10.122.10.3
 log-adjacency-changes
 auto-cost reference-bandwidth 10000
 area 2 range 2001:DB8:CAFE:2::/64 cost 10
 area 2 range 2001:DB8:CAFE:3::/64 cost 10
 passive-interface Loopback0
 passive-interface Loopback2
 passive-interface Loopback3
 passive-interface Tunnel2
 passive-interface Tunnel3
 timers spf 1 5
!
snmp-server group IPv6-ADMIN v3 auth write v1default
snmp-server contact John Doe - IPv6 ipv6rocks@cisco.com
!
```

```
ipv6 access-list SOURCE-ISATAP-2
 remark PERMIT ICMPv6 PACKETS FROM HOSTS WITH PREFIX 2001:DB8:CAFE:2::/64
 permit icmp 2001:DB8:CAFE:2::/64 any
 remark PERMIT IPv6 PACKETS FROM HOSTS WITH PREFIX 2001:DB8:CAFE:2::64
 permit ipv6 2001:DB8:CAFE:2::/64 any
 remark PERMIT ALL ICMPv6 PACKETS SOURCED BY HOSTS USING THE LINK-LOCAL PREFIX
 permit icmp FE80::/10 any
 remark DENY ALL OTHER IPv6 PACKETS AND LOG
 deny ipv6 any any log-input
!
ipv6 access-list SOURCE-ISATAP-3
 remark PERMIT ICMPv6 PACKETS FROM HOSTS WITH PREFIX 2001:DB8:CAFE:3::/64
 permit icmp 2001:DB8:CAFE:3::/64 any
 remark PERMIT IPv6 PACKETS FROM HOSTS WITH PREFIX 2001:DB8:CAFE:3::64
 permit ipv6 2001:DB8:CAFE:3::/64 any
 remark PERMIT ALL ICMPv6 PACKETS SOURCED BY HOSTS USING THE LINK-LOCAL PREFIX
 permit icmp FE80::/10 any
 remark DENY ALL OTHER IPv6 PACKETS AND LOG
 deny ipv6 any any log-input
!
ipv6 access-list BULK-APPS
 permit tcp any any eq ftp
 permit tcp any any eq ftp-data
!
ipv6 access-list TRANSACTIONAL-APPS
 permit tcp any any eq telnet
 permit tcp any any eq 22
!
ipv6 access-list MGMT-IN
 remark Permit MGMT only to Loopback0
 permit tcp 2001:DB8:CAFE::/48 host 2001:DB8:CAFE:6507::C333:3030 log-input
 deny ipv6 any any log-input
!
control-plane
!
dial-peer cor custom
!
banner login ^C
Unauthorized access to this device and/or network is prohibited.
^C
!
line con 0
 session-timeout 3
 exec-timeout 0 0
 password 7 095E4F071E0005
 logging synchronous
 login local
 transport output telnet ssh
line vty 0 4
 session-timeout 3
 access-class MGMT-IN-v4 in
 exec-timeout 30 0
 password 7 03165A05010A33
 ipv6 access-class MGMT-IN in
 logging synchronous
 login local
 exec prompt timestamp
 transport input telnet ssh
!
no cns aaa enable
end
```

6k-core-2

```
upgrade fpd auto
version 12.2
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service password-encryption
service internal
service sequence-numbers
service counters max age 5
!
hostname 6k-core-2
!
boot system flash sup-bootdisk:s3223-adventerprisek9_wan-mz.122-18.SXF5.bin
logging buffered 64000 debugging
logging rate-limit 5
no logging console
enable secret 5 $1$W031$3oHUmVfyHXW7fwdMWEBq01
!
username cisco privilege 15 secret 5 $1$vVK6$2OGixA1lDE.ufYBqWUrru/
no aaa new-model
clock timezone mst -7
ip subnet-zero
no ip source-route
ip icmp rate-limit unreachable 2000
!
ip ftp source-interface Loopback0
ip ftp username cisco
ip ftp password 7 111B180B101719
ip tftp source-interface Loopback0
no ip bootp server
ip telnet source-interface Loopback0
ip ssh time-out 30
ip ssh authentication-retries 2
ip ssh source-interface Loopback0
ip ssh version 2
no ip domain-lookup
ip domain-name cisco.com
ipv6 unicast-routing
ipv6 mfib hardware-switching replication-mode ingress
ipv6 multicast-routing
udld enable

udld message time 7

vtp domain ese-dc
vtp mode transparent
mls ip multicast flow-stat-timer 9
no mls flow ip
no mls flow ipv6
mls qos
mls rate-limit unicast ip icmp unreachable acl-drop 0
no mls acl tcam share-global
mls cef error action freeze
!
key chain eigrp
 key 100
  key-string 7 1111
!
redundancy
```

