



## Cisco NCS 560 シリーズ ルータ (Cisco IOS XR リリース 6.6.x) マルチキャスト コンフィギュレーション ガイド

|   |    |
|---|----|
| レイヤ3 マルチキャスト ルーティングの実装                  | 3  |
| マルチキャストの有効化                             | 3  |
| Protocol Independent Multicast          | 4  |
| PIM BFD の概要                             | 4  |
| Reverse Path Forwarding                 | 6  |
| IETF 標準を使用した RPF ベクトル エンコーディング          | 7  |
| PIM-Source Specific Multicast (PIM-SSM) | 7  |
| Multicast Source Discovery Protocol     | 12 |
| PIM スパース モード                            | 18 |
| PIM ブートストラップ ルータ                        | 19 |
| 指定ルータ                                   | 21 |
| インターネット グループ管理プロトコル (IGMP)              | 23 |
| 複数の送信元での IPv6 マルチキャスト                   | 26 |
| 使用例：ビデオ ストリーミング                         | 27 |
| コアでのマルチキャスト ラベル配布プロトコル (MLDP)           | 28 |
| コアでの MLDP の設定例                          | 28 |

|   |    |
|---|----|
| ラベルスイッチドマルチキャスト (LSM) マルチキャストラベル配布プロトコル (mLDP) ベース<br>のマルチキャスト VPN (mVPN) のサポート | 28 |
| エッジルータでの VRF mLDP インバンドシグナリングの設定  | 31 |
| エッジルータでの グローバル mLDP インバンドシグナリングの設定  | 32 |
| MVPN プロファイルの設定例   | 32 |
| エッジルータでのインバンド mLDP プロファイルの設定例   | 35 |
| エッジルータでの mLDP 設定の確認   | 36 |

## レイヤ3 マルチキャスト ルーティングの実装

マルチキャストルーティングはホストが、ユニキャスト送信のように単一のホストではなく、すべてのホストのサブセットに対してグループ送信として、またはブロードキャスト伝送のようにすべてのホストにパケットを送信できます。ホストのサブセットはグループメンバと呼ばれ、224.0.0.0～239.255.255.255のIPクラスDアドレス範囲に含まれる1つのマルチキャストグループアドレスによって識別されます。

マルチキャスト環境は、送信側と受信側で構成されます。どのホストも、グループのメンバであるかどうかにかかわらず、グループに送信できます。ただし、グループのメンバだけがメッセージを受信します。

Cisco NCS 560 シリーズ ルータは、マルチキャストルーティングを実装するために以下のプロトコルをサポートしています。

- IGMP：IGMPは、ホストがメンバになっているマルチキャストグループを追跡するためにネットワーク（LANなど）上のホストとそのネットワーク上のルータの間で使用されます。
- PIM SSM：Source-Specific MulticastのProtocol Independent Multicast（PIM-SSM）は、IPマルチキャストアドレスを宛先とした特定の送信元アドレス（または特定の送信元アドレスを除くすべてのアドレス）からのパケットを受信する対象をレポートする機能を備えています。



---

（注）MLD スヌーピングは、Cisco IOS XR リリース 6.5.3 までサポートされていません。将来のリリースでサポートされるようになります。

---

### Cisco NCS 560 シリーズ ルータでマルチキャストルーティングを実装するための前提条件

- マルチキャスト RPM パッケージをインストールしてアクティブにする必要があります。
- IPv4 マルチキャストルーティングの設定作業と概要に関する知識が必要です。
- ユニキャストルーティングは動作可能でなければなりません。

## マルチキャストの有効化

### 設定例

新規および既存のすべてのインターフェイスでマルチキャストルーティングおよび転送をイネーブルにします。

```
Router#config
Router(config)#multicast-routing
Router(config-mcast)#address-family ipv4
Router(config-mcast-default-ipv4)#interface all enable
*/In the above command, you can also indicate a specific interface (For example, interface TenGigE0/11/0/0)
for enabling multicast only on that interface/*
Router(config-mcast-default-ipv4)#commit
```

## 実行コンフィギュレーション

```
Router#show running multicast routing
multicast-routing
  address-family ipv4
    interface all enable
  !
```

## 確認

インターフェイスでマルチキャストが有効になっていることを確認します。

```
Router#show mfib interface location 0/RP0/cpu0
Interface : FINT0/RP0/cpu0 (Enabled)
SW Mcast pkts in : 0, SW Mcast pkts out : 0
TTL Threshold : 0
Ref Count : 2
Interface : TenGigE0/11/0/0 (Enabled)
SW Mcast pkts in : 0, SW Mcast pkts out : 0
TTL Threshold : 0
Ref Count : 3
Interface : TenGigE0/11/0/1 (Enabled)
SW Mcast pkts in : 0, SW Mcast pkts out : 0
TTL Threshold : 0
Ref Count : 13
Interface : Bundle-Ether1 (Enabled)
SW Mcast pkts in : 0, SW Mcast pkts out : 0
TTL Threshold : 0
Ref Count : 4
Interface : Bundle-Ether1.1 (Enabled)
SW Mcast pkts in : 0, SW Mcast pkts out : 0
TTL Threshold : 0
```

# Protocol Independent Multicast

Protocol Independent Multicast (PIM) は、マルチキャストデータパケットの転送に使用されるマルチキャスト配信ツリーを作成するために使用されるマルチキャストルーティングプロトコルです。

マルチキャストが適切に動作するためには、送信元またはRPへのユニキャストパスを認識する必要があります。PIMは、ユニキャストルーティングプロトコルを使用してこのリバースパス転送 (RPF) 情報を取得します。PIMという名前が示すとおり、使用されるユニキャストプロトコルとは独立して動作します。PIMはRPF情報についてルーティング情報ベース (RIB) に依存します。Protocol Independent Multicast (PIM) は、マルチキャストルーティングアップデートを送受信するように設計されています。

バンドルイーサネットサブインターフェイスでのPIMがサポートされています。

## PIM BFD の概要

PIM BFDとも呼ばれるマルチキャストのBFDサポート (PIM) 機能では、BFDのクライアントとしてPIMが登録されます。すると、PIMはBFDの高速な隣接障害検出を使用できるようになります。PIM BFDが有効の場合、BFDはPIMからのhelloメッセージを待機せずに、より速い障害検出を行えます。

BFDクライアントとしてのPIM要求時、BFDは、隣接ノードとのセッションを確立および維持することで、生存性を維持し、隣接ノードへの転送パス障害を検出します。BFDがネイバーとのBFDセッションを確立して維持した後も、

PIM hello はネイバー間で引き続き交換されます。この機能の導入により、PIM hello メカニズムの動作は変更されません。PIM は内部ゲートウェイ プロトコル (IGP) に依存し、BFD は IGP でサポートされますが、PIM BFD は IGP の BFD とは独立しています。

Protocol Independent Multicast (PIM) は、hello メカニズムを使用して、隣接ノード間の新しい PIM ネイバーを検出します。PIM の最小障害検出時間は、PIM Query-Interval の 3 倍です。より高速な障害検出を可能にするために、インターフェイス上で PIM hello メッセージが送信される速度を設定できます。ただし、間隔が短くなると、プロトコルの負荷が増加し、CPU とメモリの使用率が増加して、システム全体のパフォーマンスに悪影響を与える可能性があります。また、間隔を短くすると、ネイバーから受信した hello メッセージが処理される前にネイバーの有効期限が切れる可能性があるため、PIM ネイバーが頻繁に期限切れになる可能性があります。PIM BFD が有効の場合、BFD は PIM からの hello メッセージを待機せずに、より速い障害検出を行えます。

## PIM BFD の設定



---

(注) IPv6 での PIM BFD はサポートされていません。

---

ここでは、PIM BFD の設定方法について説明します。

```
Router# configure
Router(config)# router pim address-family ipv4
Router(config-pim-default-ipv4)# interface HundredGige0/9/0/0
Router(config-pim-ipv4-if)# bfd minimum-interval 10
Router(config-pim-ipv4-if)# bfd fast-detect
Router(config-pim-ipv4-if)# bfd multiplier 3
Router(config-pim-ipv4)# exit
Router(config-pim-default-ipv4)# interface TengigabitEthernet0/11/0/0
Router(config-pim-ipv4-if)# bfd minimum-interval 50
Router(config-pim-ipv4-if)# bfd fast-detect
Router(config-pim-ipv4-if)# bfd multiplier 3
Router(config-pim-ipv4-if)# exit
```

### 実行コンフィギュレーション

```
router pim
 address-family ipv4
  interface HundredGige 0/9/0/0
   bfd minimum-interval 10
   bfd fast-detect
   bfd multiplier 3
  !
 interface TengigabitEthernet 0/11/0/0
  bfd minimum-interval 50
  bfd fast-detect
  bfd multiplier 3
 !
 !
 !
 !
```

!

## 確認

次の項に示す show 出力には、PIM BFD の設定の詳細とその設定のステータスが表示されます。

```
Router# show bfd session
Wed Nov 22 08:27:35.952 PST
Interface          Dest Addr      Local det time(int*mult)  State   Echo      Async  H/W      NPU
-----
Hu0/9/0/0         10.12.12.2    0s (0s*0)  90ms (30ms*3)   UP
Te0/11/0/0        10.112.112.2  0s (0s*0)  90ms (30ms*3)   UP
```

```
Router# show bfd client
Name              Node           Num sessions
-----
L2VPN_ATOM       0/RP0/CPU0 0
MPLS-TR          0/RP0/CPU0 0
bgp-default      0/RP0/CPU0 0
bundlemgr_distrib 0/RP0/CPU0 14
isis-1           0/RP0/CPU0 0
object_tracking  0/RP0/CPU0 0
pim6             0/RP0/CPU0 0
pim            0/RP0/CPU0 0
service-layer    0/RP0/CPU0 0
```

## Reverse Path Forwarding

リバースパス転送 (RPF) は、マルチキャストデータグラムの転送に使用されるアルゴリズムです。これは、次のように機能します。

- ルータで送信元へのユニキャストパケットの送信に使用しているインターフェイスでデータグラムを受信すると、パケットは RPF インターフェイスに着信しています。
- パケットが RPF インターフェイスに着信した場合、ルータは、マルチキャストルーティングテーブルエントリの発信インターフェイスリストに存在するインターフェイスにパケットを転送します。
- パケットが RPF インターフェイスに着信しない場合、パケットはループを回避するためにサイレントにドロップされています。

PIM では、送信元ツリーと RP をルートとする共有ツリーの両方を使用してデータグラムを転送します。RPF チェックは、次のようにそれぞれ異なる方法で実行されます。

- PIM ルータのマルチキャストルーティングテーブル内に (S,G) エントリがある場合 (送信元ツリー ステートである場合)、マルチキャストパケットの送信元の IP アドレスに対して RPF チェックが実行されます。
- PIM ルータに明示的な送信元ツリー ステートがない場合、共有ツリー ステートと見なされます。ルータは、メンバがグループに加入したときにわかる RP のアドレスに対して RPF チェックを実行します。

空間モード PIM では、RPF ルックアップ機能を使用して、join および prune の送信先を決定します。(S,G) Join メッセージ (送信元ツリー ステート) は送信元に向け送信されます。(\*,G) Join メッセージ (共有ツリー ステート) は RP に向け送信されます。

