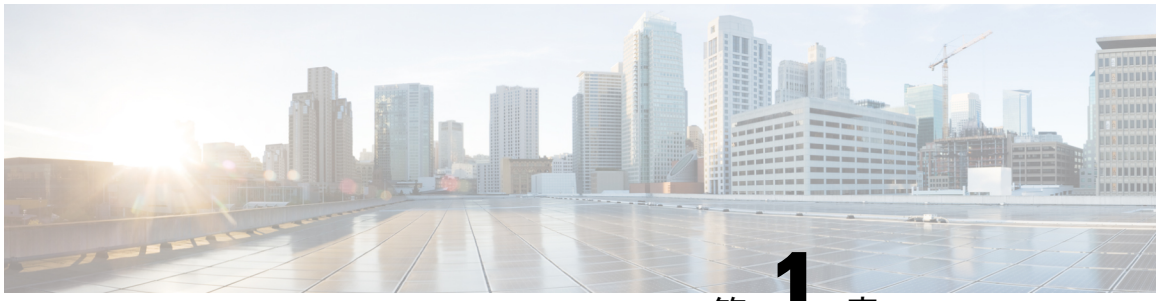
Cisco NCS 560 シリーズ ルータ（Cisco IOS XR リリース 7.1.x）マルチキャスト コンフィギュレーション ガイド

初版：2020 年 1 月 29 日

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/

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

目 次



第 1 章

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。

マルチキャスト ルーティングを実装するために次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。

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 パスを認識している必要があります。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                  Yes
 0/RP0/CPU0


Te0/11/0/0       10.112.112.2   0s(0s*0) 90ms(30ms*3)     UP                  Yes
0/RP0/CPU0



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
25.25.25.2*                  TenGigE 0/11/0/0       1w3d      00:01:41 1 (DR) B P E
32.32.32.2*                  TenGigE 0/11/0/1
       1w4d      00:01:40 1       B P E
32.32.32.3                   TenGigE 0/11/0/1
       1w4d      00:01:42 1 (DR) B P
```

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 を設定するときに、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（mc1）を設定します。

