MVPN の設定

この章には、マルチキャスト仮想プライベート ネットワーク（MVPN）の構成方法に関する情報が含まれています。

- MVPN について （1 ページ）
- BGP アドバタイズメント方式 - MVPN サポート （5 ページ）
- MVPN の前提条件 （5 ページ）
- MVPN に関する注意事項と制限事項 （6 ページ）
- MVPN のデフォルト設定 （7 ページ）
- MVPN の設定 （7 ページ）
- MVPN の設定例 （16 ページ）

MVPN について

マルチキャスト仮想プライベート ネットワーク（MVPN）機能を使用すると、レイヤー 3 VPN を介したマルチキャスト接続をサポートできます。IP マルチキャストは、ビデオ、音声、およびデータを VPN ネットワーク コアにストリーミングするために使用します。

従来、ポイントツーポイント トンネルはエンタープライズまたはサービス プロバイダー ネットワークに接続する唯一の方法でした。このようなトンネル ネットワークは、スケーラビリティの問題が発生しますが、IP マルチキャスト トラフィックを仮想プライベート ネットワーク（VPN）に通過させる唯一の方法でした。レイヤ 3 VPN はユニキャスト トラフィック接続のみをサポートするため、レイヤ 3 VPN を展開することによって、オペレーターは、レイヤ 3 VPN のカスタマーにユニキャスト接続とマルチキャスト接続の両方を提供できます。

MVPN を使用すると、MPLS 環境でマルチキャスト トラフィックを設定し、サポートできます。MVPN は、仮想ルーティングおよび転送（VRF）インスタンスごとにマルチキャスト パケットのルーティングと転送をサポートし、また、エンタープライズまたはサービス プロバイダーのバックボーン全体にわたって VPN マルチキャスト パケットを転送するためのメカニズムも提供します。IP マルチキャストは、ビデオ、音声、およびデータを VPN ネットワーク コアにストリーミングするために使用します。

VPNは、インターネットサービスプロバイダー（ISP）のような共有インフラストラクチャにネットワークの接続性を提供します。この機能により、低い所有コストでプライベートネットワークと同じポリシーとパフォーマンスを提供します。

MVPN により、企業はネットワーク バックボーン全体でプライベート ネットワークをトランスペアレントに相互接続することができます。MVPNs を使用して企業ネットワークを相互接続しても、企業ネットワークの管理方法や、企業の全体的な接続性は変更されません。

MPLS MVPN のルーティング、転送、マルチキャスト ドメイン

MVPNsは、VPNルーティングおよび転送テーブルにマルチキャストルーティング情報を導入します。プロバイダーエッジ（PE）ルータがカスタマーエッジ（CE）ルータからマルチキャスト データまたはコントロール パケットを受信する場合は、ルータが VPN ルーティング/転送（MVRF）の情報に基づいてデータまたはコントロール パケットを転送します。

マルチキャスト トラフィックを相互に送信できる MVRF のセットは、マルチキャスト ドメインの構成要素です。たとえば、特定タイプのマルチキャストトラフィックをすべてのグローバルな従業員に送信するカスタマーのマルチキャストドメインは、そのエンタープライズと関連するすべての CE ルータから構成されます。