## IETF 標準を使用した RPF ベクトル エンコーディング

RPF ベクトルは、RPF 情報のないコア ルータが外部送信元のために join/prune メッセージを転送できるようにする PIM プロキシです (たとえば、MPLS ベース、BGP フリーのコアで、MPLS コア ルータが BGP から学習された外部ルートを持たない場合など)。RPF ベクトル エンコーディングは、現在、新しい IETF エンコーディングと互換性があります。新しい IETF 標準では、PIM Hello オプション 26 を使用して PIM メッセージがエンコードされます。

### RPF ベクトルの設定 (IETF 標準エンコーディング)

次の例では、IETF 標準を使用して RPF エンコーディングを有効にする方法を示します。

```
(config)# router pim
(config-pim-default-ipv4)# address-family ipv4
(config-pim-default-ipv4)# rpf-vector use-standard-encoding
!
(config)# multicast-routing
(config-mcast)# interface TenGigE 0/11/0/0
(config-mcast)# interface TenGigE 0/11/0/1
```

### 確認

```
Router#show pim neighbor
Tue Apr 17 10:15:40.961 PDT
```

```
PIM neighbors in VRF default
Flag: B - Bidir capable, P - Proxy capable, DR - Designated Router,
      E - ECMP Redirect capable
      * indicates the neighbor created for this router
```

| Neighbor Address   | Interface               | Uptime      | Expires         | DR pri        | Flags        |
|--------------------|-------------------------|-------------|-----------------|---------------|--------------|
| 25.25.25.1         | TenGigE 0/11/0/0        | 1w3d        | 00:01:36        | 1             | B P          |
| <b>25.25.25.2*</b> | <b>TenGigE 0/11/0/0</b> | <b>1w3d</b> | <b>00:01:41</b> | <b>1 (DR)</b> | <b>B P E</b> |
| 32.32.32.2*        | TenGigE 0/11/0/1        | 1w4d        | 00:01:40        | 1             | B P E        |
| <b>32.32.32.3</b>  | <b>TenGigE 0/11/0/1</b> | <b>1w4d</b> | <b>00:01:42</b> | <b>1 (DR)</b> | <b>B P</b>   |

上記の出力では、マルチキャストが有効になっているインターフェイスに対し「P」タグが表示されています。

## PIM-Source Specific Multicast (PIM-SSM)

SSM モードで PIM を使用すると、マルチキャストルーティングの管理が簡単になります。これは、RP (ランデブーポイント) が不要なため、共有ツリー (\*,G) が構築されないためです。

PIM-SSM を定義する特定の IETF ドキュメントはありません。ただし、RFC4607 では、SSM の全体的な動作が定義されています。

このドキュメントでは、SSM を使用する場合の PIM の動作と設定について PIM-SSM という用語を使用して説明します。

Source-Specific Multicast 動作の PIM は、受信側から提供されたマルチキャスト グループの送信元アドレスから得た情報を使用して、トラフィックの送信元フィルタリングを実行します。

- デフォルトでは、PIM-SSM は、IPv4 の場合は 232.0.0.0/8 のマルチキャスト グループ範囲で動作し、IPv6 の場合は FF3x::/32 で動作します。これらの値を設定するには、**ssm range** コマンドを使用します。
- PIM-SM 用に設定されているネットワークに SSM を配置する場合、ラストホップルータのみを SSM 機能をサポートする Cisco IOS XR ソフトウェアでアップグレードする必要があります。
- SSM 範囲内の MSDP SA メッセージは、受け入れ、生成、転送のいずれも実行されません。
- SSM は **ssm disable** コマンドを使用して無効にできます。
- **ssm allow-override** コマンドを使用すると、SSM 範囲をより特定の範囲で上書きすることができます。

送信元がわかっている多くのマルチキャスト構成では、プロトコル独立型マルチキャスト送信元特定マルチキャスト (PIM-SSM) マッピングは、その単純さから、使用すべき明白なマルチキャストルーティングプロトコルの選択です。PIM-SSM のメリットを享受できる一般的なマルチキャスト構成としては、ETTH スペースなどのエンターテインメント型のソリューションや、静的な転送に完全に依存する金融機関での展開が挙げられます。

SSM では、データ グラムは (S,G) チャネルに基づいて配信されます。1 つの (S,G) チャネルのトラフィックは、IP 宛先アドレスとして IP ユニキャスト送信元アドレス S とマルチキャスト グループ アドレス G を持つデータグラムで構成されています。システムは、(S,G) チャネルのメンバになることによって、トラフィックを受信します。シグナリングは不要ですが、受信先は特定の送信元からのトラフィックを受信する場合は (S,G) チャネルに加入し、トラフィックを受信しない場合はチャネルから脱退する必要があります。チャネル加入シグナリングでは、IGMP を使用してモードメンバーシップ レポートを含めます。これは、IGMP バージョン 3 (IGMPv3) でのみサポートされています。

IGMPv3 で SSM を使用するには、マルチキャストルータ、アプリケーションが稼働しているホスト、そしてアプリケーション自体が SSM をサポートしている必要があります。Cisco IOS XR ソフトウェアでは、224.0.0.0 ~ 239.255.255.255 の IP マルチキャスト アドレス範囲の任意のサブセットの SSM 設定を許可します。

SSM 範囲が定義されると、(アプリケーションが明示的な (S,G) チャネル加入を使用するように変更されていない限り) SSM 範囲内でアドレスを使用しようとする場合に既存の IP マルチキャスト レシーバアプリケーションはトラフィックを受信しません。

## PIM-SM 経由の PIM-SSM の利点

PIM-SSM は PIM-SM から派生したものです。ただし、PIM-SM では、PIM join メッセージに応じて特定のグループに送信するすべての送信元のデータ伝送が可能なのに対し、SSM 機能は、受信先が明示的に加入した送信元からのトラフィックのみをレシーバへ転送します。PIM join および prune はトラフィックの送信元に直接送信されるため、RP と共有ツリーは不要で拒否されます。SSM が、帯域利用率を最適化し、不要なインターネットブロードキャストトラフィックを拒否するために使用されます。送信元は、IGMPv3 メンバーシップレポートを使用して対象の受信先により提供されます。

## IGMPv2

IGMPv2 をサポートするには、特定の送信元をグループの範囲に一致させるように IGMP を設定するとき、SSM マッピング設定を追加する必要があります。



## 設定例

アクセスリスト (mcl) を設定します。

```
Router#configure
Router(config)#ipv4 access-list mcl
Router(config-ipv4-acl)#permit ipv4 any 232.1.1.0 0.0.0.255
Router(config-ipv4-acl)#commit
```

指定したアクセスリスト (mcl) によって記述された SSM グループをマッピングする複数の送信元の一部としてマルチキャスト送信元 (1.1.1.1) を設定します。

```
Router#configure
Router(config)#router igmp
Router(config-igmp)#ssm map static 1.1.1.1 mcl
Router(config-igmp)#commit
```

## 実行コンフィギュレーション

```
Router#show run router igmp
router igmp
ssm map static 1.1.1.1 mcl
```

## 確認

## マルチパス オプション

マルチパス オプションは、router pim コンフィギュレーションモードで使用できます。マルチパス オプションを有効にすると、SSMは共通パスを選択するのではなく、同じ宛先に到達する異なるパスを選択します。マルチパスオプションは、SSM トラフィックのロード バランスに役立ちます。

## マルチパス オプションの設定

```
Router#configure
Router(config)#router pim address-family ipv4
Router(config-pim-default-ipv4)#multipath hash source
Router(config-pim-default-ipv4)#commit
```

## 実行コンフィギュレーション

```
Router#show running router pim
router pim
address-family ipv4
dr-priority 100
multipath hash source /*SSM traffic takes different path to reach same destination based on source hash value.*/
```

## 確認

Bundle-Ether132 と TenGigE0/11/0/1.132 は、宛先ルータ Turnin-56 に到達するための2つのパスです。マルチパス オプションを有効にしたので、送信元には 50.11.30.12 と 50.11.30.11 の2つの IP アドレスがあります。2つの送信元からのマルチキャストトラフィックは、同じ宛先に到達するために2つの異なるパス Bundle-Ether132 および TenGigE0/11/0/1.132 を使用します。

次の show run 出力は、Bundle-Ether132 と TenGigE0/11/0/1.132 が同じ宛先ルータ Turnin-56 に接続されていることを示しています。

```
Router#show run int TenGigE0/11/0/2.132
interface TenGigE0/1/11/2/3.132
  description Connected to Turin-56 ten0/11/0/1.132
  ipv4 address 13.0.2.1 255.255.255.240
  ipv6 address 2606::13:0:2:1/120
  encapsulation dot1q 132
!
```

```
Router#show run int bel32
interface Bundle-Ether132
  description Bundle between Fretta-56 and Turin-56
  ipv4 address 28.0.0.1 255.255.255.240
  ipv6 address 2606::28:0:0:1/120
  load-interval 30
```

```
Router#show mrib route 50.11.30.11 detail
```

```
IP Multicast Routing Information Base
Entry flags: L - Domain-Local Source, E - External Source to the Domain,
  C - Directly-Connected Check, S - Signal, IA - Inherit Accept,
  IF - Inherit From, D - Drop, ME - MDT Encap, EID - Encap ID,
  MD - MDT Decap, MT - MDT Threshold Crossed, MH - MDT interface handle
  CD - Conditional Decap, MPLS - MPLS Decap, EX - Extranet
  MoFE - MoFRR Enabled, MoFS - MoFRR State, MoFP - MoFRR Primary
  MoFB - MoFRR Backup, RPFID - RPF ID Set, X - VXLAN
Interface flags: F - Forward, A - Accept, IC - Internal Copy,
  NS - Negate Signal, DP - Don't Preserve, SP - Signal Present,
  II - Internal Interest, ID - Internal Disinterest, LI - Local Interest,
  LD - Local Disinterest, DI - Decapsulation Interface
  EI - Encapsulation Interface, MI - MDT Interface, LVIF - MPLS Encap,
  EX - Extranet, A2 - Secondary Accept, MT - MDT Threshold Crossed,
  MA - Data MDT Assigned, LMI - mLDP MDT Interface, TMI - P2MP-TE MDT Interface
  IRMI - IR MDT Interface

(50.11.30.11,225.255.11.1) Ver: 0x523cc294 RPF nbr: 50.11.30.11 Flags: L RPF, FGID: 11453, -1, -1
Up: 4d15h
  Incoming Interface List
    HundredGigE0/9/0/3.1130 Flags: A, Up: 4d15h
  Outgoing Interface List
    TenGigE0/11/0/6 Flags: F NS, Up: 4d15h
    TenGigE0/1/0/6/3.132 Flags: F NS, Up: 4d15h
    TenGigE0/11/0/1.122 Flags: F NS, Up: 4d15h
```

```
Router#show mrib route 50.11.30.12 detail
```

```
IP Multicast Routing Information Base
Entry flags: L - Domain-Local Source, E - External Source to the Domain,
  C - Directly-Connected Check, S - Signal, IA - Inherit Accept,
  IF - Inherit From, D - Drop, ME - MDT Encap, EID - Encap ID,
  MD - MDT Decap, MT - MDT Threshold Crossed, MH - MDT interface handle
  CD - Conditional Decap, MPLS - MPLS Decap, EX - Extranet
  MoFE - MoFRR Enabled, MoFS - MoFRR State, MoFP - MoFRR Primary
  MoFB - MoFRR Backup, RPFID - RPF ID Set, X - VXLAN
Interface flags: F - Forward, A - Accept, IC - Internal Copy,
  NS - Negate Signal, DP - Don't Preserve, SP - Signal Present,
  II - Internal Interest, ID - Internal Disinterest, LI - Local Interest,
  LD - Local Disinterest, DI - Decapsulation Interface
  EI - Encapsulation Interface, MI - MDT Interface, LVIF - MPLS Encap,
  EX - Extranet, A2 - Secondary Accept, MT - MDT Threshold Crossed,
  MA - Data MDT Assigned, LMI - mLDP MDT Interface, TMI - P2MP-TE MDT Interface
  IRMI - IR MDT Interface

(50.11.30.12,226.255.12.1) Ver: 0x5fe02e5b RPF nbr: 50.11.30.12 Flags: L RPF, FGID: 12686, -1, -1
Up: 4d15h
  Incoming Interface List
```

```
HundredGigE0/9/0/1.1130 Flags: A, Up: 4d15h
Outgoing Interface List
Bundle-Ether121 Flags: F NS, Up: 4d15h
Bundle-Ether132 Flags: F NS, Up: 4d15h
TenGigE0/11/0/6.117 Flags: F NS, Up: 4d15h
```