```
Router#configure
Router(config)#ipv4 access-list mc1
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（mc1）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 mc1
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 mc1
```

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 be132
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。

Note 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。

Before you begin

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。

Procedure

	Command or Action	Purpose
ステップ 1	**configure**	
ステップ 2	**interface** *type interface-path-id* **Example:** `RP/0/RP0/cpu 0: 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。 **Note** 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	**ipv4 address** *address mask* **Example:**	（任意）インターフェイスの IPv4 アドレスを定義します。

	Command or Action	Purpose
	`RP/0/RP0/cpu 0: router(config-if)# ipv4 address 10.0.1.3 255.255.255.0`	**Note** 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。
ステップ 4	**exit** **Example:** `RP/0/RP0/cpu 0: 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	**router msdp** **Example:** `RP/0/RP0/cpu 0: 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	**default-peer** *ip-address* [**prefix-list** *list*] **Example:** `RP/0/RP0/cpu 0: 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	**originator-id** *type interface-path-id* **Example:** `RP/0/RP0/cpu 0: 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	**peer** *peer-address* **Example:** `RP/0/RP0/cpu 0: 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。 • BGP ネイバーとしてルータを設定します。 • 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

	Command or Action	Purpose
		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。

ステップ 9	**connect-source** *type interface-path-id*
	Example:
	`RP/0/RP0/cpu 0:`
	`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	**mesh-group** *name*
	Example:
	`RP/0/RP0/cpu 0:`
	`router(config-msdp-peer)# mesh-group internal`
		（任意）MSDP ピアをメッシュ グループのメンバとして設定します。

ステップ 11	**remote-as** *as-number*
	Example:
	`RP/0/RP0/cpu 0:`
	`router(config-msdp-peer)# remote-as 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	**commit**	
ステップ 13	**show msdp** [**ipv4**] **globals** **Example:** `RP/0/RP0/cpu 0: router# show msdp globals`	MSDP のグローバル変数を表示します。
ステップ 14	**show msdp** [**ipv4**] **peer** [*peer-address*] **Example:** `RP/0/RP0/cpu 0: 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	**show msdp** [**ipv4**] **rpf** *rpf-address* **Example:** `RP/0/RP0/cpu 0: router# show msdp rpf`	RPF ルックアップを表示します。

	Command or Action	Purpose
	172.16.10.13	

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、Time To Live（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生じた場合、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。

Procedure

	Command or Action	Purpose
ステップ 1	**configure**	
ステップ 2	**router msdp** **Example:** `RP/0/RP0/cpu 0: 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。

	Command or Action	Purpose
ステップ 3	**sa-filter** {**in** | **out**} {*ip-address* | *peer-name*} [**list** *access-list-name*] [**rp-list** *access-list-name*] **Example:** `RP/0/RP0/cpu 0: router(config-msdp)# sa-filter out 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。 • **list** キーワードと **rp-list** 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。 • ステップ 7, on page 18で **ipv4 access-list** コマンドを設定する必要があります。 • すべての一致基準に当てはまる場合、ルート マップの **permit** がフィルタを通してルートを通過します。**deny** はルートをフィルタ処理します。 • 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、router.cisco.com という名前のピアに転送されるように設定します。