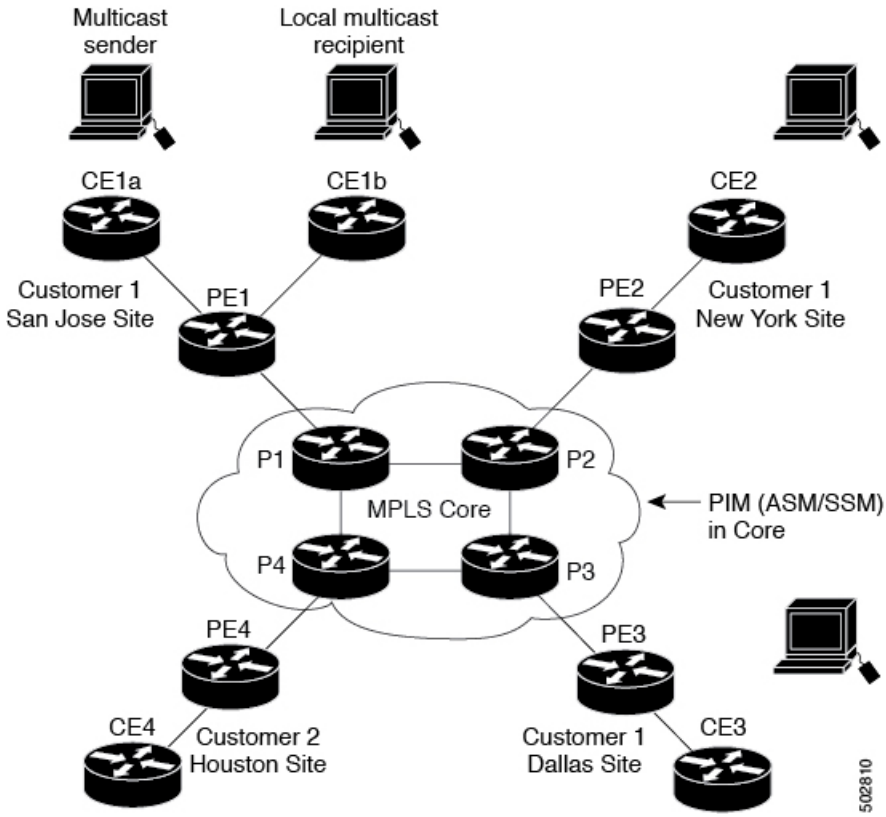
マルチキャスト配信ツリー

MVPN は、各マルチキャスト ドメインにスタティック デフォルト マルチキャスト配信ツリー（MDT）を確立します。デフォルトMDTは、PEルータが使用するパスを定義し、マルチキャスト ドメインにある他のすべての PE ルータに、マルチキャスト データとコントロール メッセージを送信します。

また、MVPN は、高帯域幅伝送用の MDT のダイナミックな作成もサポートします。データMDTは、VPN内のフルモーション ビデオなどの高帯域幅の送信元向けであり、VPNコアの最適なトラフィック転送を確保することを目的としています。

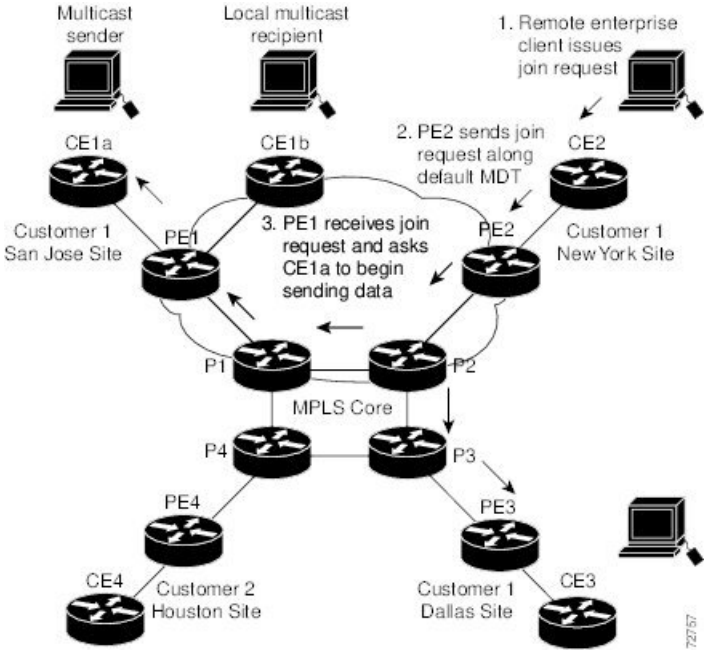
次の例のサービス プロバイダには、San Jose、New York、Dallas にオフィスがあるマルチキャストカスタマーがいます。San Joseでは、一方向のマルチキャストプレゼンテーションが行われています。サービス プロバイダー ネットワークでは、このカスタマーと関連する 3 つすべてのサイト、および別のエンタープライズカスタマーのHoustonサイトがサポートされます。エンタープライズ カスタマーのデフォルト MDT は、プロバイダのルータ P1、P2、P3、およびその関連 PE ルータから構成されています。PE4 は別のカスタマーに関連付けられているため、デフォルト MDT の一部ではありません。次の図からは、San Jose 外では誰もマルチキャストに加入していないため、データがデフォルト MDT に沿って転送されていないことがわかります。