## PIM-SSM の設定

### 設定例

アクセス リスト 4 で定義されている IPv4 アドレス範囲に SSM サービスを設定します。

```
Router#config
Router(config)#ipv4 access-list 4
Router(config-ipv4-acl)#permit ipv4 any 224.2.151.0 0.0.0.255
Router(config-ipv4-acl)#exit
Router(config)#multicast-routing
Router(config-mcast)#address-family ipv4
Router(config-mcast-default-ipv4)#ssm range 4
Router(config-mcast-default-ipv4)#commit
Router(config-mcast-default-ipv4)#end
```

### 実行コンフィギュレーション

```
Router#show running multicast-routing
multicast-routing
  address-family ipv4
    ssm range 4
  interface all enable
!
```

### 確認

設定されたパラメータに従って SSM 範囲が設定されているかどうかを確認します。

```
Router#show access-lists 4
ipv4 access-list 4
 10 permit ipv4 any 224.2.151.0 0.0.0.255

*/Verify if the SSM is configured for 224.2.151.0/24/*:
```

```
Router#show pim group-map
IP PIM Group Mapping Table
(* indicates group mappings being used)
Group Range      Proto Client  Groups RP address  Info
224.0.1.39/32*   DM    perm      1     0.0.0.0
224.0.1.40/32*   DM    perm      1     0.0.0.0
224.0.0.0/24*    NO    perm      0     0.0.0.0
224.2.151.0/24*  SSM    config    0     0.0.0.0
```

## PIM パラメータの設定

PIM 固有のパラメータを設定するには、router pim コンフィギュレーション モードが使用されます。デフォルト設定プロンプトは IPv4 用で、config-pim-default-ipv4 と表示されます。LAN セグメント上でルータを PIM DR として確実に選択するには、**dr-priority** コマンドを使用します。DR 優先度が最も高いルータが選択されます。デフォルトでは、事前設定されたしきい値で、ラストホップルータは最短パスツリーに参加してマルチキャストトラフィックを受信できます。この動作を変更するには、router pim コンフィギュレーション モードで **spt-threshold infinity** コマンドを使用しま

す。これにより、ラストホップルータが共有ツリーに永続的に参加することになります。ルータがPIM helloメッセージをネイバーに送信する頻度は、`hello-interval` コマンドで設定できます。デフォルトでは、30秒ごとにPIM helloメッセージが送信されます。`hello-interval` が `router pim` コンフィギュレーションモードで設定されている場合、PIMが有効になっているすべてのインターフェイスがこの値を継承します。インターフェイスのhello間隔を変更するには、次のように、インターフェイスコンフィギュレーションモードで `hello-interval` コマンドを使用します。

## 設定例

```
Router#configure
Router(config)#router pim
Router(config-pim-default)#address-family ipv4
Router(config-pim-default-ipv4)#dr-priority 2
Router(config-pim-default-ipv4)#spt-threshold infinity
Router(config-pim-default-ipv4)#interface TenGigE0/11/0/1
Router(config-pim-ipv4-if)#dr-priority 4
Router(config-pim-ipv4-if)#hello-interval 45
Router(config-pim-ipv4-if)#commit
```

## 実行コンフィギュレーション

```
Router#show run router pim
router pim
 address-family ipv4
  dr-priority 2
  spt-threshold infinity
  interface TenGigE0/11/0/1
    dr-priority 4
    hello-interval 45
```

## 確認

設定された値に従ってパラメータが設定されているかどうかを確認します。

```
Router#show pim interface te0/11/0/1
PIM interfaces in VRF default
Address          Interface          PIM Nbr  Hello DR      DR Count Intvl  Prior
100.1.1.1        TenGigE0/11/0/1  on  1    45   4        this system
```

# Multicast Source Discovery Protocol

Multicast Source Discovery Protocol (MSDP) は、複数のPIM スパースモードドメインを接続するためのメカニズムです。MSDPを使用すると、さまざまなドメイン内のすべてのランデブーポイント (RP) に、グループのマルチキャスト送信元を通知できます。各PIM-SMドメインは自身のRPを使用するため、他のドメインのRPに依存する必要はありません。

PIM-SMドメインのRPは、他のドメインのMSDP対応ルータとのMSDPピアリング関係を持ちます。各ピアリング関係は、下位のルーティングシステムによって維持されるTCP接続上で行われます。

MSDPスピーカーは、Source Active (SA) メッセージとも呼ばれるメッセージを交換します。RPは、一般にPIM registerメッセージを通じてローカルアクティブソースについて学習するとき、MSDPプロセスがSAメッセージのregisterをカプセル化し、ピアに情報を転送します。メッセージには、マルチキャストフローの送信元およびグループの情報と、カプセル化されたデータが格納されます。ネイバーRPにマルチキャストグループのローカル加入者がある場合、RP

は S,G ルートをインストールし、SA メッセージに含まれるカプセル化データを転送し、送信元に向けて PIM join を逆に送信します。このプロセスは、マルチキャストパスをドメイン間で構築する方法について説明します。



(注) 最適な MSDP ドメイン間動作のために BGP またはマルチプロトコル BGP を設定することをお勧めしますが、Cisco IOS XR ソフトウェアの実装では必須とは見なされません。BGP またはマルチプロトコル BGP を MSDP とともに使用する方法については、インターネット技術特別調査委員会 (IETF) インターネットドラフト『Multicast Source Discovery Protocol (MSDP)』に記載されている MSDP RPF ルールを参照してください。

## PIM-SM ドメインと MSDP の相互接続

別のドメインの MSDP 対応ルータとの MSDP ピアリング関係を設定するには、ローカルルータに、MSDP ピアを設定します。

ドメインに BGP ピアを設定しないか設定できない場合、すべての Source-Active (SA) メッセージを受け入れるデフォルト MSDP ピアを定義できます。

最後に、MSDP メッシュグループ内の複数のルータで論理 RP を設定するときに、送信元 ID を変更できます。

### 始める前に

すべての MSDP ピアのアドレスが BGP またはマルチプロトコル BGP で認識されていない場合、MSDP のデフォルトピアリング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 | <b>configure</b>  |  |
| ステップ 2 | <b>interface type interface-path-id</b><br>例 :<br><br>RP/0/RP0/CPU0:router(config)# interface loopback 0            | (任意) インターフェイス コンフィギュレーションモードを開始し、インターフェイスの IPv4 アドレスを定義します。<br><br>(注) この手順は、プライマリアドレスが TCP 接続の送信元 IP アドレスとなるインターフェイスのタイプおよび番号を指定する場合に必要です。                  |
| ステップ 3 | <b>ipv4 address address mask</b><br>例 :<br><br>RP/0/RP0/CPU0:router(config-if)# ipv4 address 10.0.1.3 255.255.255.0 | (任意) インターフェイスの IPv4 アドレスを定義します。<br><br>(注) この手順は、プライマリアドレスが TCP 接続の送信元 IP アドレスとなるインターフェイスのタイプおよび番号を指定する場合にのみ必要です。connect-source コマンドの設定については、オプションを参照してください。 |

|         | コマンドまたはアクション  | 目的   |
|---------|---|--|
| ステップ 4  | <b>exit</b><br>例：<br><br>RP/0/RP0/CPU0:router(config-if)# end   | インターフェイス コンフィギュレーション モードを終了します。  |
| ステップ 5  | <b>router msdp</b><br>例：<br><br>RP/0/RP0/CPU0:router(config)# router msdp   | MSDP プロトコル コンフィギュレーション モードを開始します。  |
| ステップ 6  | <b>default-peer ip-address [ prefix-list list]</b><br>例：<br><br>RP/0/RP0/CPU0:router(config-msdp)# default-peer 172.23.16.0 | (任意) すべての MSDP SA メッセージの受信元となるデフォルト ピアを定義します。  |
| ステップ 7  | <b>originator-id type interface-path-id</b><br>例：<br><br>RP/0/RP0/CPU0:router(config-msdp)# originator-id /1/1/0            | (任意) Source-Active (SA) メッセージのソースの MSDP スピーカーがインターフェイスの IP アドレスを SA メッセージ内で RP アドレスとして使用できるようにします。   |
| ステップ 8  | <b>peer peer-address</b><br>例：<br><br>RP/0/RP0/CPU0:router(config-msdp)# peer 172.31.1.2                                    | MSDP ピア コンフィギュレーション モードを開始し、MSDP ピアを設定します。<br><br><ul style="list-style-type: none"> <li>• BGP ネイバーとしてルータを設定します。</li> <li>• この MSDP ピアとともに BGP ピアも使用する場合は、MSDP と BGP で同一の IP アドレスを使用する必要があります。MSDP ピア間に BGP またはマルチプロトコル BGP パスがある場合は、MSDP ピアとともに BGP またはマルチプロトコル BGP を実行する必要はありません。</li> </ul> |
| ステップ 9  | <b>connect-source type interface-path-id</b><br>例：<br><br>RP/0/RP0/CPU0:router(config-msdp-peer)# connect-source loopback 0 | (任意) MSDP 接続に使用される送信元アドレスを設定します。   |
| ステップ 10 | <b>mesh-group name</b><br>例：  | (任意) MSDP ピアをメッシュ グループのメンバーとして設定します。   |

|         | コマンドまたはアクション  | 目的                            |
|---------|---|-------------------------------|
|         | RP/0/RP0/CPU0:router(config-msdp-peer)#<br>mesh-group internal  |                               |
| ステップ 11 | <b>remote-as <i>as-number</i></b><br>例：<br><br>RP/0/RP0/CPU0:router(config-msdp-peer)# remote-as<br>250         | (任意) このピアのリモート自律システム番号を設定します。 |
| ステップ 12 | <b>commit</b>   |                               |
| ステップ 13 | <b>show msdp [ipv4] globals</b><br>例：<br><br>RP/0/RP0/CPU0:router# show msdp globals                            | MSDP のグローバル変数を表示します。          |
| ステップ 14 | <b>show msdp [ipv4] peer [<i>peer-address</i>]</b><br>例：<br><br>RP/0/RP0/CPU0:router# show msdp peer 172.31.1.2 | MSDP ピアに関する詳細情報を表示します。        |
| ステップ 15 | <b>show msdp [ipv4] rpf <i>rpf-address</i></b><br>例：<br><br>RP/0/RP0/CPU0:router# show msdp rpf 172.16.10.13    | RPF ルックアップを表示します。             |