```
 mode sso
 main-cpu
  auto-sync running-config
!
spanning-tree mode rapid-pvst
spanning-tree loopguard default
no spanning-tree optimize bpdu transmission
spanning-tree extend system-id
environment temperature-controlled
system flowcontrol bus auto
diagnostic cns publish cisco.cns.device.diag_results
diagnostic cns subscribe cisco.cns.device.diag_commands
!
vlan internal allocation policy descending
vlan dot1q tag native
vlan access-log ratelimit 2000
!
class-map match-all CAMPUS-BULK-DATA
  match access-group name BULK-APPS
class-map match-all CAMPUS-TRANSACTIONAL-DATA
  match access-group name TRANSACTIONAL-APPS
!
policy-map IPv6-ISATAP-MARK
  class CAMPUS-BULK-DATA
   set dscp af11
  class CAMPUS-TRANSACTIONAL-DATA
   set dscp af21
  class class-default
   set dscp default
!
interface Loopback0
 ip address 10.122.10.4 255.255.255.255
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ipv6 address 2001:DB8:CAFE:6507::D444:4040/64
 no ipv6 redirects
 ipv6 ospf 1 area 0
!
interface Loopback2
 description Tunnel source for ISATAP-VLAN2
 ip address 10.122.10.102 255.255.255.255
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 delay 1000
!
interface Loopback3
 description Tunnel source for ISATAP-VLAN3
 ip address 10.122.10.103 255.255.255.255
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 delay 1000
!
interface Tunnel2
 description ISATAP VLAN2
 no ip address
 no ip redirects
 ipv6 address 2001:DB8:CAFE:2::/64 eui-64
 ipv6 traffic-filter SOURCE-ISATAP-2 in
 no ipv6 redirects
 no ipv6 nd suppress-ra
 ipv6 cef
```

```
 ipv6 ospf 1 area 2
 tunnel source Loopback2
 tunnel mode ipv6ip isatap
!
interface Tunnel3
 description ISATAP VLAN3
 no ip address
 no ip redirects
 ipv6 address 2001:DB8:CAFE:3::/64 eui-64
 ipv6 traffic-filter SOURCE-ISATAP-3 in
 no ipv6 redirects
 no ipv6 nd suppress-ra
 ipv6 cef
 ipv6 ospf 1 area 2
 tunnel source Loopback3
 tunnel mode ipv6ip isatap
!
interface Null0
 no ip unreachables
!
interface GigabitEthernet1/1
 description to 3750-dist-1
 dampening
 ip address 10.122.0.49 255.255.255.252
 no ip redirects
 no ip proxy-arp
 ip hello-interval eigrp 10 1
 ip hold-time eigrp 10 3
 load-interval 30
 carrier-delay msec 0
 mls qos trust dscp
!
interface GigabitEthernet1/2
 description to 3750-dist-2
 dampening
 ip address 10.122.0.53 255.255.255.252
 no ip redirects
 no ip proxy-arp
 ip hello-interval eigrp 10 1
 ip hold-time eigrp 10 3
 load-interval 30
 carrier-delay msec 0
 mls qos trust dscp
!
interface GigabitEthernet2/1
 description to 6k-agg-1
 dampening
 ip address 10.122.0.30 255.255.255.252
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ip hello-interval eigrp 10 1
 ip hold-time eigrp 10 3
 ip authentication mode eigrp 10 md5
 ip authentication key-chain eigrp 10 eigrp
 load-interval 30
 carrier-delay msec 0
 ipv6 address 2001:DB8:CAFE:7007::D444:4040/64
 no ipv6 redirects
 ipv6 nd suppress-ra
 ipv6 cef
 ipv6 ospf network point-to-point
 ipv6 ospf hello-interval 1
 ipv6 ospf dead-interval 3
```

```
 ipv6 ospf 1 area 0
 wrr-queue bandwidth 30 70
 wrr-queue queue-limit 40 30
 wrr-queue random-detect min-threshold 1 40 80
 wrr-queue random-detect min-threshold 2 70 80
 wrr-queue random-detect max-threshold 1 80 100
 wrr-queue random-detect max-threshold 2 80 100
 wrr-queue cos-map 1 1 1
 wrr-queue cos-map 1 2 0
 wrr-queue cos-map 2 1 2 3 4
 wrr-queue cos-map 2 2 6 7
 mls qos trust dscp
 service-policy output IPv6-ISATAP-MARK