図 *1 :* デフォルト マルチキャスト配信ツリーの概要



New York の従業員がマルチキャスト セッションに加入します。New York のサイトに関連付けられている PE ルータは、カスタマーのマルチキャスト ドメインのデフォルト MDT を介して転送される加入要求を送信します。PE1 は、マルチキャスト セッションの送信元に関連付けられている PE ルータであり、この要求を受信します。次の図は、PE ルータが、マルチキャスト送信元（CE1a）と関連付けられた CE ルータに要求を転送することを示しています。

図 *2:* データ *MDT* の初期化



CE ルータ（CE1a）が関連する PE ルータ（PE1）へマルチキャスト データの送信を開始すると、PE ルータ（PE1）は、デフォルト MDT に沿ってマルチキャスト データを送信します。PE1 はデータ MDT を作成し、データ MDT に関する情報を含むデフォルト MDT を使用して、すべてのルータにメッセージを送信し、3 秒後、データ MDT を使用して、その特定のストリームのマルチキャスト データを送信し始めます。この送信元に関係する受信先は PE2 だけにあるので、PE2 だけがデータ MDT に加入し、データ MDT でトラフィックを受信します。（データ MDT が設定されず、デフォルト MDT のみが設定されている場合、すべてのカスタマー サイトが不要なトラフィックを受信することになります）。PE ルータは、デフォルト MDT を介して他の PE ルータと PIM 関係を維持するとともに、直接接続された P ルータとの PIM 関係をも維持します。

マルチキャスト トンネル インターフェイス

マルチキャスト ドメインごとに作成される VPN ルーティング/転送（MVRF）では、ルータは、すべての MVRF トラフィックが発信されるトンネル インターフェイスを作成する必要があります。マルチキャスト トンネル インターフェイスは、MVRF がマルチキャスト ドメインにアクセスするために使用するインターフェイスです。インターフェイスは、MVRF とグローバル MVRF を接続するコンジットです。MVRF ごとに 1 つのトンネル インターフェイスが作成されます。

MPLS MVPN の利点

MVPNs の利点は、次のとおりです。

- 複数の場所に情報を動的に送信するスケーラブルなメソッドを提供します。

- 高速な情報伝送を提供します。
- 共有インフラストラクチャを介して接続性を提供します。

BGP アドバタイズメント方式 - MVPN サポート

PIM-SM 環境ではなく PIM Source Specific Multicast（PIM-SSM）環境でデフォルト MDT を設定する場合は、受信側 PE は送信元 PE とデフォルト MDT に関する情報を必要とします。この情報は、送信元 PE に（S,G）join を送信し、送信元 PE からの配信ツリーを構築するために使用されます。ランデブーポイント（RP）は必要ありません。送信元のプロバイダーエッジ（PE）アドレスとデフォルト MDT のアドレスは、ボーダー ゲートウェイ プロトコル（BGP）を使用して送信されます。

BGP MDT SAFI

BGP MDT SAFI は、MVPNs に使用される BGP アドバタイズメント メソッドです。現在のリリースでは、IPv4 のみがサポートされています。MDT SAFI の設定は次のとおりです。