## MSDP ピア ルータの送信元情報の制御

MSDP ピア ルータは、送信、転送、受信、キャッシュ、カプセル化される送信元情報を制御するようにカスタマイズできます。

Source-Active (SA) メッセージを送信する場合、送信元情報の送信先を、情報を要求している送信元に基づいて制御できます。

SA メッセージを転送する場合、次のことを行うことができます。

- すべての送信元とグループのペアのフィルタリング
- 特定の送信元とグループのペアだけが通過するように、拡張アクセス リストを指定
- ルート マップの一致条件に基づくフィルタリング

SA メッセージを受信する場合、次のことを行うことができます。

- MSDP ピアからのすべての着信 SA メッセージのフィルタリング
- 特定の送信元とグループのペアが通過するように、拡張アクセス リストを指定
- ルート マップの一致条件に基づくフィルタリング

また、TimeToLive (TTL) を使用して、各送信元の最初の SA メッセージにカプセル化されるデータを制御できます。たとえば、内部トラフィックの TTL を 8 ホップに制限したとします。他のグループを外部に送信する場合は、これらのパケットの TTL を 8 ホップより大きく設定して送信します。

デフォルトでは、新しいメンバがグループに加入してマルチキャスト トラフィックを受信する必要がある場合、MSDP はピアに SA メッセージを自動的に送信します。指定された MSDP ピアへの SA 要求を設定する必要はなくなりました。

## 手順

|        | コマンドまたはアクション   | 目的   |
|--------|--|--|
| ステップ 1 | <b>configure</b>   |  |
| ステップ 2 | <b>router msdp</b><br>例：<br><br>RP/0/RP0/CPU0:router(config)# router msdp  | MSDP プロトコル コンフィギュレーション モードを開始します。  |
| ステップ 3 | <b>sa-filter {in   out} {ip-address   peer-name} [ list access-list-name] [ rp-list access-list-name]</b><br>例：<br><br>RP/0/RP0/CPU0:router(config-msdp)# sa-filter out<br>router.cisco.com list 100 | 指定の MSDP ピアから受信するメッセージの着信または発信フィルタ リストを設定します。<br><br><ul style="list-style-type: none"> <li>• <b>list</b> キーワードと <b>rp-list</b> キーワードの両方を指定した場合、送信 Source-Active (SA) メッセージ内の任意の送信元とグループ (S, G) のペアが通過するためには、すべての条件に当てはまる必要があります。</li> <li>• <a href="#">ステップ 7 (17 ページ)</a> で <b>ipv4 access-list</b> コマンドを設定する必要があります。</li> <li>• すべての一致基準に当てはまる場合、ルートマップの <b>permit</b> がフィルタを通してルートを通過します。<b>deny</b> はルートをフィルタ処理します。</li> <li>• 次の例では、アクセス リスト 100 を通過する (S,G) ペアだけが SA メッセージに格納され、<b>router.cisco.com</b> という名前のピアに転送されるように設定します。</li> </ul> |



|        | コマンドまたはアクション  | 目的  |
|--------|---|---|
| ステップ 4 | <p><b>cache-sa-state</b> [ <b>list</b> <i>access-list-name</i>] [ <b>rp-list</b> <i>access-list-name</i>]</p> <p>例 :</p> <pre>RP/0/RP0/CPU0:router(config-msdp)# cache-sa-state 100</pre>                                     | <p>受信した Source-Active (SA) メッセージから送信元とグループのペアを作成し、アクセスリストを通じてペアを制御します。</p>  |
| ステップ 5 | <p><b>ttl-threshold</b> <i>ttl-value</i></p> <p>例 :</p> <pre>RP/0/RP0/CPU0:router(config-msdp)# ttl-threshold 8</pre>   | <p>(任意) SA メッセージで MSDP ピアに送信されるマルチキャストデータを制限します。</p> <ul style="list-style-type: none"> <li>• IP ヘッダーの TTL が <i>ttl-value</i> 引数以上であるマルチキャストパケットだけが、IP アドレスまたは名前により指定された MSDP ピアに送信されます。</li> <li>• TTL によりマルチキャストデータトラフィックを検査する場合、このコマンドを使用します。たとえば、内部トラフィックの TTL を 8 に制限したとします。その他のグループが外部の場所に移動できるようにするには、8 よりも大きい TTL を使用してパケットを送信します。</li> <li>• 次の例では、TTL しきい値を 8 ホップに設定します。</li> </ul> |
| ステップ 6 | <p><b>exit</b></p> <p>例 :</p> <pre>RP/0/RP0/CPU0:router(config-msdp)# exit</pre>  | <p>現在のコンフィギュレーションモードを終了します。</p>   |
| ステップ 7 | <p><b>ipv4 access-list</b> <i>name</i> [<i>sequence-number</i>] <b>permit</b> <i>source</i> [<i>source-wildcard</i>]</p> <p>例 :</p> <pre>RP/0/RP0/CPU0:router(config)# ipv4 access-list 100 20 permit 239.1.1.1 0.0.0.0</pre> | <p>SA フィルタリングによって使用される IPv4 アクセスリストを定義します。</p> <ul style="list-style-type: none"> <li>• この例では、アクセスリスト 100 がマルチキャストグループ 239.1.1.1 を許可します。</li> <li>• SA フィルタリングのために <a href="#">ステップ 3 (16 ページ)</a> でキーワード <b>list</b> が設定されている場合は、<b>ipv4 access-list</b> コマンドが必要です。</li> </ul>   |
| ステップ 8 | <p><b>commit</b></p>  |   |

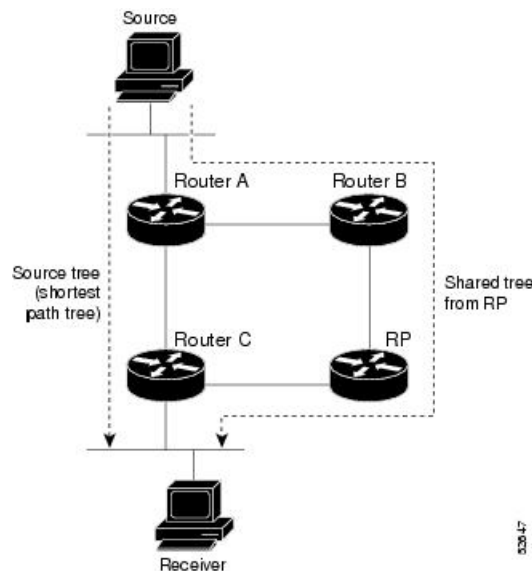
## PIM スパース モード

通常、スパースモードのPIM (PIM-SM) 動作は、マルチキャストネットワークで比較的少数のルータがマルチキャストに関連する場合に使用されます。ルータは、トラフィックの明示的な要求がない場合、グループのマルチキャストパケットを転送しません。要求は、ツリーのルートノードに向けてホップバイホップで送信されるPIM joinメッセージを使用して行われます。PIM-SMのツリーのルートノードは、共有ツリーの場合はランデブーポイント (RP)、最短パスツリー (SPT) の場合はマルチキャスト送信元に直接接続されているファーストホップルータになります。RPはマルチキャストグループを追跡し、マルチキャストパケットを送信する送信元は送信元のファーストホップルータによってRPに登録されます。

PIM joinがツリーの上位方向に送信されると、要求されたマルチキャストトラフィックがツリーの下位方向に転送されるように、パス上のルータがマルチキャスト転送状態を設定します。マルチキャストトラフィックが不要になったら、ルータはルートノードに向けてツリーの上位方向にPIM pruneメッセージを送信し、不必要なトラフィックをプルーニング (削除) 送信します。このPIM pruneがホップごとにツリーを上位方向に移動する際、各ルータはその転送状態を適切に更新します。最終的に、マルチキャストグループまたは送信元に関連付けられている転送状態は削除されます。また、pruneが明示的に送信されない場合、以降のjoinメッセージがないと、PIMステートがタイムアウトし削除されます。

この図は、マルチキャスト環境で動作しているIGMPとPIM-SMを示しています。

図1: 共有ツリーおよびソースツリー (最短パスツリー)



PIM-SMでは、特定のグループにデータを送信する送信元と、そのグループにjoinを送信する受信先をブリッジングするために、ランデブーポイント (RP) が使用されます。状態の初期設定では、対象の受信先は、RPをルートとする単一のデータ配布ツリーを通じて、送信側からグループへのデータを受信します。上の図4: 共有ツリーおよびソースツリー (最短パスツリー) に示すように、このタイプの配布ツリーは共有ツリーまたはランデブーポイントツリー (RPT) と呼ばれます。送信側からのデータは、RPに配信され、その共有ツリーに加入しているグループメンバに配布されます。

コマンドが設定されていない場合、この初期状態は、トラフィックがリーフルータ（受信先ホストに最も近い指定ルータ）で受信されるとすぐに別の状態になります。リーフルータが RPT 上の RP からトラフィックを受信すると、ルータはトラフィックを送信する送信元で開始されるデータ配信ツリーに切り替えを開始します。このタイプの配布ツリーは、最短パス ツリーまたはソース ツリーと呼ばれます。デフォルトでは、Cisco IOS XR ソフトウェアが送信元から最初のデータ パケットを受信すると、送信元ツリーに切り替わります。

次に、共有ツリーから送信元ツリーに切り替わるプロセスの詳細を示します。

1. 受信先がグループに加入します。リーフルータ C が RP に join メッセージを送信します。
2. RP がルータ C へのリンクを発信インターフェイス リストに登録します。
3. 送信元がデータを送信します。ルータ A が Register にデータをカプセル化し、それを RP に送信します。
4. RP が共有ツリーの下位方向のルータ C にデータを転送し、送信元に join メッセージを送信します。この時点で、データは RP に 2 回（カプセル化された状態で 1 回、ネイティブの状態ですべて 1 回）着信する可能性があります。
5. データがネイティブ状態（カプセル化されていない状態）で RP に着信すると、RP は register-stop メッセージをルータ A に送信します。
6. デフォルトでは、ルータ C は、最初のデータ パケットを受信した時点で、送信元に join メッセージを送信します。
7. ルータ C が (S,G) でデータを受信すると、ルータ C は共有ツリーの上位方向にある送信元に prune メッセージを送信します。
8. RP が (S,G) の発信インターフェイスからルータ C へのリンクを削除します。RP が送信元への prune メッセージをトリガーします。
9. 送信元および RP に join および prune メッセージが送信されます。これらのメッセージはホップバイホップで送信され、送信元または RP に向かうパス上の各 PIM ルータによって処理されます。register および register-stop メッセージは、ホップバイホップで送信されません。これらのメッセージは、送信元に直接接続されている指定ルータと、そのグループの RP の間で、直接ユニキャスト通信を使用して交換されます。



---

(注) **spt-threshold infinity** コマンドを使用すると、最短パス ツリー（SPT）に切り替わらないようにルータを設定できます。

---

## PIM ブートストラップルータ

PIM ブートストラップルータ（BSR）は、Auto-RP プロセスを簡素化する、フォールトトレラントで自動的な RP 検出と配信メカニズムを提供します。この機能はデフォルトでイネーブルになり、ルータはグループから RP へのマッピングを動的に学習できます。

PIM は BSR を使用して各グループプレフィックスの RP 設定情報を検出し、PIM ドメイン内のすべてのルータにアナウンスします。これは、Auto-RP によって行われるのと同じ機能ですが、BSR は PIM 仕様の一部です。BSR メカニズムは、Cisco ルータ上の Auto-RP と相互運用します。

シングルポイント障害を回避するために、1 つの PIM ドメインに複数の候補 BSR を設定できます。BSR は候補 BSR の中から自動的に選択されます。

候補はブートストラップメッセージを使用して最もプライオリティの高い BSR を検出します。プライオリティの高い候補は、PIM ドメイン内のすべての PIM ルータに、BSR であると通知を送信します。