!
interface GigabitEthernet2/2
 description to 6k-agg-2
 dampening
 ip address 10.122.0.38 255.255.255.252
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ip hello-interval eigrp 10 1
 ip hold-time eigrp 10 3
 ip authentication mode eigrp 10 md5
 ip authentication key-chain eigrp 10 eigrp
 load-interval 30
 carrier-delay msec 0
 ipv6 address 2001:DB8:CAFE:7008::D444:4040/64
 no ipv6 redirects
 ipv6 nd suppress-ra
 ipv6 cef
 ipv6 ospf network point-to-point
 ipv6 ospf hello-interval 1
 ipv6 ospf dead-interval 3
 ipv6 ospf 1 area 0
 wrr-queue bandwidth 30 70
 wrr-queue queue-limit 40 30
 wrr-queue random-detect min-threshold 1 40 80
 wrr-queue random-detect min-threshold 2 70 80
 wrr-queue random-detect max-threshold 1 80 100
 wrr-queue random-detect max-threshold 2 80 100
 wrr-queue cos-map 1 1 1
 wrr-queue cos-map 1 2 0
 wrr-queue cos-map 2 1 2 3 4
 wrr-queue cos-map 2 2 6 7
 mls qos trust dscp
 service-policy output IPv6-ISATAP-MARK
!
interface GigabitEthernet2/3
 description to 6k-core-1
 dampening
 ip address 10.122.0.22 255.255.255.252
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ip hello-interval eigrp 10 1
 ip hold-time eigrp 10 3
 ip authentication mode eigrp 10 md5
 ip authentication key-chain eigrp 10 eigrp
 load-interval 30
 carrier-delay msec 0
 ipv6 address 2001:DB8:CAFE:7009::D444:4040/64
 no ipv6 redirects
```

```
 ipv6 nd suppress-ra
 ipv6 cef
 ipv6 ospf network point-to-point
 ipv6 ospf hello-interval 1
 ipv6 ospf dead-interval 3
 ipv6 ospf 1 area 0
 wrr-queue bandwidth 30 70
 wrr-queue queue-limit 40 30
 wrr-queue random-detect min-threshold 1 40 80
 wrr-queue random-detect min-threshold 2 70 80
 wrr-queue random-detect max-threshold 1 80 100
 wrr-queue random-detect max-threshold 2 80 100
 wrr-queue cos-map 1 1 1
 wrr-queue cos-map 1 2 0
 wrr-queue cos-map 2 1 2 3 4
 wrr-queue cos-map 2 2 6 7
 mls qos trust dscp
!
router eigrp 10
 passive-interface Loopback0
 passive-interface Loopback2
 passive-interface Loopback3
 network 10.0.0.0
 no auto-summary
 eigrp router-id 10.122.10.4
!
ip classless
!
no ip http server
!
ip access-list extended MGMT-IN-v4
 remark Permit v4MGMT only to Lo0
 permit tcp 10.120.0.0 0.0.255.255 any log-input
 permit tcp 10.121.0.0 0.0.255.255 any log-input
 permit tcp 10.122.0.0 0.0.255.255 any log-input
 deny   ip any any log-input
!
logging source-interface Loopback0
logging 10.121.11.9
ipv6 router ospf 1
 router-id 10.122.10.4
 log-adjacency-changes
 auto-cost reference-bandwidth 10000
 area 2 range 2001:DB8:CAFE:2::/64 cost 20
 area 2 range 2001:DB8:CAFE:3::/64 cost 20
 passive-interface Loopback0
 passive-interface Loopback2
 passive-interface Loopback3
 passive-interface Tunnel2
 passive-interface Tunnel3
 timers spf 1 5
!
!
snmp-server group IPv6-ADMIN v3 auth write v1default
snmp-server contact John Doe - IPv6 ipv6rocks@cisco.com
!
ipv6 access-list SOURCE-ISATAP-2
 remark PERMIT ICMPv6 PACKETS FROM HOSTS WITH PREFIX 2001:DB8:CAFE:2::/64
 permit icmp 2001:DB8:CAFE:2::/64 any
 remark PERMIT IPv6 PACKETS FROM HOSTS WITH PREFIX 2001:DB8:CAFE:2::64
 permit ipv6 2001:DB8:CAFE:2::/64 any
 remark PERMIT ALL ICMPv6 PACKETS SOURCED BY HOSTS USING THE LINK-LOCAL PREFIX
 permit icmp FE80::/10 any
 remark DENY ALL OTHER IPv6 PACKETS AND LOG
```