ステップ 4	**cache-sa-state** [**list** *access-list-name*] [**rp-list** *access-list-name*] **Example:** `RP/0/RP0/cpu 0: router(config-msdp)# cache-sa-state 100`	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。
ステップ 5	**ttl-threshold** *ttl-value* **Example:** `RP/0/RP0/cpu 0: router(config-msdp)# ttl-threshold 8`	（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。 • IP ヘッダーの TTL が *ttl-value* 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。 • 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

	Command or Action	Purpose
		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。 • 次の例では、TTL しきい値を 8 ホップに設定します。
ステップ 6	**exit** **Example:** `RP/0/RP0/cpu 0: router(config-msdp)# exit`	現在のコンフィギュレーション モードを終了します。
ステップ 7	**ipv4 access-list** *name* [*sequence-number*] **permit** *source* [*source-wildcard*] **Example:** `RP/0/RP0/cpu 0: router(config)# ipv4 access-list 100 20 permit 239.1.1.1 0.0.0.0`	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。 • 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。 • SA フィルタリングのためにステップ 3, on page 17でキーワード **list** が設定されている場合は、**ipv4 access-list** コマンドが必要です。
ステップ 8	**commit**	

PIM スパース モード

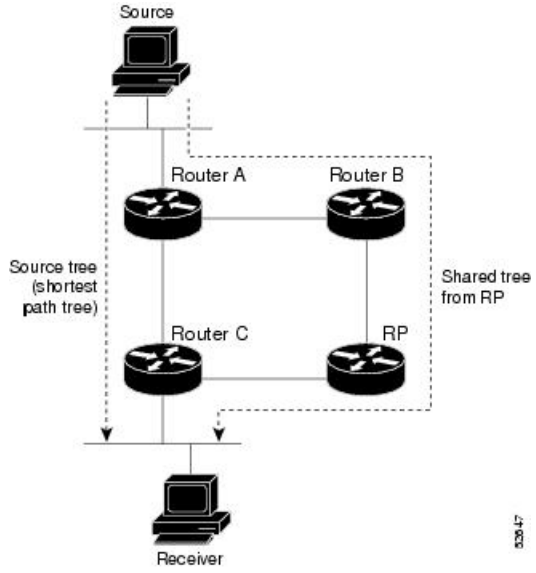
通常、スパース モードの PIM（PIM-SM）動作は、マルチキャスト ネットワークで比較的少数のルータがマルチキャストに関連する場合に使用されます。ルータは、トラフィックの明示的な要求がない場合、グループのマルチキャスト パケットを転送しません。要求は、ツリーのルート ノードに向けてホップバイホップで送信される PIM join メッセージを使用して行われます。PIM-SM のツリーのルート ノードは、共有ツリーの場合はランデブー ポイント（RP）、最短パス ツリー（SPT）の場合はマルチキャスト送信元に直接接続されているファーストホップ ルータになります。RP はマルチキャスト グループを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

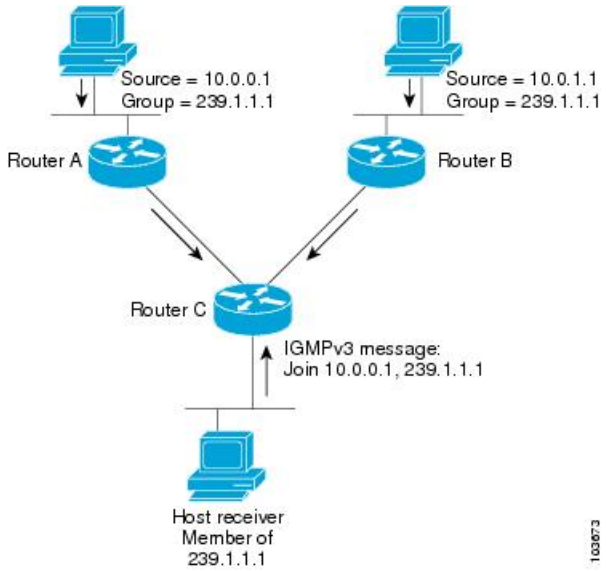
指定ルータは、PIM register メッセージ、PIM join メッセージ、および PIM prune メッセージを RP に送信し、ホスト グループ メンバーシップに関する情報を通知します。

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。

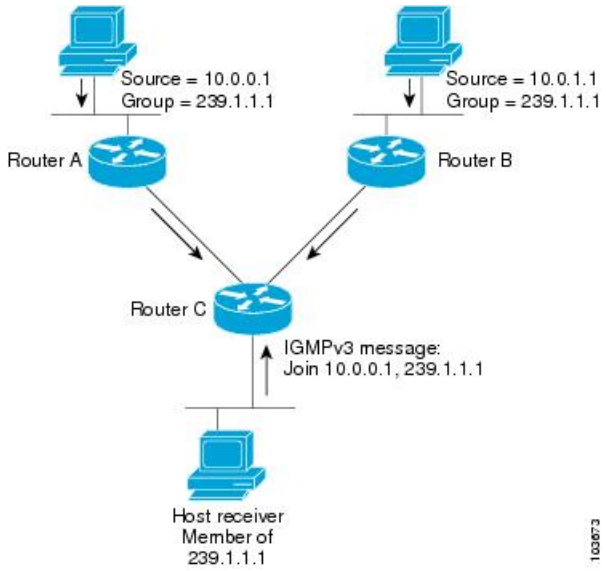
IGMP ルーティングの機能

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プルーニングし、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 ルート 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

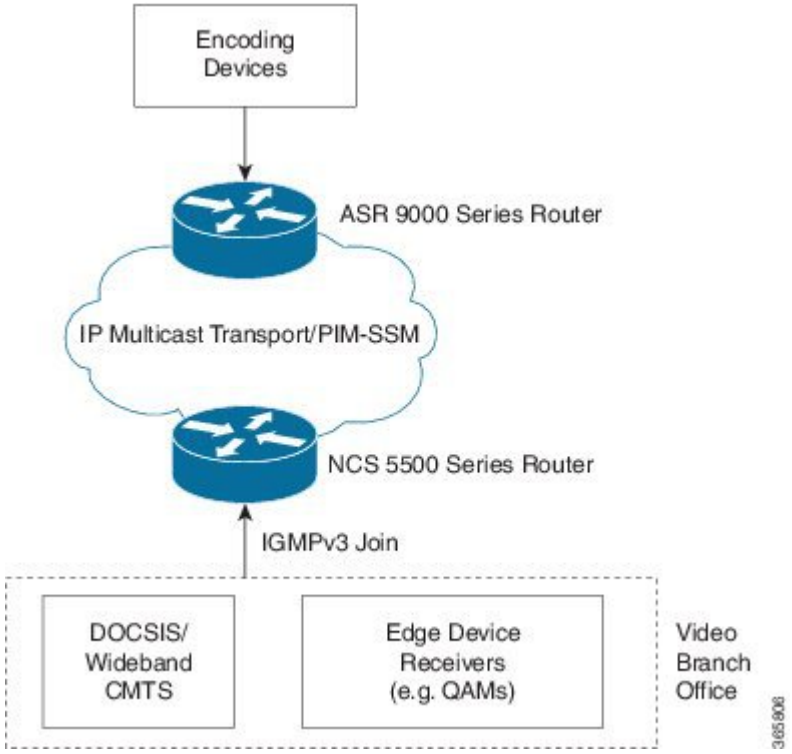
今日のブロードキャスト ビデオ ネットワークでは、独自のトランスポート システムを使用して、各ビデオ ブランチ オフィスにすべてのチャネル ラインナップを配信しています。IP ベースのトランスポート ネットワークは、他の IP ベースのサービスの配信と組み合わせたビデオ サービスを提供するためのコスト効率のよい/便利な代替手段となります。（インターネット配信またはビジネス サービス）

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



アクセス擬似回線を介したマルチキャスト

アクセス擬似回線（PW）を介したマルチキャストにより、CE で終端する MLDP コアおよび PW でのマルチキャストトラフィックのフラッディングが可能になります。したがって、2 つの IGMP ドメインを接続し、レイヤ 3（VRF またはグローバル）ドメインまたは PW を使用したレイヤ 2 ドメインで終端する MPLS ネットワーク経由で MVPN トラフィックを拡張します。

アクセス PW を介したマルチキャストにより、サービスプロバイダーがハードウェアを拡張しながらコストを削減できるようになります。

（注） この機能は、NCS 560 ルータではサポートされていません。

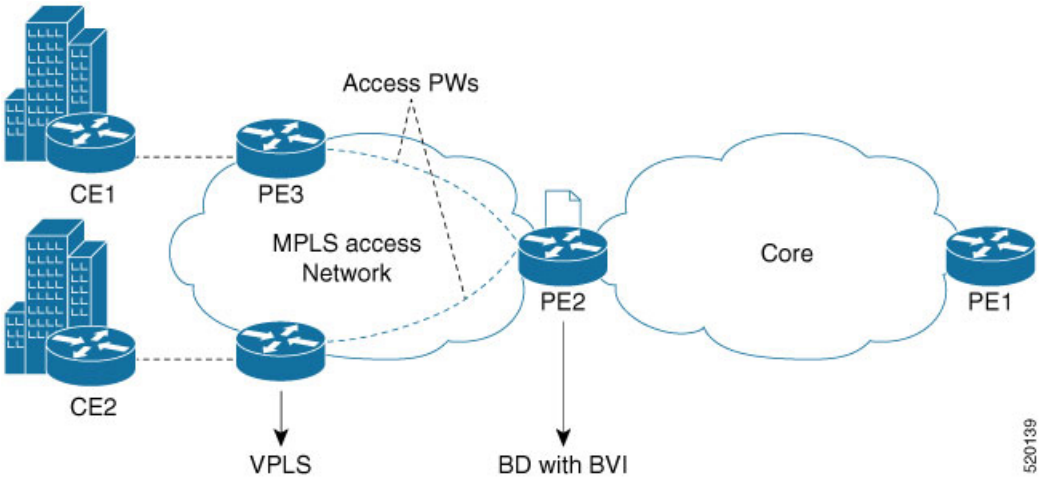
実装の注意事項

- アクセス PW を介した IGMP および MLD スヌーピングはサポートしていません
- フラッドモードのみをサポートしています
- SSM ルートのみをサポートしています
- アクセス PW を介した QoS（入力/出力）はサポートしていません

- アクセス PW のエンドポイントとして機能するデバイスの最大 MTU を設定します。これにより、プロトコルパケットを簡単に移動できます。

アクセス擬似回線を介したマルチキャストの設定

下の図のサンプルトポロジについて考えます。



上記のトポロジでは、次のようになります。

- CE は PE3（アクセスデバイス）に接続されています。PE3 にはアクセス PW が設定されています。PE3 は 192.127.0.1 でアクセスできます。
- PE2（NCS 5500 または NCS 540）には、BVI とアクセス PW が設定された VPLS があります。
- ポイントツーマルチポイント接続は、BD および BVI インターフェイスで擬似回線を介して PE2 と PE3 の間で確立されます。
- アクセス PW を介して CE から受信したマルチキャストパケットは、着信インターフェイスとして BVI で PE2 に送信されます。
- コアから受信したマルチキャストパケットは、PE3 に対しアクセス PW を介して複製され、CE に複製および転送されます。ここで、BVI は転送先インターフェイスとして機能します。

設定例を次に示します。