候補 RP として設定されたルータは、BSR に、各自が担当するグループ範囲をユニキャストします。BSR はブートストラップメッセージにこの情報を含め、ドメイン内のすべての PIM ルータに広めます。この情報に基づいて、すべてのルータが特定の RP にマルチキャストグループをマッピングできます。ルータがブートストラップメッセージを受信する限り、RP マップは最新になります。

## PIM ブートストラップルータの設定

### 設定例

ハッシュ マスク長が 30 の候補 BSR としてルータを設定します。

```
Router#config
Router(config)#router pim
Router(config-pim-default-ipv4)#bsr candidate-bsr 1.1.1.1 hash-mask-len 30 priority 1
Router(config-pim-default-ipv4-if)#commit
```

ルータが自身を候補ランデブーポイントとして PIM ドメイン内の BSR にアドバタイズするようルータを設定します。アクセスリスト番号 4 は候補ランデブーポイントアドレス 1.1.1.1 に関連付けられたプレフィックスを指定します。このランデブーポイントは、プレフィックス 239 を持つグループに関連します。

```
Router#config
Router(config)#router pim
Router(config-pim-default-ipv4)#bsr candidate-rp 1.1.1.1 group-list 4 priority 192 interval 60

Router(config-pim-default-ipv4)#exit
Router(config)#ipv4 access-list 4
Router(config-ipv4-acl)#permit ipv4 any 239.0.0.0 0.255.255.255
Router(config-ipv4-acl)#commit
```

### 実行コンフィギュレーション

```
Router#show run router pim
router pim
  address-family ipv4
    bsr candidate-bsr 1.1.1.1 hash-mask-len 30 priority 1
    bsr candidate-rp 1.1.1.1 group-list 4 priority 192 interval 60
```

### 確認

```
Router#show pim rp mapping
PIM Group-to-RP Mappings
Group(s) 239.0.0.0/8
  RP 1.1.1.1 (?), v2
    Info source: 1.1.1.1 (?), elected via bsr, priority 192, holdtime 150
    Uptime: 00:02:50, expires: 00:01:54
```

```
Router#show pim bsr candidate-rp
PIM BSR Candidate RP Info
Cand-RP      mode  scope priority uptime      group-list
1.1.1.1      BD    16     192     00:04:06    4
```

```
Router#show pim bsr election
PIM BSR Election State
Cand/Elect-State      Uptime      BS-Timer      BSR              C-BSR
Elected/Accept-Pref  00:03:49  00:00:25  1.1.1.1 [1, 30]  1.1.1.1 [1, 30]
```

## 指定ルータ

Cisco ルータは、LAN セグメント上に複数のルータが存在する場合、PIM を使用してマルチキャスト トラフィックを転送し、選択プロセスに従って指定ルータ (DR) を選択します。

指定ルータは、PIM register メッセージ、PIM join メッセージ、および PIM prune メッセージを RP に送信し、ホストグループメンバーシップに関する情報を通知します。

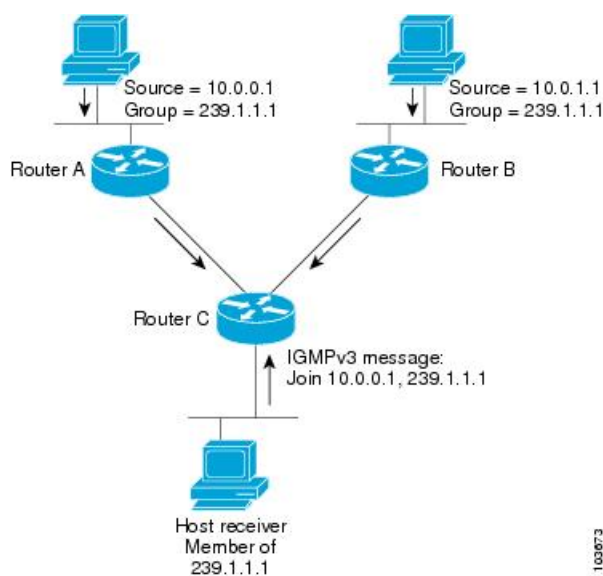
LAN 上に複数の PIM ルータが存在する場合は、指定ルータを選択して、接続されているホストに対するマルチキャスト トラフィックの重複を回避する必要があります。 **dr-priority** コマンドを使用して DR の選択を強制することを選択しない限り、最も大きい IP アドレスの PIM ルータが LAN の DR になります。 DR プライオリティ オプションを使用すると、LAN セグメント上の各ルータの DR プライオリティ (デフォルトのプライオリティ=1) を指定して、最もプライオリティの高いルータが DR として選択されるようにすることができます。 LAN セグメント上のすべてのルータのプライオリティが同じ場合にも、最上位 IP アドレスを持つルータが選択されます。



(注) DR 選択プロセスは、マルチアクセス LAN のみで必要です。ホストに直接接続されているラストホップルータが DR です。

下の図「マルチアクセス セグメントでの指定ルータの選択」では、マルチアクセス セグメントでどのようなことが行われるかを示します。ルータ A (10.0.0.253) とルータ B (10.0.0.251) は、グループ A のアクティブな受信先としてホスト A (10.0.0.1) を持つ共通のマルチアクセスイーサネットセグメントに接続されています。明示的な Join モデルが使用されているので、DR として動作しているルータ A のみが RP に結合し、グループ A の共有ツリーを構築します。ルータ B も (\*,G) Join を RP に送信することが許可されていた場合は、パラレルパスが作成され、ホスト A が重複マルチキャスト トラフィックを受信します。ホスト A がグループにマルチキャスト トラフィックを送信し始めたら、DR は register メッセージを RP に送信する役割を担います。両方のルータに役割が割り当てられている場合は、RP が重複マルチキャスト パケットを受信します。

図 2: マルチアクセス セグメントでの指定ルータの選択



DR で障害が発生した場合、PIM はルータ A の障害を検出し、フェールオーバー DR を選択する手段を提供します。DR (ルータ A) が動作不能になると、ルータ A との隣接ルータとの隣接関係がタイムアウトしたときに、ルータ B はその状況を検出します。ルータ B はホスト A から IGMP メンバーシップ レポートを受けているため、このインターフェイスでグループ A の IGMP ステートをすでに持ち、新しい DR になると即座に RP に join を送信します。この段階で、ルータ B を使用する共有ツリーの新しいブランチの下位方向へのトラフィック フローが再び確立されます。また、ホスト A がトラフィックをソーシングしていた場合、ルータ B は、ホスト A から次のマルチキャスト パケットを受信した直後に、新しい登録プロセスを開始します。このアクションで、RP による、ルータ B を経由する新しいブランチを使用したホスト A への SPT 加入がトリガーされます。



---

(注) 2つのPIMルータが直接接続されている場合、これらのルータはネイバーになります。PIMネイバーを表示するには、EXECモードでshow pim neighbor コマンドを使用します。

---

- ユニキャスト ルーティングに使用されませんが、PIM によってのみ PIM 送信元への IPv4 ネクスト ホップの検索に使用されます。
- 転送情報ベース (FIB) にパブリッシュされません。
- IGP で multicast-intact がイネーブルのときには、リンクステート アドバタイズメントを通して学んだすべての IPv4 の宛先が、等コストの mcast-intact ネクスト ホップのセットと共に RIB に発行されます。この属性はネイティブのネクスト ホップに IGP ショートカットがない場合にも適用されます。
- IS-IS では、ネイティブと mcast-intact の両方のネクスト ホップ数を合計して、最大パス制限が適用されます (OSPFv2 ではこの動作は多少異なります)。

## 設定例

TenGigE インターフェイス 0/11/0/1 では DR 優先度 4 を使用し、他のインターフェイスでは DR 優先度 2 を継承するようにルータを設定します。

```
Router#configure
Router(config)#router pim
Router(config-pim-default)#address-family ipv4
Router(config-pim-default-ipv4)#dr-priority 2
Router(config-pim-default-ipv4)#interface TenGigE0/11/0/1
Router(config-pim-ipv4-if)#dr-priority 4
Router(config-ipv4-acl)#commit
```

## 実行コンフィギュレーション

```
Router#show run router pim
router pim
address-family ipv4
dr-priority 2
spt-threshold infinity
interface TenGigE0/11/0/1
dr-priority 4
hello-interval 45
```

## 確認

設定された値に従ってパラメータが設定されているかどうかを確認します。

```
Router#show pim interface
PIM interfaces in VRF default
Address      Interface      PIM Nbr  Hello DR  DR Count Intvl  Prior
100.1.1.1    TenGigE0/11/0/1  on  1    45  4    this system
```

## インターネット グループ管理プロトコル (IGMP)

Cisco IOS XR ソフトウェアは、IPv4 上のインターネット グループ管理プロトコル (IGMP) をサポートします。

IGMP は、ホストが関心を持っているマルチキャストトラフィックを示し、ルータがネットワーク全体でマルチキャストトラフィックのフローを制御および制限するための方法を提供します。ルータは、IGMP メッセージ（つまり、ルータのクエリーおよびホスト レポート）を使用して状態を構築します。

同じ送信元からのマルチキャストデータストリームを受信する一連のルータおよびホストは、マルチキャストグループと呼ばれます。ホストでは、IGMP メッセージを使用して、マルチキャストグループに加入し、マルチキャストグループを脱退します。



---

(注) IGMP メッセージはクラス D の IP アドレスであるグループアドレスを使用します。クラス D アドレスの上位 4 ビットは 1110 です。ホストグループアドレスの範囲は、224.0.0.0 ~ 239.255.255.255 です。アドレスは、どのグループにも割り当てられません。アドレス 224.0.0.1 は、サブネットのシステムすべてに割り当てられます。アドレス 224.0.0.2 は、サブネットのルータすべてに割り当てられます。

---

### 制約事項

VPLS ブリッジ ドメインでの IGMP スヌーピングはサポートされていません。

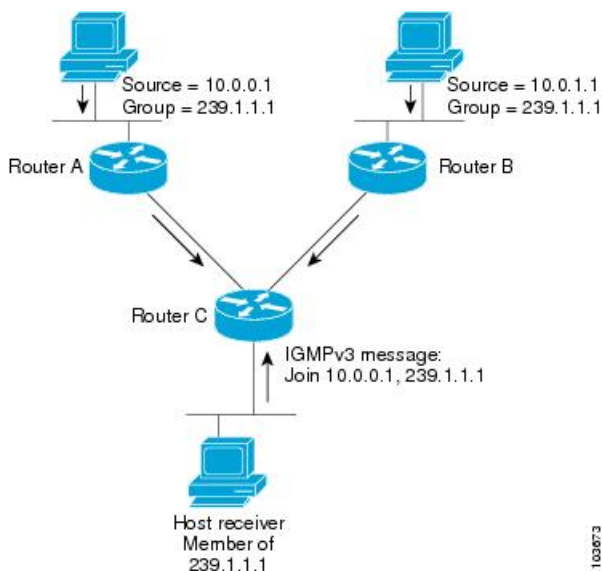
### IGMP ルーティングの機能

次のイメージ「IGMP シグナリング」は、グループ 239.1.1.1 にマルチキャストする 2 つの送信元、10.0.0.1 および 10.0.1.1 を示しています。

レシーバは、グループ 239.1.1.1 宛のトラフィックのうち、送信元 10.0.0.1 からのトラフィックを受信し、送信元 10.0.1.1 からのトラフィックを受信しません。