```
 deny ipv6 any any log-input
!
ipv6 access-list SOURCE-ISATAP-3
 remark PERMIT ICMPv6 PACKETS FROM HOSTS WITH PREFIX 2001:DB8:CAFE:3::/64
 permit icmp 2001:DB8:CAFE:3::/64 any
 remark PERMIT IPv6 PACKETS FROM HOSTS WITH PREFIX 2001:DB8:CAFE:3::64
 permit ipv6 2001:DB8:CAFE:3::/64 any
 remark PERMIT ALL ICMPv6 PACKETS SOURCED BY HOSTS USING THE LINK-LOCAL PREFIX
 permit icmp FE80::/10 any
 remark DENY ALL OTHER IPv6 PACKETS AND LOG
 deny ipv6 any any log-input
!
ipv6 access-list BULK-APPS
 permit tcp any any eq ftp
 permit tcp any any eq ftp-data
!
ipv6 access-list TRANSACTIONAL-APPS
 permit tcp any any eq telnet
 permit tcp any any eq 22
!
ipv6 access-list MGMT-IN
 remark Permit MGMT only to Loopback0
 permit tcp 2001:DB8:CAFE::/48 host 2001:DB8:CAFE:6507::D444:4040 log-input
 deny ipv6 any any log-input
!
control-plane
!
dial-peer cor custom
!
banner login ^C
Unauthorized access to this device and/or network is prohibited.
^C
!
line con 0
 session-timeout 3
 exec-timeout 0 0
 password 7 120B0419150E1E
 logging synchronous
 login local
 transport output telnet ssh
line vty 0 4
 session-timeout 3
 access-class MGMT-IN-v4 in
 exec-timeout 30 0
 password 7 105C0817021200
 ipv6 access-class MGMT-IN in
 logging synchronous
 login local
 exec prompt timestamp
 transport input telnet ssh
!
no cns aaa enable
end
```

サービス ブロック モデル（SBM）

ここでは、サービス ブロック スイッチ（6k-sb-1/6k-sb-2）についてのみ設定を示します。アクセス、ディストリビューション、およびコア レイヤのその他の設定はすべて、DSM セクションで示した IPv4 設定を使用します。

6k-sb-1

```
upgrade fpd auto
version 12.2
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service password-encryption
service internal
service sequence-numbers
service counters max age 5
!
hostname 6k-sb-1
!
boot system flash sup-bootdisk:s3223-adventerprisek9_wan-mz.122-18.SXF5.bin
logging buffered 64000 debugging
logging rate-limit 5
no logging console
enable secret 5 $1$EZB7$nbqNvH9QH4qo3zpGsZog6/
!
username cisco privilege 15 secret 5 $1$VwbR$aXCTEAusOPhpmcfg7nOn01
no aaa new-model
clock timezone mst -7
ip subnet-zero
no ip source-route
ip icmp rate-limit unreachable 2000
!
ip ftp source-interface Loopback0
ip ftp username cisco
ip ftp password 7 121A0C041104
ip tftp source-interface Loopback0
no ip bootp server
ip telnet source-interface Loopback0
ip ssh time-out 30
ip ssh authentication-retries 2
ip ssh source-interface Loopback0
ip ssh version 2
no ip domain-lookup
ip domain-name cisco.com
ipv6 unicast-routing
ipv6 mfib hardware-switching replication-mode ingress
udld enable

udld message time 7

vtp domain ese-dc
vtp mode transparent
mls ip cef load-sharing full
mls ip multicast flow-stat-timer 9
no mls flow ip
no mls flow ipv6
mls qos
mls rate-limit unicast ip icmp unreachable acl-drop 0
no mls acl tcam share-global
mls cef error action freeze
!
key chain eigrp
 key 100
  key-string 7 1111
!
redundancy
```

```
 mode sso
 main-cpu
  auto-sync running-config
!
spanning-tree mode rapid-pvst
spanning-tree loopguard default
no spanning-tree optimize bpdu transmission
spanning-tree extend system-id
environment temperature-controlled
system flowcontrol bus auto
diagnostic cns publish cisco.cns.device.diag_results
diagnostic cns subscribe cisco.cns.device.diag_commands
!
vlan internal allocation policy descending
vlan dot1q tag native
vlan access-log ratelimit 2000
!
class-map match-all CAMPUS-BULK-DATA
  match access-group name BULK-APPS
class-map match-all CAMPUS-TRANSACTIONAL-DATA
  match access-group name TRANSACTIONAL-APPS
!
policy-map IPv6-ISATAP-MARK
  class CAMPUS-BULK-DATA
   set dscp af11
  class CAMPUS-TRANSACTIONAL-DATA
   set dscp af21
  class class-default
   set dscp default
!
interface Loopback0
 description Tunnel source for 6k-agg-1
 ip address 10.122.10.9 255.255.255.255
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ipv6 address 2001:DB8:CAFE:6507::A111:1010/128
 no ipv6 redirects
 ipv6 ospf 1 area 0
!
interface Loopback1
 description Tunnel source for 6k-agg-2
 ip address 10.122.10.19 255.255.255.255
 no ip redirects
 no ip unreachables
 no ip proxy-arp
!
interface Loopback2
 description Tunnel source for ISATAP-VLAN2
 ip address 10.122.10.102 255.255.255.255
 no ip redirects
 no ip unreachables
 no ip proxy-arp
!
interface Loopback3
 description Tunnel source for ISATAP-VLAN3
 ip address 10.122.10.103 255.255.255.255
 no ip redirects
 no ip unreachables
 no ip proxy-arp
!
interface Tunnel0
 description tunnel to 6k-agg-1
 no ip address
```