- AFI = 1
- SAFI = 66

Cisco NX-OS では、BGP MDT SAFI のアップデートを使用して送信元 PE アドレスと MDT アドレスが PIM に渡されます。ルート記述子（RD）は RD type 0 に変更されており、BGP は PIM に情報を渡す前に、MDT アップデートのための最良パスを決定します。

address-family ipv4 mdt コマンドを使用して、BGP ネイバーの MDT SAFI アドレス ファミリを設定する必要があります。また、ローカル BGP の設定で MDT SAFI をサポートしていないネイバーをイネーブルにする必要があります。MDT SAFI が導入される前、VPNv4 ユニキャスト設定からの追加の BGP 設定は、MVPNs をサポートするために必要ではありませんでした。

MVPN の前提条件

MVPN の設定には、次の前提条件があります。

- ネットワークに MPLS およびラベル配布プロトコル（LDP）を設定する必要があります。PE ルータを含む、コア内のすべてのルータは、MPLS 転送をサポートできる必要があります。PE 送信元アドレスにラベル付きパスが存在しない場合、VPNv4 ルートは BGP によってインストールされません。
- MPLS の正しいライセンスおよび MPLS で使用する他の機能をインストールすることが必要です。

MVPN に関する注意事項と制限事項

MVPN の設定に関する注意事項と制約事項は次のとおりです。

- MVPN は、Cisco NX-OS リリース 9.3(3) 以降でサポートされます。
- MVPN は、-R/-RX ライン カード（N9K-X96136YC-R ライン カードを除く）を搭載した Nexus 9500 プラットフォーム スイッチでサポートされます。
- 双方向フォワーディング検出（BFD）は、マルチキャスト トンネル インターフェイス（MTI）ではサポートされていません。
- デフォルトでは、BGP アップデートのソースは、MVPN トンネルのソースとして使用されます。ただし、mdt source を使用して BGP アップデートのソースを上書きし、マルチキャスト トンネルに異なる送信元を提供することができます。
- MVPN は、最大 16 の MDT 送信元インターフェイスをサポートします。
- MVPN 操作に参加するすべてのルータで MDT SAFI を設定する必要があります。
- コネクタ属性を伝送する VPNv4 内部 BGP（iBGP）セッションには、拡張コミュニティが必要です。
- MDT の MTU 設定はサポートされていません。MVPN 経由で送信できる最大カスタマー マルチキャスト パケット サイズは、コア インターフェイスの MTU によって制限されます。例：
  - MTU 1500 – カスタマー IP パケット サイズ = 1476
  - MTU 9216 – カスタマー IP パケット サイズ = 9192
- 一部の MVPN マルチキャスト制御パケットは、copp-system-p-class-l2-default CoPP ポリシーに分類されます。違反数が増加した場合は、CoPP ポリシーを変更して、このクラスのポリサー レートを増やすことをお勧めします。
- MDT 双方向有効化はサポートされていません。
- vPC は MVPN ではサポートされていません。
- トランジット PE ルータにレシーバがなく、RP である CE に接続されている場合、データ MDT エントリはキャッシュされません。データ MDT エントリは、ローカル レシーバがこの PE ルータに接続されている場合にのみキャッシュされます。ただし、エントリが事前にダウンロードされないため、切り替えに遅延が発生します。
- 日付 MDT の場合、「即時切り替え」モードのみがサポートされます。しきい値ベースのスイッチングはサポートされていません。
- PE デバイスと P /PE デバイス間のサブインターフェイスおよび SVI サポートは利用できません。
- MVPN 整合性チェッカーは、Cisco Nexus リリース 9.3(3) ではサポートされていません。

- MTI インターフェイスの統計は、Cisco Nexus リリース 9.3(3) ではサポートされていません。
- Cisco Nexus リリース 9.3(3) では、ASIC ごとに最大 40G のマルチキャスト トラフィックがサポートされます。
- VRF にデフォルト以外の MTU を設定できるのは、VRF から MDT MTU 設定を削除した場合に限られます。これは、デフォルト以外の MDT MTU を持つ VRF が使用可能なスイッチで MTI がダウンしている場合に発生します。
- ハードウェアの制限により、MTI TX パケット数はサポートされていません。ただし、すべての MTI RX パケットとバイト カウントがサポートされます。