ホストは、参加する送信元とグループ (S,G) のリストと、参加しない送信元とグループ (S,G) のリストを含む IGMPv3 メッセージを送信する必要があります。ルータ C は、この情報を使用して、送信元 10.0.1.1 からのトラフィックをルーティングし、送信元 10.0.0.1 のトラフィックのみがルータ C に配信されるようにすることができます。

図 3: IGMP シグナリング



## IGMP Per Interface States Limit の設定

IGMP Per Interface States Limit は、IGMP インターフェイスの OIF を作成する際の制限を設定するものです。設定された制限に達すると、グループはこのインターフェイスに対しては考慮されませんが、グループは他のインターフェイス用に IGMP コンテキスト内に存在することができます。

- ユーザが最大 20 のグループを設定していて、グループの最大数に達した場合、それ以上グループを作成することはできません。ユーザがグループの最大数を 10 に減らすと、20 の Join が残り、最大数に到達するというメッセージが表示されます。グループ数が 10 未満になるまで、Join を追加することはできません。
- ユーザがすでに最大 30 の Join を設定していて、最大 20 を追加した場合、最大数に達したことを示すメッセージが表示されます。状態の変更は行われません。また、グループのしきい値数がグループの最大数を下回るまで、Join は発生しなくなります。

### 設定例

すべてのインターフェイスに対し、インターフェイスごとのグループの最大数を 4000 に設定します。ただし、TenGigE インターフェイス 0/11/0/0 は例外で、このインターフェイスでは 3000 に設定します。

```
Router#config
Router(config)#router igmp
Router(config-igmp)#maximum groups-per-interface 4000
Router(config-igmp)#interface TenGigE0/11/0/0
Router(config-igmp-default-if)#maximum groups-per-interface 3000
Router(config-igmp-default-if)#commit
```

### 実行コンフィギュレーション

```
router igmp
interface TenGigE0/11/0/0
maximum groups-per-interface 3000
!
```



```
maximum groups-per-interface 4000
!
```

## 確認

```
Router#show igmp summary
Robustness Value 2
No. of Group x Interfaces 37
Maximum number of Group x Interfaces 50000
Supported Interfaces : 9
Unsupported Interfaces: 0
Enabled Interfaces : 8
Disabled Interfaces : 1
MTE tuple count : 0
Interface          Number  Max #
                   Groups   Groups
Loopback0          4       4000
TenGigE0/11/0/0    5       4000
TenGigE0/11/0/1    5       4000
TenGigE0/11/0/2    0       4000
TenGigE0/11/0/3    5       4000
TenGigE0/11/0/4    5       3000
TenGigE0/11/0/5    5       4000
TenGigE0/11/0/6    5       4000
TenGigE0/11/0/6.1  3       4000
```

## SSM 静的送信元マッピング

指定したアクセスリスト (4) によって記述された SSM グループをマッピングする複数の送信元の一部として送信元 (1.1.1.1) を設定します。

## 設定例

```
Router#configure
Router(config)#ipv4 access-list 4
Router(config-ipv4-acl)#permit ipv4 any 229.1.1.0 0.0.0.255
Router(config-ipv4-acl)#exit
Router(config)# multicast-routing
Router(config-mcast)#address-family ipv4
Router(config-mcast-default-ipv4)#ssm range 4
Router(config-mcast-default-ipv4)#exit
Router(config-mcast)#exit
Router(config)#router igmp
Router(config-igmp)#ssm map static 1.1.1.1 4
*/Repeat the above step as many times as you have source addresses to include in the set for SSM mapping/*
Router(config-igmp)#interface TenGigE0/11/0/3
Router(config-igmp-default-if)#static-group 229.1.1.1
Router(config-igmp-default-if)#commit
```

## 実行コンフィギュレーション

```
Router#show run multicast-routing
multicast-routing
 address-family ipv4
  ssm range 4
 interface all enable
!
!
Router#show access-lists 4
ipv4 access-list 4
```

```
10 permit ipv4 any 229.1.1.0 0.0.0.255
```

```
Router#show run router igmp
router igmp
 interface TenGigE0/11/0/3
 static-group 229.1.1.1
 !
 ssm map static 1.1.1.1 4
```

## 確認

設定された値に従ってパラメータが設定されているかどうかを確認します。

```
Router#show mrib route 229.1.1.1 detail
IP Multicast Routing Information Base
Entry flags: L - Domain-Local Source, E - External Source to the Domain,
 C - Directly-Connected Check, S - Signal, IA - Inherit Accept,
 IF - Inherit From, D - Drop, ME - MDT Encap, EID - Encap ID,
 MD - MDT Decap, MT - MDT Threshold Crossed, MH - MDT interface handle
 CD - Conditional Decap, MPLS - MPLS Decap, EX - Extranet
 MoFE - MoFRR Enabled, MoFS - MoFRR State, MoFP - MoFRR Primary
 MoFB - MoFRR Backup, RPFID - RPF ID Set, X - VXLAN
Interface flags: F - Forward, A - Accept, IC - Internal Copy,
 NS - Negate Signal, DP - Don't Preserve, SP - Signal Present,
 II - Internal Interest, ID - Internal Disinterest, LI - Local Interest,
 LD - Local Disinterest, DI - Decapsulation Interface
 EI - Encapsulation Interface, MI - MDT Interface, LVIF - MPLS Encap,
 EX - Extranet, A2 - Secondary Accept, MT - MDT Threshold Crossed,
 MA - Data MDT Assigned, LMI - mLDP MDT Interface, TMI - P2MP-TE MDT Interface
 IRMI - IR MDT Interface
(1.1.1.1,229.1.1.1) RPF nbr: 1.1.1.1 Flags: RPF
Up: 00:01:11
Incoming Interface List
Loopback0 Flags: A, Up: 00:01:11
Outgoing Interface List
TenGigE0/11/0/3 Flags: F NS LI, Up: 00:01:11
```

## 複数の送信元での IPv6 マルチキャスト

このリリースまで、IPv6 マルチキャストのサポートでは、各マルチキャストグループに対して送信元が1つに制限されていました。ただし、複数の送信元が関係している場合は、複数の送信元のマルチキャストフローが、対象の受信者すべてに対して複製されていました。

リリース 6.6.1 以降では、IPv6 マルチキャストは、1つのマルチキャストグループに対して複数の送信元をサポートしています。



---

(注) ルータに LC がある場合（外部 TCAM の有無にかかわらず）、ルータはデフォルトの IPv6 マルチキャストルーティングスケールで動作します。これは、外部 TCAM を使用せずに LC 上でプログラミングされます。

---

## 使用例：ビデオストリーミング

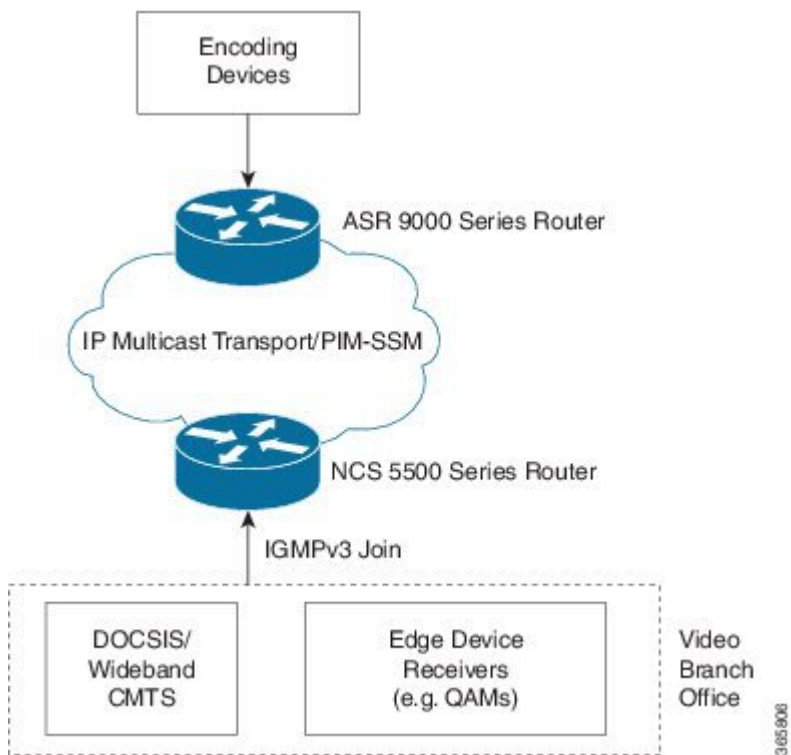
今日のブロードキャストビデオネットワークでは、独自のトランスポートシステムを使用して、各ビデオブランチオフィスにすべてのチャンネルラインナップを配信しています。IP ベースのトランスポートネットワークは、他の IP ベースのサービスの配信と組み合わせたビデオ サービスを提供するためのコスト効率のよい/便利な代替手段となります。（インターネット配信またはビジネス サービス）

ブロードキャストビデオは、その性質上、エンドカスタマーに到達するためのより効率的な配信メカニズムとして IP マルチキャストを使用するのに適したサービスです。

ブロードキャストビデオの IP マルチキャスト配信の説明は次のとおりです。

1. デジタル マスターヘッドエンドでデバイスをエンコーディングし、1 つまたは複数のビデオチャンネルを、IP マルチキャストを介してネットワークで伝送される Moving Pictures Expert Group (MPEG) ストリームにエンコードします。
2. ビデオブランチオフィスのデバイスは、オペレータによって、IGMP Join を介して目的のマルチキャストコンテンツを要求するように構成されます。
3. マルチキャストルーティングプロトコルとして PIM-SSM を使用するネットワークは、マルチキャストストリームをデジタルマスターヘッドエンドからビデオブランチオフィスにあるエッジデバイスレシーバにルーティングします。これらのエッジデバイスは、RF 周波数の場合は MPEG ストリームを、または DOCSIS の場合は CMTS を調整するエッジ QAM デバイスが考えられます。

図 4: ビデオストリーミング



## コアでのマルチキャスト ラベル配布プロトコル (MLDP)

マルチキャスト ラベル配布プロトコル (MLDP) は、マルチプロトコル ラベル スイッチング (MPLS) ネットワークにポイントツーマルチポイント (P2MP) およびマルチポイントツーマルチポイント (MP2MP) ラベル スイッチドパス (LSP) を設定できるようにラベル配布プロトコル (LDP) を拡張したものです。

MLDP はコア全体にわたり、マルチキャスト パケットを転送するためのネイティブ マルチキャスト PIM の使用を無効化します。MLDP マルチキャスト トラフィックは、コア全体でラベル スイッチングされます。これにより、多くのコントロールプレーン処理の作業が削減されます。

### コアでの MLDP プロファイルの特性

ルータがコア ルータとして設定されている場合、次の MLDP プロファイルがサポートされます。

- プロファイル 5 : パーティション MDT - MLDP P2MP - BGP-AD - PIM C-mcast シグナリング
- プロファイル 6 : VRF MLDP - インバンド シグナリング
- プロファイル 7 : グローバル MLDP - インバンド シグナリング
- プロファイル 8 : グローバル P2MP-TE
- プロファイル 10 : BGP AD を使用した VRF Static-P2MP-TE
- プロファイル 12 : デフォルト MDT - MLDP - P2MP - BGP-AD - BGP C-mcast シグナリング
- プロファイル 14 : パーティション MDT - MLDP P2MP - BGP-AD - BGP C-mcast シグナリング
- プロファイル 17 : デフォルト MDT - MLDP - P2MP - BGP-AD - PIM C-mcast シグナリング