```
 ipv6 address 2001:DB8:CAFE:6501::A111:1010/64
 no ipv6 redirects
 ipv6 nd reachable-time 5000
 ipv6 cef
 ipv6 ospf network point-to-point
 ipv6 ospf hello-interval 1
 ipv6 ospf dead-interval 3
 ipv6 ospf 1 area 0
 tunnel source Loopback0
 tunnel destination 10.122.10.1
 tunnel mode ipv6ip
 service-policy output IPv6-ISATAP-MARK
!
interface Tunnel1
 description tunnel to 6k-agg-2
 no ip address
 ipv6 address 2001:DB8:CAFE:6502::A111:1010/64
 no ipv6 redirects
 ipv6 nd reachable-time 5000
 ipv6 cef
 ipv6 ospf network point-to-point
 ipv6 ospf hello-interval 1
 ipv6 ospf dead-interval 3
 ipv6 ospf 1 area 0
 tunnel source Loopback1
 tunnel destination 10.122.10.2
 tunnel mode ipv6ip
 service-policy output IPv6-ISATAP-MARK
!
interface Tunnel2
 description ISATAP VLAN2
 no ip address
 no ip redirects
 ipv6 address 2001:DB8:CAFE:2::/64 eui-64
 ipv6 traffic-filter SOURCE-ISATAP-2 in
 no ipv6 redirects
 no ipv6 nd suppress-ra
 ipv6 cef
 ipv6 ospf 1 area 2
 tunnel source Loopback2
 tunnel mode ipv6ip isatap
!
interface Tunnel3
 description ISATAP VLAN3
 no ip address
 no ip redirects
 ipv6 address 2001:DB8:CAFE:3::/64 eui-64
 ipv6 traffic-filter SOURCE-ISATAP-3 in
 no ipv6 redirects
 no ipv6 nd suppress-ra
 ipv6 cef
 ipv6 ospf 1 area 2
 tunnel source Loopback3
 tunnel mode ipv6ip isatap
!
interface TenGigabitEthernet1/1
 description to 6k-sb-2
 dampening
 ip address 10.122.0.93 255.255.255.252
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ip hello-interval eigrp 10 1
 ip hold-time eigrp 10 3
```

```
 ip authentication mode eigrp 10 md5
 ip authentication key-chain eigrp 10 eigrp
 load-interval 30
 carrier-delay msec 0
 ipv6 address 2001:DB8:CAFE:6505::A111:1010/64
 no ipv6 redirects
 ipv6 nd suppress-ra
 ipv6 cef
 ipv6 ospf network point-to-point
 ipv6 ospf hello-interval 1
 ipv6 ospf dead-interval 3
 ipv6 ospf 1 area 0
 mls qos trust dscp
 service-policy output IPv6-ISATAP-MARK
!
interface GigabitEthernet4/1
 description to 6k-core-1
 dampening
 ip address 10.122.0.78 255.255.255.252
 ip access-group 101 in
 no ip redirects
 no ip proxy-arp
 ip hello-interval eigrp 10 1
 ip hold-time eigrp 10 3
 ip authentication mode eigrp 10 md5
 ip authentication key-chain eigrp 10 eigrp
 load-interval 30
 carrier-delay msec 0
 mls qos trust dscp
!
interface GigabitEthernet4/2
 description to 6k-core-2
 dampening
 ip address 10.122.0.86 255.255.255.252
 ip access-group 101 in
 no ip redirects
 no ip proxy-arp
 ip hello-interval eigrp 10 1
 ip hold-time eigrp 10 3
 ip authentication mode eigrp 10 md5
 ip authentication key-chain eigrp 10 eigrp
 load-interval 30
 carrier-delay msec 0
 mls qos trust dscp
!
router eigrp 10
 passive-interface Loopback0
 passive-interface Loopback1
 passive-interface Loopback2
 passive-interface Loopback3
 network 10.0.0.0
 no auto-summary
 eigrp router-id 10.122.10.9
!
ip classless
!
no ip http server
!
ip access-list extended MGMT-IN-v4
 remark Permit v4MGMT only to Lo0
 permit tcp 10.120.0.0 0.0.255.255 any log-input
 permit tcp 10.121.0.0 0.0.255.255 any log-input
 permit tcp 10.122.0.0 0.0.255.255 any log-input
 deny   ip any any log-input
```