MVPN のデフォルト設定

表 *1*: デフォルトの *MVPN* パラメータ

パラメータ	デフォルト
mdt default *address*	デフォルトなし
mdt enforce-bgp-mdt-safi	有効
mdt source	デフォルトなし
mdt ip pim hello-interval *interval*	30000 ミリ秒
mdt ip pim jp-interval *interval*	60000 ミリ秒
mdt default asm-use-shared-tree	ディセーブル

MVPN の設定

この章では、Cisco NX-OS デバイスでマルチキャスト仮想プライベート ネットワーク（MVPN）を設定する方法について説明します。

（注） MVPN の場合、新しい TCAM 領域「ing-mvpn」が使用されます（デフォルト サイズは 10）。この領域は自動的に分割されるため、分割する必要はありません。この TCAM 領域が分割されているかどうかを確認するには、次のコマンドを使用します。

```
switch# show hardware access-list tcam region | i ing-mvpn
Ingress mVPN [ing-mvpn] size = 10
switch#
```

なんらかの理由で領域が分割されていない場合（サイズが0と示される）、次のコマンドを使用して TCAM 領域をサイズ 10 に分割し、デバイスをリロードできます。TCAM はサイズ 10 に分割されているものと予期されています。

```
switch (config)# hardware access-list tcam region ing-mvpn 10
WARNING: On module 2,
WARNING: On module 4,
Warning: Please reload all linecards for the configuration to take effect
switch (config)#
```

MVPN の有効化

Cisco NX-OS リリース 9.3(3) 以降、Cisco Nexus 9500-R スイッチで MVPN を設定できます。

始める前に

install feature-set mpls コマンドと **feature-set mpls** コマンドを使用して、MPLS 機能セットをインストールして有効にする必要があります。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch#configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します

ステップ 2	**feature bgp** 例： `switch(config)#feature bgp`	BGP 機能と構成を有効にします。
ステップ 3	**feature pim** 例： `switch(config)#feature pim`	PIM 機能をイネーブルにします。
ステップ 4	**feature mvpn** 例： `switch(config)#feature mvpn`	MVPN 機能をイネーブルにします。
ステップ 5	**feature mpls l3vpn** 例： `switch(config)#feature mpls l3vpn`	MPLS レイヤ 3 VPN 機能をイネーブルにします。これにより、サイト間のユニキャスト ルートが決定されます。
ステップ 6	**feature mpls ldp** 例： `switch(config)#feature mpls ldp`	MPLS ラベル配布プロトコル（LDP）をイネーブルにします。

インターフェイスでの PIM のイネーブル化

IP マルチキャストに使用されるすべてのインターフェイスのプロトコル独立マルチキャスト（PIM）を設定することができます。バックボーンに接続されるプロバイダー エッジ（PE）ルータのすべての物理インターフェイスで PIM スパース モードに設定することをお勧めします。また、すべてのループバック インターフェイスについて、それが BGP ピアリングに使用される場合や、その IP アドレスが PIM の RP アドレスとして使用される場合は、PIM スパース モードに設定することをお勧めします。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch#configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します

ステップ 2	**ip pim sparse-mode** 例： `switch(config)#ip pim sparse-mode`	インターフェイスで PIM スパース モードをイネーブルにします。

VRF のデフォルト MDT の設定

VRF のデフォルト MDT を設定できます。

始める前に

デフォルト MDT は、同じ VPN に属するすべてのルータの設定と同じであることが必要です。送信元 IP アドレスは、BGP セッションの送信元を特定するために使用するアドレスです。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch#configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します

ステップ 2	**vrf context** *VRF_NAME* 例： `switch(config)#vrf context vrf1`	VRF を設定します。

	コマンドまたはアクション	目的
ステップ 3	**mdt default** *address* 例： `switch(config)#mdt default 232.0.0.1`	VRF に、データ MDTs のマルチキャスト アドレスの範囲を次のように設定します。 • このコマンドによって、トンネル インターフェイスが作成されます。 • デフォルトでは、トンネルヘッダーの宛先アドレスは address 引数です。