```
/* Enter global configuration mode */
Router# configure
Router(config)# l2vpn

/* Configure pseudowire class name */
Router(config-l2vpn)# pw-class mpls

/* Configure MPLS encapsulation for the pseudowire */
Router(config-l2vpn-pwc)# encapsulation mpls
Router(config-l2vpn-pwc-mpls)#control-word
```

```
Router(config-l2vpn-pwc-mpls)#transport-mode ethernet
Router(config-l2vpn-pwc-mpls)#load-balancing
Router(config-l2vpn-pwc-mpls-load-bal)#flow-label both
Router(config-l2vpn-pwc-mpls-load-bal)#exit
Router(config-l2vpn-pwc-mpls)#exit
Router(config-l2vpn-pwc)#exit

/* Configure bridge group and bridge domain, then assign network interfaces to the bridge
 domain. */
Router(config-l2vpn)#bridge group bvi-access-pw
Router(config-l2vpn-bg)#bridge-domain 1
Router(config-l2vpn-bg-bd)#interface tengigE 0/0/0/0.1
Router(config-l2vpn-bg-bd-ac)#exit

/* Configure the pseudowire port to the bridge domain and the peer to the bridge domain.
 */
Router(config-l2vpn-bg-bd)#neighbor 192.127.0.1 pw-id 1
Router(config-l2vpn-bg-bd-pw)#exit
Router(config-l2vpn-bg-bd)#routed interface bvi1
Router(config-l2vpn-bg-bd)# commit
```

ランニング コンフィギュレーション

このセクションでは、アクセスPWの実行コンフィギュレーションによるマルチキャストが表示されています。

```
l2vpn
pw-class mpls
  encapsulation mpls
   control-word
   transport-mode ethernet
   load-balancing
    flow-label both
   !
  !

bridge group BVI-ACCESS-PW
  bridge-domain 1
   interface TenGigE0/0/0/0.1
   !
   neighbor 192.127.0.1 pw-id 1
    pw-class mpls
   !
   routed interface BVI1
   !
```

確認

show l2vpn bridge-domain コマンドを使用して、PW のステータスを確認します。

```
RP/0/RP0/CPU0# show l2vpn bridge-domain bd-name 1 detail

Legend: pp = Partially Programmed.
Bridge group: BVI-ACCESS-PW, bridge-domain: 1, id: 1, state: up, ShgId: 0, MSTi: 0
  Coupled state: disabled
  VINE state: BVI Resolved
  MAC learning: enabled
  MAC withdraw: enabled
    MAC withdraw for Access PW: enabled
    MAC withdraw sent on: bridge port up
    MAC withdraw relaying (access to access): disabled
  Flooding:
    Broadcast & Multicast: enabled
```