### コアでの MLDP の設定例

```
mpls ldp
 mldp
  logging notifications
  address-family ipv4
  !
 !
 !
```

## ラベルスイッチドマルチキャスト (LSM) マルチキャスト ラベル配布プロトコル (mLDP) ベースのマルチキャスト VPN (mVPN) のサポート

ラベルスイッチドマルチキャスト (LSM) はラベルカプセル化を使用してマルチキャストをサポートする MPLS テクノロジーの拡張機能です。次世代 MVPN は、MPLS ネットワークを介して P2MP および MP2MP LSP を構築するため

に使用できるマルチキャストラベル配布プロトコル (mLDP) に基づいています。これらの LSP は、グローバルテーブルまたは VPN のコンテキストで IPv4 と IPv6 の両方のマルチキャストパケット転送に使用できます。mLDP は、コアルータとエッジルータの両方でサポートされます。

ルータが mLDP を実行するコアルータとして配置されている場合、エッジルータでサポートされているプロファイルに関係なく、プロファイル 5、6、7、12、14、および 17 のみがサポートされます。

ルータが mLDP を実行するエッジルータとして配置されている場合、プロファイル 6、7、8、および 10 のみがサポートされます。



---

(注) IPv6 はプロファイル 10 ではサポートされていません。また、IPv4 SM は、エッジルータの mLDP プロファイルではサポートされていません。

---

## LSM mLDP based MVPN の利点

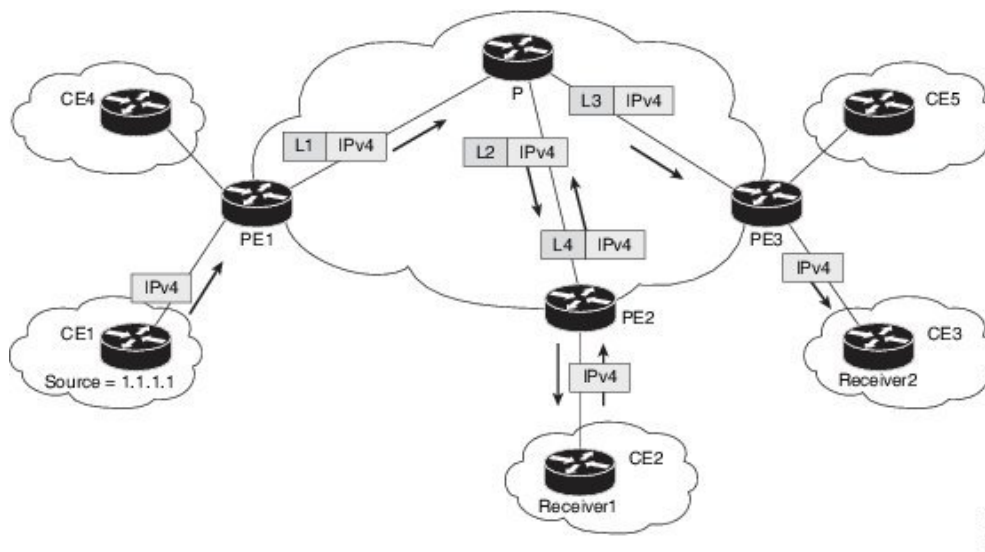
LSM には、コア内のカスタマートラフィックを転送するために現在使用されている GRE コアトンネルと比較した場合、次の利点があります。

- IP マルチキャストパケットを転送するための MPLS インフラストラクチャを活用し、ユニキャストとマルチキャストのための共通のデータプレーンを提供します。
- MPLS の利点を高速再ルーティング (FRR) などの IP マルチキャストに適用します。
- PIM に関連した複雑さを解消します。

## MLDP MVPN の設定

MLDP MVPN の設定により、MPLS を使用した IPv4 マルチキャストパケット配信をイネーブルにします。この設定では、MPLS ラベルを使用して、デフォルトおよびデータマルチキャスト配信ツリー (MDT) を構築します。MPLS レプリケーションは、コアネットワークおよびエッジネットワークの転送メカニズムとして使用されます。MLDPMVPN の設定を有効にするには、MPLS mLDP のグローバル設定がイネーブルであることを確認します。MVPN エクストラネットサポートを設定するには、レシーバプロバイダーエッジ (PE) ルータにソースのマルチキャスト VPN ルーティングおよび転送 (mVRF) を設定するか、ソース PE にレシーバの mVRF を設定します。MLDP MVPN は、イントラネットとエクストラネットの両方に対してサポートされます。

図 5: コア ルータおよびエッジルータの場合の **MLDP based MPLS** ネットワーク



## mLDP ベースのマルチキャスト VPN 内のパケット フロー

着信するパケットごとに、MPLS は複数の外側ラベルを作成します。ソース ネットワークからのパケットは、レシーバネットワークへのパス上で複製されます。CE1 ルータは、ネイティブの IP マルチキャストトラフィックを送信します。プロバイダーエッジ 1 (PE1) ルータは着信マルチキャストパケットにラベルを付加し、MPLS コア ネットワークへのラベル付きパケットを複製します。パケットは、コア ルータ (P) に到達すると、MP2MP のデフォルト MDT または P2MP のデータ MDT に対応する適切なラベル付きで複製され、すべての出力 PE に送信されます。パケットが出力 PE (エッジルータ) に到達すると、ラベルが削除され、IP マルチキャストパケットは VRF インターフェイスに複製されます。基本的に、パケットは PE ルータのヘッドエンドでカプセル化され、テールエンドでカプセル化解除されます。

## mLDP ベースのマルチキャスト VPN の実現

mLDP によって構築されたラベルスイッチドパス (LSP) は、アプリケーションの要件や性質に応じて、次のようないくつかの方法で使用できます。

- インバンドシグナリングを使用したグローバルテーブル中継マルチキャスト用の P2MP LSP。
- MI-PMSI (Multidirectional Inclusive Provider Multicast Service Instance) に基づいた MVPN 用の P2MP/MP2MP LSP (Rosen ドラフト)。
- MS-PMSI (Multidirectional Selective Provider Multicast Service Instance) に基づいた MVPN 用の P2MP/MP2MP LSP (パーティション化 E-LAN)。

ルータは、MLDP の実装のために次の重要な機能を実行します。

1. VRF マルチキャスト IP パケットの GRE/ラベルによるカプセル化、およびコア インターフェイスへの複製 (インポジション ノード)。
2. マルチキャスト ラベル パケットの異なるラベルによる別のインターフェイスへの複製 (中間ノード)。

3. ラベルパケットのカプセル化解除、および VRF インターフェイスへの複製（ディスポジション ノード）。

## エッジルータでの mLDP の制約事項

エッジルータでの mLDP に適用される制約事項は次のとおりです。

- プロファイル 6 および プロファイル 7 については、MVPN 上の NETCONF/YANG はサポートされていません。
- MLDP ping traceroute はサポートされていません。
- IPv6 BVI はサポートされていません。
- MPLS カプセル化マルチキャスト パケットについては Netflow はサポートされていません。

## エッジルータでの VRF MLDP インバンド シグナリングの設定

エッジルータで VRF MLDP インバンド シグナリング（プロファイル 6）を設定するには、次のタスクを実行する必要があります。

1. PIM でルート ポリシーを割り当てることにより、Reverse Path Forwarding（RPF）トポロジを選択します。
2. マルチキャスト配信ツリー（MDT）タイプを MLDP インバンドに設定するルート ポリシーを設定します。
3. マルチキャストルーティングでの MLDP インバンド シグナリングを有効化します。
4. MLDP の MPLS を有効化します。

### 設定

*/\* PIM でルート ポリシーを割り当てることにより、Reverse Path Forwarding（RPF）トポロジを選択 \*/*

```
RP/0/RP0/CPU0:router(config)#router pim
RP/0/RP0/CPU0:router(config-pim)#vrf one
RP/0/RP0/CPU0:router(config-pim-one)#address-family ipv4
RP/0/RP0/CPU0:router(config-pim-one-ipv4)#rpf topology route-policy rpf-vrf-one
```

*/\* MDT タイプを MLDP インバンドに設定するルート ポリシーを設定 \*/*

```
RP/0/RP0/CPU0:router(config)#route-policy rpf-vrf-one
RP/0/RP0/CPU0:router(config-rpl)#set core-tree mldp-inband
RP/0/RP0/CPU0:router(config-rpl)#end-policy
```

*/\* マルチキャストルーティングでの MLDP インバンド シグナリングの有効化 \*/*

```
RP/0/RP0/CPU0:router(config)#multicast-routing
RP/0/RP0/CPU0:router(config-mcast)#vrf one
RP/0/RP0/CPU0:router(config-mcast-one)#address-family ipv4
RP/0/RP0/CPU0:router(config-mcast-one-ipv4)#mdt source loopback 0
RP/0/RP0/CPU0:router(config-mcast-one-ipv4)#mdt mldp in-band-signaling ipv4
RP/0/RP0/CPU0:router(config-mcast-one-ipv4)#interface all enable
```

*/\* MLDP の MPLS を有効化 \*/*

```
RP/0/RP0/CPU0:router(config)#mpls ldp
RP/0/RP0/CPU0:router(config-ldp)#mldp
```

# エッジルータでのグローバルMLDPインバンドシグナリングの設定

エッジルータでグローバルMLDPインバンドシグナリング（プロファイル6）を設定するには、次のタスクを実行する必要があります。

1. PIMでルートポリシーを割り当てることにより、Reverse Path Forwarding（RPF）トポロジを選択します。
2. MDTタイプをMLDPインバンドに設定するルートポリシーを設定します。
3. マルチキャストルーティングでのMLDPインバンドシグナリングを有効化します。
4. MLDPのMPLSを有効化します。

## 設定

*/\* PIMでルートポリシーを割り当てることにより、Reverse Path Forwarding（RPF）トポロジを選択 \*/*

```
RP/0/RP0/CPU0:router(config)#router pim
RP/0/RP0/CPU0:router(config-pim)#address-family ipv4
RP/0/RP0/CPU0:router(config-pim-default-ipv4)#rpf topology route-policy rpf-global
RP/0/RP0/CPU0:router(config-pim-default-ipv4)#interface TenGigE 0/11/0/1
RP/0/RP0/CPU0:router(config-pim-ipv4-if)#enable
```

*/\* MDTタイプをMLDPインバンドに設定するルートポリシーを設定 \*/*

```
RP/0/RP0/CPU0:router(config)#route-policy rpf-global
RP/0/RP0/CPU0:router(config-rpl)#set core-tree mldp-inband
RP/0/RP0/CPU0:router(config-rpl)#end-policy
```

*/\* マルチキャストルーティングでのMLDPインバンドシグナリングの有効化 \*/*

```
RP/0/RP0/CPU0:router(config)#multicast-routing
RP/0/RP0/CPU0:router(config-mcast)#address-family ipv4
RP/0/RP0/CPU0:router(config-mcast-default-ipv4)#interface loopback 0
RP/0/RP0/CPU0:router(config-mcast-default-ipv4-if)#enable
RP/0/RP0/CPU0:router(config-mcast-default-ipv4-if)#exit
RP/0/RP0/CPU0:router(config-mcast-default-ipv4)#mdt source loopback 0
RP/0/RP0/CPU0:router(config-mcast-default-ipv4)#mdt mldp in-band-signaling ipv4
RP/0/RP0/CPU0:router(config-mcast-default-ipv4)#interface all enable
```

*/\* MLDPのMPLSを有効化 \*/*

```
RP/0/RP0/CPU0:router(config)#mpls ldp
RP/0/RP0/CPU0:router(config-ldp)#mldp
```

## MVPN プロファイルの設定例

ここでは、さまざまなMVPNプロファイルについて、プロファイルごとの設定例を示します。

### インバンドmLDPプロファイルの設定例

プロファイル6：VRFインバンドmLDP



```

router bgp 100
 mvpn
 !
multicast-routing
 mdt source Loopback0
 vrf v61
  address-family ipv4
   mdt mtu 1600
   mdt mldp in-band-signaling ipv4
   interface all enable
  !
  address-family ipv6
   mdt mtu 1600
   mdt mldp in-band-signaling ipv4
   interface all enable
  !
 !
router pim
 vrf v61
  address-family ipv4
   rpf topology route-policy mldp-inband
  !
  address-family ipv6
   rpf topology route-policy mldp-inband
  !
 !
route-policy mldp-inband
 set core-tree mldp-inband
end-policy
 !