```
!
logging source-interface Loopback0
logging 10.121.11.9
access-list 101 permit 41 10.120.2.0 0.0.0.255 host 10.122.10.102
access-list 101 permit 41 10.120.3.0 0.0.0.255 host 10.122.10.103
access-list 101 permit 41 host 10.122.10.1 host 10.122.10.9
access-list 101 permit 41 host 10.122.10.2 host 10.122.10.19
access-list 101 permit 41 host 10.122.10.11 host 10.122.10.10
access-list 101 permit 41 host 10.122.10.12 host 10.122.10.20
access-list 101 deny   41 any any
access-list 101 permit ip any any
ipv6 router ospf 1
 router-id 10.122.10.9
 log-adjacency-changes
 auto-cost reference-bandwidth 10000
 area 2 range 2001:DB8:CAFE:2::/64 cost 10
 area 2 range 2001:DB8:CAFE:3::/64 cost 10
 passive-interface Loopback0
 passive-interface Tunnel2
 passive-interface Tunnel3
 timers spf 1 5
!
snmp-server group IPv6-ADMIN v3 auth write v1default
snmp-server contact John Doe - ipv6rocks@cisco.com
!
ipv6 access-list SOURCE-ISATAP-2
 remark PERMIT ICMPv6 PACKETS FROM HOSTS WITH PREFIX 2001:DB8:CAFE:2::/64
 permit icmp 2001:DB8:CAFE:2::/64 any
 remark PERMIT IPv6 PACKETS FROM HOSTS WITH PREFIX 2001:DB8:CAFE:2::64
 permit ipv6 2001:DB8:CAFE:2::/64 any
 remark PERMIT ALL ICMPv6 PACKETS SOURCED BY HOSTS USING THE LINK-LOCAL PREFIX
 permit icmp FE80::/10 any
 remark DENY ALL OTHER IPv6 PACKETS AND LOG
 deny ipv6 any any log-input
!
ipv6 access-list SOURCE-ISATAP-3
 remark PERMIT ICMPv6 PACKETS FROM HOSTS WITH PREFIX 2001:DB8:CAFE:3::/64
 permit icmp 2001:DB8:CAFE:3::/64 any
 remark PERMIT IPv6 PACKETS FROM HOSTS WITH PREFIX 2001:DB8:CAFE:3::64
 permit ipv6 2001:DB8:CAFE:3::/64 any
 remark PERMIT ALL ICMPv6 PACKETS SOURCED BY HOSTS USING THE LINK-LOCAL PREFIX
 permit icmp FE80::/10 any
 remark DENY ALL OTHER IPv6 PACKETS AND LOG
 deny ipv6 any any log-input
!
ipv6 access-list BULK-APPS
 permit tcp any any eq ftp
 permit tcp any any eq ftp-data
!
ipv6 access-list TRANSACTIONAL-APPS
 permit tcp any any eq telnet
 permit tcp any any eq 22
!
ipv6 access-list MGMT-IN
 remark Permit MGMT only to Loopback0
 permit tcp 2001:DB8:CAFE::/48 host 2001:DB8:CAFE:6507::A111:1010 log-input
 deny ipv6 any any log-input
!
control-plane
!
dial-peer cor custom
!
banner login ^C
Unauthorized access to this device and/or network is prohibited!
```

```
^C
!
line con 0
 session-timeout 3
 password 7 06140E2F4B4B1B
 logging synchronous
 login local
 transport output none
line vty 0 4
 session-timeout 3
 access-class MGMT-IN-v4 in
 password 7 08334D400E1C17
 ipv6 access-class MGMT-IN in
 logging synchronous
 login local
 exec prompt timestamp
 transport input telnet ssh
!
no cns aaa enable
end
```

6k-sb-2

```
upgrade fpd auto
version 12.2
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service password-encryption
service internal
service sequence-numbers
service counters max age 5
!
hostname 6k-sb-2
!
boot system flash sup-bootdisk:s3223-adventerprisek9_wan-mz.122-18.SXF5.bin
logging buffered 64000 debugging
logging rate-limit 5
no logging console
enable secret 5 $1$0UKB$YN.zu/IQt0ivlkqLsdxtY0
!
username cisco privilege 15 secret 5 $1$SUYV$ShOXyooFT..fL/4tyOnAN1
no aaa new-model
clock timezone mst -7
ip subnet-zero
no ip source-route
ip icmp rate-limit unreachable 2000
!
ip ftp source-interface Loopback0
ip ftp username cisco
ip ftp password 7 01100F175804
ip tftp source-interface Loopback0
no ip bootp server
ip telnet source-interface Loopback0
ip ssh time-out 30
ip ssh authentication-retries 2
ip ssh source-interface Loopback0
ip ssh version 2
no ip domain-lookup
ip domain-name cisco.com
```