```
    Unknown unicast: enabled
  MAC aging time: 300 s, Type: inactivity
  MAC limit: 64000, Action: none, Notification: syslog
  MAC limit reached: no, threshold: 75%
  MAC port down flush: enabled
  MAC Secure: disabled, Logging: disabled
  Split Horizon Group: none
  Dynamic ARP Inspection: disabled, Logging: disabled
  IP Source Guard: disabled, Logging: disabled
  DHCPv4 Snooping: disabled
  DHCPv4 Snooping profile: none
  IGMP Snooping: disabled
  IGMP Snooping profile: none
  MLD Snooping profile: none
  Storm Control: disabled
  Bridge MTU: 9086
  MIB cvplsConfigIndex: 2
  Filter MAC addresses:
  P2MP PW: disabled
  Multicast Source: IPv4
  Create time: 22/09/2019 15:00:09 (2w5d ago)
  No status change since creation
  ACs: 2 (2 up), VFIs: 0, PWs: 1 (1 up), PBBs: 0 (0 up), VNIs: 0 (0 up)
  List of ACs:
    AC: BVI1, state is up
      Type Routed-Interface
      MTU 1514; XC ID 0x800001f7; interworking none
      BVI MAC address:
        0032.1772.20dc
      Split Horizon Group: Access
      PD System Data: AF-LIF-IPv4: 0x00000000  AF-LIF-IPv6: 0x00000000
     AC: TenGigE0/0/0/0.1, state is up
      Type VLAN; Num Ranges: 1
      Rewrite Tags: []
      VLAN ranges: [1, 1]
      MTU 9086; XC ID 0x1; interworking none
      MAC learning: enabled
      Flooding:
        Broadcast & Multicast: enabled
        Unknown unicast: enabled
      MAC aging time: 300 s, Type: inactivity
      MAC limit: 64000, Action: none, Notification: syslog
      MAC limit reached: no, threshold: 75%
      MAC port down flush: enabled
      MAC Secure: disabled, Logging: disabled
      Split Horizon Group: none
      E-Tree: Root
      Dynamic ARP Inspection: disabled, Logging: disabled
      IP Source Guard: disabled, Logging: disabled
      DHCPv4 Snooping: disabled
      DHCPv4 Snooping profile: none
      IGMP Snooping: disabled
      IGMP Snooping profile: none
      MLD Snooping profile: none
      Storm Control: bridge-domain policer
      Static MAC addresses:
      Statistics:
        packets: received 221328661592 (multicast 0, broadcast 0, unknown unicast 0,
unicast 0), sent 4516080000
        bytes: received 24346154850336 (multicast 0, broadcast 0, unknown unicast 0,
unicast 0), sent 559962777746
        MAC move: 0
      Storm control drop counters:
        packets: broadcast 0, multicast 0, unknown unicast 0
```

```
      bytes: broadcast 0, multicast 0, unknown unicast 0
    Dynamic ARP inspection drop counters:
      packets: 0, bytes: 0
    IP source guard drop counters:
      packets: 0, bytes: 0
    PD System Data: AF-LIF-IPv4: 0x00013806  AF-LIF-IPv6: 0x00013807

List of Access PWs:
  PW: neighbor 192.127.0.1, PW ID 1, state is up ( established )
    PW class mpls, XC ID 0xc0000001 .
    Encapsulation MPLS, protocol LDP
    Source address 8.8.8.8
    PW type Ethernet, control word enabled, interworking none
    PW backup disable delay 0 sec
    Sequencing not set
    LSP : Up
    Flow Label flags configured (Tx=1,Rx=1), negotiated (Tx=0,Rx=0)

    PW Status TLV in use
      MPLS         Local                          Remote
      ------------ ------------------------------ ------------------------------
      Label        24007                          24000
      Group ID     0x1                            0x1
      Interface    Access PW                      1
      MTU          9086                           9086
      Control word enabled                        enabled
      PW type      Ethernet                       Ethernet
      VCCV CV type 0x2                            0x2
                   (LSP ping verification)        (LSP ping verification)
      VCCV CC type 0x7                            0x7
                   (control word)                 (control word)
                   (router alert label)           (router alert label)
                   (TTL expiry)                   (TTL expiry)
      ------------ ------------------------------ ------------------------------
    Incoming Status (PW Status TLV):
      Status code: 0x0 (Up) in Notification message
    MIB cpwVcIndex: 3221225473
    Create time: 22/09/2019 15:00:09 (2w5d ago)
    Last time status changed: 26/09/2019 11:17:06 (2w1d ago)
    MAC withdraw messages: sent 3, received 0
    Forward-class: 0
    Static MAC addresses:
    Statistics:
      packets: received 0 (unicast 0), sent 0
      bytes: received 0 (unicast 0), sent 0
      MAC move: 0
    Storm control drop counters:
      packets: broadcast 0, multicast 0, unknown unicast 0
      bytes: broadcast 0, multicast 0, unknown unicast 0
    MAC learning: enabled
    Flooding:
      Broadcast & Multicast: enabled
      Unknown unicast: enabled
    MAC aging time: 300 s, Type: inactivity
    MAC limit: 64000, Action: none, Notification: syslog
    MAC limit reached: no, threshold: 75%
    MAC port down flush: enabled
    MAC Secure: disabled, Logging: disabled
    Split Horizon Group: none
    E-Tree: Root
    DHCPv4 Snooping: disabled
    DHCPv4 Snooping profile: none
    IGMP Snooping: disabled
    IGMP Snooping profile: none
```