VRF の MDT SAFI の設定

デフォルトでは、VRF の MDT 後続アドレス ファミリ識別子（SAFI）が適用されます。必要に応じて、MDT SAFI をサポートしていないピアと相互運用するように MDT を構成できます。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch#configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します

ステップ 2	**vrf context** *VRF_NAME*
	例：
	`switch(config)#vrf context vrf1`
	`switch(config-vrf)#`
		VRF を設定します。

ステップ 3	**no mdt enforce-bgp-mdt-safi** 例： `switch(config-vrf)#no mdt enforce-bgp-mdt-safi`	MDT SAFI をサポートしていないピアとの相互運用を可能にします。Any Source Multicast（ASM）の範囲内であるときは、初期状態ではデフォルト MDT グループの（*,G）エントリのみが読み込まれます。その後、トラフィックに基づき、（S,G）エントリは、通常の ASM ルートと同じように学習されます。 コマンドから **no** オプションを削除すると、指定された VRF に対して MDT SAFI の使用が強制されます。

MVPN のための BGP における MDT アドレス ファミリの設定

PE ルータに MDT アドレス ファミリ セッションを設定し、MVPN の MDT ピアリング セッションを確立することができます。

MDT アドレス ファミリ セッションを設定するには、ネイバー モードで **address-family ipv4 mdt** コマンドを使用してください。MDT アドレス ファミリ セッションは、BGP MDT Subaddress Family Identifier（SAFI）のアップデートを使用して PIM に送信元 PE アドレスと MDT アドレスを渡すために使用されます。

始める前に

MVPN ピアリングが MDT アドレス ファミリを介して確立できるようにするには、CE ルータに VPN サービスを提供する PE ルータで BGP ネットワークの MPLS とマルチプロトコル BGP を設定する必要があります。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch#configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**feature bgp** *as-number* 例： `switch(config)#feature bgp 65635`	スイッチ コンフィギュレーション モードを開始して、BGP ルーティング プロセスを作成します。

ステップ 3	**vrf context** *VRF_NAME*
	例：
	`switch(config)#vrf context vpn1`
	`switch(config-vrf)#`
		vrf-name で識別される VPN ルーティング インスタンスを定義し、VRF コンフィギュレーション モードを開始します。vrf-name 引数には最大 32 文字の英数字文字列を指定します。大文字と小文字は区別されます。

ステップ 4	**rd** *route-distinguisher* 例： `switch(config-vrf)#rd 1.2.1`	VRF の vrf-name にルート識別子を割り当てます。route-distinguisher 引数によって、8 バイトの値が IPv4 プレフィックスに追加され、VPN IPv4 プレフィックスが作成されます。RD は、次のいずれかの形式で入力できます。 • 16 ビットまたは 32 ビットの AS 番号:32 ビットの番号。1.2:3 など。 • 32 ビットの IP アドレス:16 ビットの番号。192.0.2.1:1 など。

	コマンドまたはアクション	目的

ステップ 5	**address-family ipv4 unicast**
	例：
	`switch(config-vrf)#address-family ipv4unicast`
	`switch(config-vrf-af)#`
		IPv4 アドレス ファミリ タイプを指定し、アドレス ファミリ コンフィギュレーション モードを開始します。

ステップ 6	**route-target import** *route-target-ext-community* 例： `switch(config-vrf-af)# route-target import 1.0.1`	VRF 用にルート ターゲット拡張コミュニティを指定します。**import** キーワードを使用すると、ルーティング情報がターゲット VPN 拡張コミュニティからインポートされます。 *route-target-ext-community* 引数により、ルート ターゲット拡張コミュニティ属性が、インポート ルート ターゲット拡張コミュニティの VRF リストに追加されます。*route-target-ext-community* 引数は、次のいずれかの形式で入力できます。 • 16 ビットまたは 32 ビットの AS 番号:32 ビットの番号。1.2:3 など。 • 32 ビットの IP アドレス：16 ビットの番号。192.0.2.1:1 など。
ステップ 7	**route-target export** *route-target-ext-community* 例： `switch(config-vrf-af)# route-target export 1.0.1`	VRF 用にルート ターゲット拡張コミュニティを指定します。**export** キーワードを使用すると、ルーティング情報がターゲット VPN 拡張コミュニティからインポートされます。 *route-target-ext-community* 引数により、ルート ターゲット拡張コミュニティ属性が、インポート ルート ターゲット拡張コミュニティの VRF リストに追加されます。*route-target-ext-community* 引数は、次のいずれかの形式で入力できます。 • 16 ビットまたは 32 ビットの AS 番号:32 ビットの番号。1.2:3 など。 • 32 ビットの IP アドレス：16 ビットの番号。192.0.2.1:1 など。