```
ipv6 unicast-routing
ipv6 mfib hardware-switching replication-mode ingress
udld enable

udld message time 7

vtp domain ese-dc
vtp mode transparent
mls ip cef load-sharing full
mls ip multicast flow-stat-timer 9
no mls flow ip
no mls flow ipv6
mls qos
mls rate-limit unicast ip icmp unreachable acl-drop 0
no mls acl tcam share-global
mls cef error action freeze
!
key chain eigrp
 key 100
  key-string 7 1111
!
!
redundancy
 mode sso
 main-cpu
  auto-sync running-config
!
spanning-tree mode rapid-pvst
spanning-tree loopguard default
no spanning-tree optimize bpdu transmission
spanning-tree extend system-id
environment temperature-controlled
system flowcontrol bus auto
diagnostic cns publish cisco.cns.device.diag_results
diagnostic cns subscribe cisco.cns.device.diag_commands
!
vlan internal allocation policy descending
vlan dot1q tag native
vlan access-log ratelimit 2000
!
class-map match-all CAMPUS-BULK-DATA
  match access-group name BULK-APPS
class-map match-all CAMPUS-TRANSACTIONAL-DATA
  match access-group name TRANSACTIONAL-APPS
!
policy-map IPv6-ISATAP-MARK
  class CAMPUS-BULK-DATA
   set dscp af11
  class CAMPUS-TRANSACTIONAL-DATA
   set dscp af21
  class class-default
   set dscp default
!
interface Loopback0
 description Tunnel source for 6k-agg-1
 ip address 10.122.10.10 255.255.255.255
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ipv6 address 2001:DB8:CAFE:6507::B222:2020/128
 no ipv6 redirects
 ipv6 ospf 1 area 0
!
interface Loopback1
```

```
 description Tunnel source for 6k-agg-2
 ip address 10.122.10.20 255.255.255.255
 no ip redirects
 no ip unreachables
 no ip proxy-arp
!
interface Loopback2
 description Tunnel source for ISATAP-VLAN2
 ip address 10.122.10.102 255.255.255.255
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 delay 1000
!
interface Loopback3
 description Tunnel source for ISATAP-VLAN3
 ip address 10.122.10.103 255.255.255.255
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 delay 1000
!
interface Tunnel0
 description tunnel to 6k-agg-1
 no ip address
 load-interval 30
 ipv6 address 2001:DB8:CAFE:6503::B222:2020/64
 no ipv6 redirects
 ipv6 nd reachable-time 5000
 ipv6 cef
 ipv6 ospf network point-to-point
 ipv6 ospf hello-interval 1
 ipv6 ospf dead-interval 3
 ipv6 ospf 1 area 0
 tunnel source Loopback0
 tunnel destination 10.122.10.11
 tunnel mode ipv6ip
 service-policy output IPv6-ISATAP-MARK
!
interface Tunnel1
 description tunnel to 6k-agg-2
 no ip address
 load-interval 30
 ipv6 address 2001:DB8:CAFE:6504::B222:2020/64
 no ipv6 redirects
 ipv6 nd reachable-time 5000
 ipv6 cef
 ipv6 ospf network point-to-point
 ipv6 ospf hello-interval 1
 ipv6 ospf dead-interval 3
 ipv6 ospf 1 area 0
 tunnel source Loopback1
 tunnel destination 10.122.10.12
 tunnel mode ipv6ip
 service-policy output IPv6-ISATAP-MARK
!
interface Tunnel2
 description ISATAP VLAN2
 no ip address
 ip access-group 100 in
 no ip redirects
 load-interval 30
 ipv6 address 2001:DB8:CAFE:2::/64 eui-64
 ipv6 traffic-filter SOURCE-ISATAP-2 in
```

```
 no ipv6 redirects
 no ipv6 nd suppress-ra
 ipv6 cef
 ipv6 ospf 1 area 2
 tunnel source Loopback2
 tunnel mode ipv6ip isatap
!
interface Tunnel3
 description ISATAP VLAN3
 no ip address
 no ip redirects
 load-interval 30
 ipv6 address 2001:DB8:CAFE:3::/64 eui-64
 ipv6 traffic-filter SOURCE-ISATAP-3 in
 no ipv6 redirects
 no ipv6 nd suppress-ra
 ipv6 cef
 ipv6 ospf 1 area 2
 tunnel source Loopback3
 tunnel mode ipv6ip isatap
!
interface TenGigabitEthernet1/1
 description to 6k-sb-1
 dampening
 ip address 10.122.0.94 255.255.255.252
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ip hello-interval eigrp 10 1
 ip hold-time eigrp 10 3
 ip authentication mode eigrp 10 md5
 ip authentication key-chain eigrp 10 eigrp
 load-interval 30
 carrier-delay msec 0
 ipv6 address 2001:DB8:CAFE:6505::B222:2020/64
 no ipv6 redirects
 ipv6 nd suppress-ra
 ipv6 cef
 ipv6 ospf network point-to-point
 ipv6 ospf hello-interval 1
 ipv6 ospf dead-interval 3
 ipv6 ospf 1 area 0
 mls qos trust dscp
 service-policy output IPv6-ISATAP-MARK
!
interface GigabitEthernet4/1
 description to 6k-core-1
 dampening
 ip address 10.122.0.82 255.255.255.252
 ip access-group 101 in
 no ip redirects
 no ip proxy-arp
 ip hello-interval eigrp 10 1
 ip hold-time eigrp 10 3
 ip authentication mode eigrp 10 md5
 ip authentication key-chain eigrp 10 eigrp
 load-interval 30
 carrier-delay msec 0
 mls qos trust dscp
!
interface GigabitEthernet4/2
 description to 6k-core-2
 dampening
 ip address 10.122.0.90 255.255.255.252
```