```
      MLD Snooping profile: none
      Storm Control: bridge-domain policer
  List of VFIs:
  List of Access VFIs:
```

show mrib vrf vrf1000 route コマンドを使用して BVI 発信インターフェイスのステータスを確認し、FGID を収集します。

```
RP/0/RP0/CPU0:# show mrib vrf vrf1000 route 232.1.1.1 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

(87.2.1.2,232.1.1.1) Ver: 0xa5b9 RPF nbr: 87.2.1.2 Flags: RPF, FGID: 24312, Statistics
enabled: 0x3
  Up: 00:13:05
  Incoming Interface List
    TenGigE0/0/0/0.2 Flags: A, Up: 00:13:05
  Outgoing Interface List
    BVI1 Flags: F NS LI, Up: 00:13:05
```

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

エッジルータでのマルチキャスト MLDP プロファイル 14 のサポート

ルータがエッジルータとして設定されている場合、MLDP プロファイル 14 がサポートされます。

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。ルータがエッジルータとして設定されている場合、IPTV コンテンツを配信するために、MLDP プロファイル 14（パーティション MDT）がサポートされます。

このプロファイル 14 の特性は次のとおりです。

- BGP C マルチキャストルーティングを使用した、P2MP mLDP コアツリーのフルメッシュ（デフォルト MDT として）。
- デフォルト MDT がサポートされています。
- 顧客のトラフィックは SSM です。
- Inter-AS オプション A、B、および C がサポートされています。
- すべての PE に一意の BGP ルート識別子（RD）値が必要です。

エッジルータでの mLDP プロファイル 14 の設定例

```
vrf one
 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
   mdt c-multicast-routing bgp
   !
   interface GigabitEthernet0/1/0/0
    enable
   !
  !
 !
!

route-policy rpf-for-one
  set core-tree mldp-partitioned-p2mp
end-policy
!

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

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

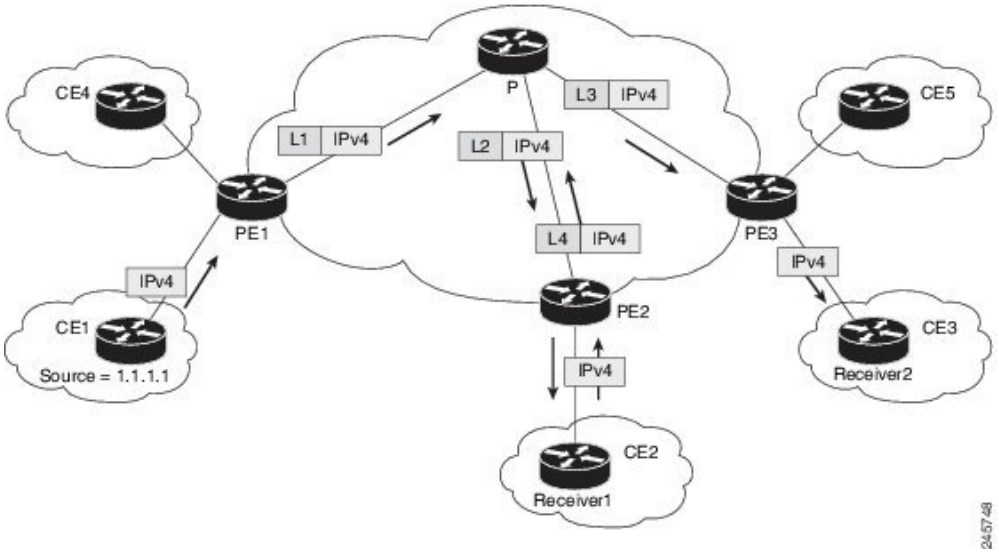
LSM には、コア内のカスタマー トラフィックを転送するために現在使用されている GRE コア トンネルと比較した場合、次の利点があります。

- 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。MLDP MVPN 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 7）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
```

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
```