	コマンドまたはアクション	目的

ステップ 8	**router bgp** *as-number*
	例：
	`switch(config)#router bgp 1.1`
	`switch(config-router)#`
		BGP ルーティング プロセスを設定し、ルータ コンフィギュレーション モードを開始します。as-number 引数は、ルータを他の BGP ルータに対して識別し、転送するルーティング情報にタグを設定する自律システムの番号を示します。AS 番号は 16 ビット整数または 32 ビット整数にできます。上位 16 ビット 10 進数と下位 16 ビット 10 進数による xx.xx という形式です。

ステップ 9	**address-family ipv4 mdt** 例： `switch(config-router)#address-family ipv4 mdt`	IPv4 MDT アドレス ファミリ コンフィギュレーション モードを開始します。

ステップ 10	**address-family** {**vpn4**} [**unicast**]
	例：
	`switch(config-router-af)# address-family vpnv4`
	`switch(config-router-af)#`
		アドレス ファミリ コンフィギュレーション モードを開始して、標準 VPNv4 または VPNv6 アドレス プレフィックスを使用する、BGP などのルーティング セッションを設定します。**unicast** キーワード（任意）では、VPNv4 または VPNv6 ユニキャスト アドレス プレフィックスを指定します。

ステップ 11	**address-family** {**ipv4**} **unicast**
	例：
	`switch(config-router-af)# address-family ipv4 unicast`
	`switch(config-router-af)#`
		標準 IPv4 または VPNv6 アドレス プレフィックスを使用するルーティング セッションを設定するために、アドレス ファミリ コンフィギュレーション モードを開始します。

ステップ 12	**neighbor** *neighbor-address* 例： `switch(config-switch-af)# neighbor 192.168.1.1`	ネイバー コンフィギュレーション モードを開始します。
ステップ 13	**update source** *interface* 例： `switch(config-switch-neighbor)# update-source loopback 1`	アップデート ソースを loopback1 に設定します。
ステップ 14	**address-family ipv4 mdt** 例： `switch(config-router-neighbor)# address-family ipv4 mdt`	アドレス ファミリ コンフィギュレーションを開始し、IP MDT アドレス ファミリ セッションを作成します。

	コマンドまたはアクション	目的
ステップ 15	**send-community extended** 例： `switch(config-router-neighbor-af)#send-community extended`	拡張コミュニティ属性が BGP ネイバーに送信されるように指定します。
ステップ 16	**show bgp** {**ipv4**} **unicast neighbors vrf***VRF_NAME* 例： `switch(config-router-neighbor-af)#show bgp ipv4 unicast neighbors vrf vpn1`	BGP ネイバーに関する情報を表示します。vrf-name 引数には最大 32 文字の英数字文字列を指定します。大文字と小文字は区別されます。
ステップ 17	**copy running-config startup-config** 例： `switch(config-router-neighbor-af)#copy running-config startup-config`	実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

データ MDT の設定

データ MDT を設定できます。データ MDT の作成に使用されるマルチキャスト グループは、設定済み IP アドレスのプールからダイナミックに選択されます。ストリームの数が PE 単位、VRF 単位の MDT より大きい場合、複数のストリームが同じデータ MDT を共有します。

始める前に

データ MDT を設定する前に、VRF のデフォルト MDT を設定する必要があります。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch#configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します