```
 ip access-group 101 in
 no ip redirects
 no ip proxy-arp
 ip hello-interval eigrp 10 1
 ip hold-time eigrp 10 3
 ip authentication mode eigrp 10 md5
 ip authentication key-chain eigrp 10 eigrp
 load-interval 30
 carrier-delay msec 0
 mls qos trust dscp
!
router eigrp 10
 passive-interface Loopback0
 passive-interface Loopback1
 passive-interface Loopback2
 passive-interface Loopback3
 network 10.0.0.0
 no auto-summary
 eigrp router-id 10.122.10.10
!
ip classless
!
no ip http server
!
ip access-list extended MGMT-IN-v4
 remark Permit v4MGMT only to Lo0
 permit tcp 10.120.0.0 0.0.255.255 any log-input
 permit tcp 10.121.0.0 0.0.255.255 any log-input
 permit tcp 10.122.0.0 0.0.255.255 any log-input
 deny   ip any any log-input
!
logging source-interface Loopback0
logging 10.121.11.9
access-list 101 permit 41 10.120.2.0 0.0.0.255 host 10.122.10.102
access-list 101 permit 41 10.120.3.0 0.0.0.255 host 10.122.10.103
access-list 101 permit 41 host 10.122.10.1 host 10.122.10.9
access-list 101 permit 41 host 10.122.10.2 host 10.122.10.19
access-list 101 permit 41 host 10.122.10.11 host 10.122.10.10
access-list 101 permit 41 host 10.122.10.12 host 10.122.10.20
access-list 101 deny   41 any any
access-list 101 permit ip any any
ipv6 router ospf 1
 router-id 10.122.10.10
 log-adjacency-changes
 auto-cost reference-bandwidth 10000
 area 2 range 2001:DB8:CAFE:2::/64 cost 20
 area 2 range 2001:DB8:CAFE:3::/64 cost 20
 passive-interface Loopback0
 passive-interface Tunnel2
 passive-interface Tunnel3
 timers spf 1 5
!
snmp-server group IPv6-ADMIN v3 auth write v1default
snmp-server contact John Doe - ipv6rocks@cisco.com
!
ipv6 access-list SOURCE-ISATAP-2
 remark PERMIT ICMPv6 PACKETS FROM HOSTS WITH PREFIX 2001:DB8:CAFE:2::/64
 permit icmp 2001:DB8:CAFE:2::/64 any
 remark PERMIT IPv6 PACKETS FROM HOSTS WITH PREFIX 2001:DB8:CAFE:2::64
 permit ipv6 2001:DB8:CAFE:2::/64 any
 remark PERMIT ALL ICMPv6 PACKETS SOURCED BY HOSTS USING THE LINK-LOCAL PREFIX
 permit icmp FE80::/10 any
 remark DENY ALL OTHER IPv6 PACKETS AND LOG
 deny ipv6 any any log-input
```

```
!
ipv6 access-list SOURCE-ISATAP-3
 remark PERMIT ICMPv6 PACKETS FROM HOSTS WITH PREFIX 2001:DB8:CAFE:3::/64
 permit icmp 2001:DB8:CAFE:3::/64 any
 remark PERMIT IPv6 PACKETS FROM HOSTS WITH PREFIX 2001:DB8:CAFE:3::64
 permit ipv6 2001:DB8:CAFE:3::/64 any
 remark PERMIT ALL ICMPv6 PACKETS SOURCED BY HOSTS USING THE LINK-LOCAL PREFIX
 permit icmp FE80::/10 any
 remark DENY ALL OTHER IPv6 PACKETS AND LOG
 deny ipv6 any any log-input
!
ipv6 access-list BULK-APPS
 permit tcp any any eq ftp
 permit tcp any any eq ftp-data
!
ipv6 access-list TRANSACTIONAL-APPS
 permit tcp any any eq telnet
 permit tcp any any eq 22
!
ipv6 access-list MGMT-IN
 remark Permit MGMT only to Loopback0
 permit tcp 2001:DB8:CAFE::/48 host 2001:DB8:CAFE:6507::B222:2020 log-input
 deny ipv6 any any log-input
!
control-plane
!
dial-peer cor custom
!
banner login ^C

Unauthorized access to this device and network is prohibited.

^C
!
line con 0
 session-timeout 3
 password 7 021405550C031D
 logging synchronous
 login local
 transport output none
line vty 0 4
 session-timeout 3
 access-class MGMT-IN-v4 in
 password 7 071D2042490C0B
 ipv6 access-class MGMT-IN in
 logging synchronous
 login local
 exec prompt timestamp
 transport input telnet ssh
!
no cns aaa enable
end
```