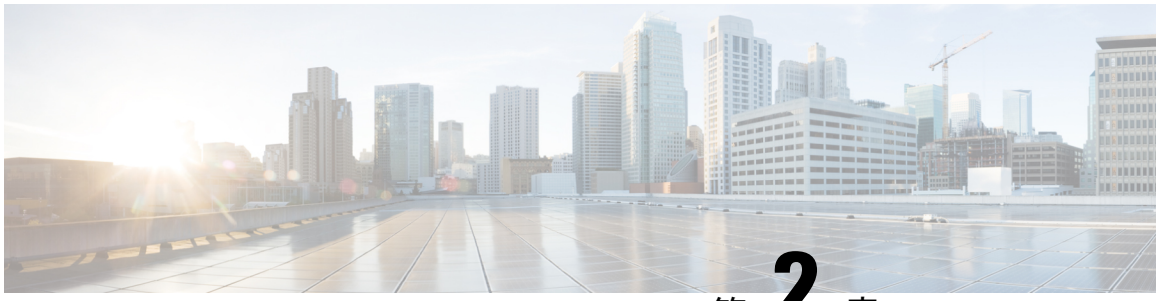
ラベル情報ベース（LIB）の内容を表示するには、**show mpls mldp bindings** コマンドを使用します。

```
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 [vpnv6 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
```



第 2 章

IGMP スヌーピングを使用したレイヤ 2 マルチキャストの実装

インターネット グループ管理プロトコル（IGMP）スヌーピングは、少なくとも 1 つの関与する受信先を持つセグメントに対してのみにレイヤ 2 でマルチキャスト フローを制限します。このモジュールでは、IGMP スヌーピングの実装方法について説明します。

IGMP スヌーピングの前提条件

IGMP スヌーピングを実装する前に、次の前提条件を満たす必要があります。

- ネットワークは、レイヤ 2 VPN（L2VPN）で設定する必要があります。
- 適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。このコマンド リファレンスには、各コマンドに必要なタスク ID が含まれます。ユーザ グループの割り当てが原因でコマンドを使用できないと考えられる場合、AAA 管理者に連絡してください。

IGMP スヌーピングの制約事項

- IGMP スヌーピングは、L2VPN ブリッジ ドメインだけでサポートされます。

- IPv4 マルチキャストは、BVI インターフェイスの背後にあるマルチキャスト送信元でサポートされています。たとえば、次の設定は、IPv4 マルチキャストの BVI の背後にある送信元を設定する方法を示しています。

```
l2vpn
bridge group 1
  bridge-domain 1
   multicast-source ipv4
   igmp snooping profile grp1
   !
   interface TenGigE0/0/0/3.32
   !
   routed interface BVI1
```

- 明示的ホスト トラッキング（IGMPv3 スヌーピング機能）はサポートされません。
- IGMPv1 はサポートされていません。

IGMP スヌーピングの情報

IGMP スヌーピングの概要

基本機能の説明

IGMP スヌーピングは、レイヤ 2 でマルチキャスト トラフィックを抑制する方法を提供します。IGMP スヌーピング アプリケーションは、ブリッジ ドメインのホストによって送信された IGMP メンバーシップ レポートをスヌーピングすることで、レイヤ 2 マルチキャスト転送テーブルを設定して、少なくとも 1 つの関係メンバーを持つポートだけにトラフィックを送信できます。これにより、マルチキャスト トラフィックの量が大幅に削減されます。

IGMP は、レイヤ 3 で設定され、IPv4 マルチキャスト ネットワーク内のホストが、関与するマルチキャスト トラフィックを通知する手段、ルータがレイヤ 3のネットワーク内のマルチキャスト トラフィックのフローを制御および制限する手段を提供します。

IGMP スヌーピングは、IGMP メンバーシップ レポート メッセージの情報を使用して、対応する情報を転送テーブルに構築し、レイヤ 2 の IP マルチキャスト トラフィックを制限します。転送テーブルのエントリは <ルート, OIF リスト> という形式で、

- ルートは <*, G> ルートまたは <S, G> ルートです。
- OIF リストは、指定されたルートに関する IGMP メンバーシップ レポートを送信したすべてのブリッジ ポートで構成されます。

マルチキャスト ネットワークに実装された IGMP スヌーピングには、次の属性があります。

- 基本的には、IGMP スヌーピングはブリッジ ドメイン全体をフラッディングする可能性があるマルチキャスト トラフィックを削減することにより、帯域幅使用量を減らします。

- 一部のオプションの設定を使用して、1 つのブリッジ ポートのホストから受信した IGMP レポートをフィルタリングし、他のブリッジポートのホストへの漏洩を防止することで、ブリッジ ドメイン間のセキュリティを提供します。

ハイ アベイラビリティ機能

すべてのハイ アベイラビリティ機能は、IGMP スヌーピングを有効にする以上の追加設定を行わずに、IGMP スヌーピング プロセスに適用されます。次のハイ アベイラビリティ機能がサポートされています。