ステップ 2	**vrf context** *VRF_NAME* 例： `switch#ip vrf vrf1`	VRF コンフィギュレーション モードを開始し、VRF 名を割り当てることにより VPN ルーティング インスタンスを定義します。
ステップ 3	**mdt data** *prefix* [**immediate-switch**] [**route-map** *policy-name*] 例：	次のように値の範囲を指定します。 • *prefix* は、データ MDT プールで使用されるアドレスの範囲を指定します。

	コマンドまたはアクション	目的

	`switch(config-vrf)# mdt data 225.1.1.1/32 immediate-switch route-map test`
	例：
	`switch(config-vrf)# mdt data 225.1.1.1/32 route-map test`
		• *policy-name* は、データ MDT への切り替えで考慮されるカスタマーデータ ストリームを定義するポリシー ファイルを定義します。
		（注） このコマンドは、immediate-switch オプションの有無にかかわらず同じ効果があります。

ステップ 4	**exit** 例： `switch(config)#exit`	グローバル コンフィギュレーション モードに戻ります。

MVPN の設定の確認

MVPN の設定を表示するには、次のいずれかの作業を行います。

表 *2 : MVPN* の設定の確認

コマンド	目的
show interface	インターフェイスの詳細を表示します。
show ip mroute vrf	マルチキャスト ルートを表示します。
show ip pim event-history mvpn	MVPN のイベント履歴ログの詳細を表示します。
show ip pim mdt	MVPN によって作成された MTI トンネルの詳細を表示します。
show ip pim mdt receive vrf vrf-name	カスタマー ソース、データ MDT 送信元へのカスタマー グループ、および受信側のデータ MDT グループそれぞれのマッピングを表示します。
show ip pim mdt send vrf vrf-name	カスタマー ソース、データ MDT 送信元へのカスタマー グループ、および送信側のデータ MDT グループそれぞれのマッピングを表示します。
show ip pim neighbor	確立された PIM ネイバーの詳細を表示します。

コマンド	目的
show ip route detail	ユニキャストルーティングテーブルの詳細を表示します。
show mvpn bgp mdt-safi	MVPN の BGP MDT SAFI データベースを表示します。
show mvpn mdt encap vrf *vrf*	MVPN のカプセル化テーブルを表示します。このテーブルは、デフォルト vrf で MVPN パケットを送信するときにカプセル化する方法を示しています。
show mvpn mdt route	デフォルトおよびMDTルートの詳細を表示します。このデータは、デフォルト VRF でカスタマー データと制御トラフィックを送信する方法を決定します。
show routing [**ip**] **multicast mdt encap**	MRIB のカプセル化テーブルを表示します。このテーブルは、デフォルト vrf で MVPN パケットを送信するときにカプセル化する方法を示しています。

MVPN の設定例

次に、MVPN の設定例を 2 つのコンテキストで示します。

```
vrf context vpn1
  ip pim rp-address 10.10.1.2 -list 224.0.0.0/8
  ip pim ssm range 232.0.0.0/8
  rd auto
  mdt default 232.1.1.1
  mdt source loopback1
  mdt data 225.122.111.0/24 immediate-switch
vrf context vpn4
  ip pim rp-address 10.10.4.2 -list 224.0.0.0/8
  ip pim ssm range 232.0.0.0/8
  mdt default 235.1.1.1
  mdt asm-use-shared-tree
ip pim rp-address 10.11.0.2 -list 224.0.0.0/8
ip pim rp-address 10.11.0.4 -list 235.0.0.0/8
ip pim ssm range 232.0.0.0/8
```

次に、「blue」と名づけられた VRF を VPN ルーティング インスタンスに割り当てる方法の例を示します。VPN VRF の MDT デフォルトは 10.1.1.1、MDT のマルチキャスト アドレスの範囲は 10.1.2.0（ワイルドカード ビットが 0.0.0.3）です。

```
Vrf context blue
mdt data 225.122.111.0/24 immediate-switch
```

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