```

#### プロファイル 7 : グローバル インバンド mLDP

```

multicast-routing
 address-family ipv4
  mdt source Loopback0
  mdt mldp in-band-signaling ipv4
  ssm range Global-SSM-Group
  interface all enable
 !
 address-family ipv6
  mdt source Loopback0
  mdt mldp in-band-signaling ipv4
  ssm range Global-SSM-Group-V6
  interface all enable
 !
router pim
 address-family ipv4
  rpf topology route-policy mldp-inband
 !
 address-family ipv6
  rpf topology route-policy mldp-inband
 !
 !
route-policy mldp-inband
 set core-tree mldp-inband
end-policy
 !

```

## Rosen mLDP プロファイルの設定例

プロファイル 12 : BGP-AD および BGP シグナリングを使用した Rosen mLDP P2MP

```

!
multicast-routing
 mdt source Loopback0
 vrf v121
  address-family ipv4
   mdt mtu 1600
 mdt default mldp p2mp
 mdt data 255
  interface all enable
  bgp auto-discovery mldp
  !
  address-family ipv6
   mdt mtu 1600
 mdt default mldp p2mp
 mdt data 255
  interface all enable
  bgp auto-discovery mldp
  !
!
router pim
 vrf v121
  address-family ipv4
   rpf topology route-policy rosen-mldp
 mdt c-multicast-routing bgp
  !
  address-family ipv6
   rpf topology route-policy rosen-mldp
 mdt c-multicast-routing bgp
  !
!
route-policy rosen-mldp
 set core-tree mldp-default
end-policy
!

```

#### プロファイル 17 : デフォルト MDT - MLDP - P2MP - BGP-AD - PIM C-Mcast シグナリング

```

vrf one
 vpn id 1:1
 address-family ipv4 unicast
  import route-target
   1:1
  !
  export route-target
   1:1
  !
!

router pim
 vrf one
  address-family ipv4
   rpf topology route-policy rpf-for-one
  !
  interface GigabitEthernet0/1/0/0
   enable
  !
  !
!

route-policy rpf-for-one
 set core-tree mldp-default
end-policy
!

```

```

multicast-routing
vrf one
  address-family ipv4
    mdt source Loopback0
    mdt default mldp p2mp
    mdt data 100
    rate-per-route
    interface all enable
    bgp auto-discovery mldp
    !
    accounting per-prefix
  !
!
!

mpls ldp
mldp
  logging notifications
  address-family ipv4
  !
!
!

```

## エッジルータでのインバンド mLDP プロファイルの設定例

### VRF MLDP インバンド シグナリング（プロファイル 6）の実行コンフィギュレーション

```

router pim
vrf one
  address-family ipv4
    rpf topology route-policy rpf-vrf-one

    route-policy rpf-vrf-one
      set core-tree mldp-inband
    end-policy

multicast-routing
vrf one
  address-family ipv4
    mdt source Loopback0
    mdt mldp in-band-signaling ipv4
  interface all enable

mpls ldp
mldp

```

### グローバル MLDP インバンド シグナリング（プロファイル 7）の実行コンフィギュレーション

```

router pim
  address-family ipv4
    rpf topology route-policy rpf-global
    interface TenGigabitEthernet0/11/0/1
      enable

  route-policy rpf-global
    set core-tree mldp-inband
  end-policy

multicast-routing
  address-family ipv4

```

```

interface Loopback0
  enable
!
mdt source Loopback0
mdt mldp in-band-signaling ipv4
interface all enable
!
mpls ldp
  mldp

```

## エッジルータでの MLDP 設定の確認

エッジルータの MLDP 設定を確認するには、次のコマンドを使用します。

MLDP ネイバーをチェックするには、**show mpls mldp neighbor** コマンドを使用します。

```

RP/0/RP0/CPU0:Head# show mpls mldp neighbors
mLDP neighbor database
MLDP peer ID      : 2.2.2.2:0, uptime 07:47:59 Up,
  Capabilities    : GR, Typed Wildcard FEC, P2MP, MP2MP
  Target Adj      : No
  Upstream count  : 1
  Branch count    : 1
  LDP GR          : Enabled
                  : Instance: 1
  Label map timer : never
  Policy filter in :
  Path count      : 1
  Path(s)         : 12.1.1.2          TenGigE0/11/0/1 LDP
  Adj list        : 12.1.1.2          TenGigE0/11/0/1
  Peer addr list  : 2.25.32.2
                  : 2.2.2.2
                  : 11.1.1.1
                  : 12.1.1.2
                  : 13.10.1.1

```

ラベル情報ベース (LIB) の内容を表示するには、**show mpls mldp bindings** コマンドを使用します。

```

RP/0/RP0/CPU0:Head#show mpls mldp bindings
mLDP MPLS Bindings database

LSP-ID: 0x00001 Paths: 7 Flags:
0x00001 P2MP 5.5.5.5 [vpn6 1:1 2015:1:1::3 ff3e::1]
  Local Label: 70009
  Remote Label: 64018 NH: 12.1.1.2 Inft: TenGigE0/11/0/1
  Remote Label: 64022 NH: 50.1.1.1 Inft: TenGigE0/11/0/1
  Remote Label: 30002 NH: 30.10.1.2 Inft: Bundle-Ether56
  Remote Label: 64023 NH: 60.1.1.2 Inft: HundredGigE0/0/1/1
  Remote Label: 64024 NH: 70.1.1.1 Inft: TenGigE0/11/0/2
  Remote Label: 64022 NH: 40.1.1.1 Inft: TenGigE0/11/0/3

```

MLDP イベント トレースを表示するには、**show mpls MLDP trace** コマンドを使用します。

```

RP/0/RP0/CPU0:Head#show mpls mldp trace
3535 wrapping entries (631040 possible, 35584 allocated, 0 filtered, 3535 total)
May 30 23:30:21.121 MLDP GLO 0/RP0/CPU0 t6746 GEN : Trace pre-init iox success
May 30 23:30:21.121 MLDP GLO 0/RP0/CPU0 t6746 GEN : Debug pre-init iox success
May 30 23:30:21.121 MLDP GLO 0/RP0/CPU0 t6746 GEN : API pre-init iox success
May 30 23:30:21.121 MLDP GLO 0/RP0/CPU0 t6746 GEN : Bitfield pre-init iox success

```

May 31 12:08:39.465 MLDP GLO 0/RP0/CPU0 t6746 GEN : mldp\_evm 0x563de8f01698 allocated  
May 31 12:08:39.465 MLDP GLO 0/RP0/CPU0 t6746 GEN : EVM init iox success  
May 31 12:08:39.472 MLDP GLO 0/RP0/CPU0 t6746 GEN : Registered EDM on active success  
May 31 12:08:39.472 MLDP GLO 0/RP0/CPU0 t6746 GEN : EDM Ac/St init iox again  
May 31 12:08:39.472 MLDP GLO 0/RP0/CPU0 t6746 GEN : Registered EDM Location on active success  
May 31 12:08:39.472 MLDP GLO 0/RP0/CPU0 t6746 GEN : EDM Loc init iox success  
May 31 12:08:39.475 MLDP GLO 0/RP0/CPU0 t6746 GEN : LMRIB init iox success  
May 31 12:08:39.475 MLDP GLO 0/RP0/CPU0 t18944 MRIB : MRIB connection established  
May 31 12:08:39.475 MLDP GLO 0/RP0/CPU0 t6746 GEN : Interface manager init iox success  
May 31 12:08:39.475 MLDP GLO 0/RP0/CPU0 t6746 GEN : Async init iox success  
May 31 12:08:39.475 MLDP GLO 0/RP0/CPU0 t6746 GEN : Boolean init iox success  
May 31 12:08:39.475 MLDP GLO 0/RP0/CPU0 t6746 GEN : Timers init iox success  
May 31 12:08:39.479 MLDP GLO 0/RP0/CPU0 t6746 GEN : RUMP init iox success  
May 31 12:08:39.479 MLDP GLO 0/RP0/CPU0 t6746 GEN : Chunks init iox success  
May 31 12:08:39.509 MLDP ERR 0/RP0/CPU0 t6746 RIB : RIB not ready  
May 31 12:08:39.509 MLDP ERR 0/RP0/CPU0 t6746 RIB : RIB not ready  
May 31 12:08:39.512 MLDP GLO 0/RP0/CPU0 t6746 GEN : mldp\_ens\_event\_ctx\_chunk is NULL  
May 31 12:08:39.512 MLDP GLO 0/RP0/CPU0 t6746 GEN : Context Table init iox success  
May 31 12:08:39.512 MLDP GLO 0/RP0/CPU0 t6746 GEN : mldp\_rib\_main\_evm 0x563de8fd23e8 allocated  
May 31 12:08:39.512 MLDP GLO 0/RP0/CPU0 t6746 GEN : RIB Thread EVM init rib success  
May 31 12:08:39.512 MLDP GLO 0/RP0/CPU0 t6746 GEN : RIB Thread Chunk init rib success  
May 31 12:08:39.512 MLDP GLO 0/RP0/CPU0 t6746 GEN : RIB Thread queue init rib success  
May 31 12:08:39.512 MLDP GLO 0/RP0/CPU0 t6746 RIB : Bound to RIB, fd: 354

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com go trademarks](http://www.cisco.com/go/trademarks). Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2019 Cisco Systems, Inc. All rights reserved.

【注意】シスコ製品をご使用になる前に、安全上の注意（[www.cisco.com/jp/go/safety\\_warning/](http://www.cisco.com/jp/go/safety_warning/)）をご確認ください。本書は、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。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

©2008 Cisco Systems, Inc. All rights reserved.

Cisco, Cisco Systems, およびCisco Systemsロゴは、Cisco Systems, Inc.またはその関連会社の米国およびその他の一定の国における登録商標または商標です。

本書類またはウェブサイトに掲載されているその他の商標はそれぞれの権利者の財産です。

「パートナー」または「partner」という用語の使用はCiscoと他社との間のパートナーシップ関係を意味するものではありません。(0809R)

この資料の記載内容は2008年10月現在のものです。

この資料に記載された仕様は予告なく変更する場合があります。



#### シスコシステムズ合同会社

〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー

<http://www.cisco.com/jp>

お問い合わせ先：シスコ コンタクトセンター

0120-092-255 (フリーコール、携帯・PHS含む)

電話受付時間：平日 10:00～12:00、13:00～17:00

<http://www.cisco.com/jp/go/contactcenter/>