- プロセスの再起動
- RP フェールオーバー
- ステートフル スイッチオーバー（SSO）
- ノンストップ フォワーディング（NSF）：プロセスの再起動またはルート プロセッサ（RP）のフェールオーバー後にコントロールプレーンが復元されている間、フォワーディングは影響を受けません。
- ラインカードの活性挿抜（OIR）

ブリッジ ドメインのサポート

IGMP スヌーピングは、ブリッジ ドメイン レベルで動作します。IGMP スヌーピングがブリッジ ドメインでイネーブルの場合、スヌーピング機能は、ブリッジ ドメインに属する次のポートを含むすべてのポートに適用されます。

- ブリッジ ドメインの物理ポート。
- イーサネット フロー ポイント（EFP）：EFP には VLANを指定できます。
- イーサネット バンドル：イーサネット バンドルには、IEEE 802.3ad リンク バンドルおよび Cisco EtherChannel バンドルが含まれます。IGMP スヌーピング アプリケーションの観点では、イーサネット バンドルは単なる EFP の 1 つです。 の転送アプリケーションは、バンドルから単一のポートをランダムに指定して、マルチキャスト トラフィックを伝送します。

マルチキャスト ホスト ポート

IGMP スヌーピングは、各ポート（EFP、物理ポート、または EFP バンドルなど）をホスト ポートとして分類します。つまり、mrouter ポートではないすべてのポートはホスト ポートです。

IGMPスヌーピングをイネーブルにしたブリッジドメイン内のマルチキャストトラフィック処理

次の表では、IGMP スヌーピングおよびホスト ポートによるトラフィック処理の動作について説明します。Table 1: IGMPv2 クエリアのマルチキャスト トラフィック処理, on page 48 では

IGMPv2 クエリのトラフィック処理について説明します。Table 2: IGMPv3 クエリアのマルチキャスト トラフィック処理, on page 48 は IGMPv3 クエリに適用されます。

デフォルトでは、IGMP スヌーピングは IGMPv2 および IGMPv3 をサポートしています。ブリッジ ドメインで検出された IGMP クエリのバージョンによって、スヌーピング プロセスの動作のバージョンが決まります。IGMPv3 の最小バージョンをサポートするように IGMP スヌーピングを設定してデフォルトを変更すると、IGMP スヌーピングは IGMPv2 クエリを無視します。

***Table 1: IGMPv2* クエリアのマルチキャスト トラフィック処理**

トラフィック タイプ	ホスト ポートで受信した場合
IP マルチキャストの送信元トラフィック	すべての mrouter ポートと、関与を示しているホスト ポートに転送します。
IGMP の一般クエリー	—
IGMP グループに固有なクエリー	切断
IGMPv2 の join	レポートを検査（スヌーピング）します。 • レポート抑制がイネーブルの場合、新しいグループに対する最初の join か、既存のグループに対する一般クエリーに続く最初の join を転送します。 • レポート抑制がディセーブルの場合、すべての mrouter ポートに転送します。
IGMPv3 の report	無視
IGMPv2 の leave	最後のメンバ クエリー処理を呼び出します。

***Table 2: IGMPv3* クエリアのマルチキャスト トラフィック処理**

トラフィック タイプ	ホスト ポートで受信した場合
IP マルチキャストの送信元トラフィック	すべての mrouter ポートと、関与を示しているホスト ポートに転送します。
IGMP の一般クエリー	—
IGMP グループに固有なクエリー	—
IGMPv2 の join	IGMPv3 IS_EX{} レポートとして処理します。
IGMPv3 の report	• プロキシ レポート機能がイネーブルの場合：状態または送信元リストが変更されると、すべての mrouter ポートで状態変更レポートを生成します。 • プロキシ レポート機能がディセーブルの場合：すべての mrouter ポートに転送します。

トラフィック タイプ	ホスト ポートで受信した場合
IGMPv2 の leave	IGMPv3 IS_IN{} レポートとして処理します。

IGMP スヌーピング設定プロファイルに関する情報

ブリッジ ドメインで IGMP スヌーピングをイネーブルにするには、ブリッジ ドメインにプロファイルを対応付ける必要があります。最小設定は、空のプロファイルです。プロファイルが空の場合、IGMP スヌーピングのデフォルト設定, on page 51に記載されている IGMP スヌーピングのデフォルト設定オプションおよび設定値がイネーブルになります。

ブリッジ ドメインまたはブリッジ ドメインに属するポートに、IGMP スヌーピング プロファイルを適用できます。次のガイドラインでは、ポートおよびブリッジ ドメインに適用されるプロファイル間の関係について説明します。

- ブリッジ ドメインに適用されている任意の IGMP プロファイル（空のプロファイルを含む）によって、IGMP スヌーピングがイネーブルになります。IGMP スヌーピングをディセーブルにするには、ブリッジ ドメインからプロファイルの適用を解除します。
- プロファイルが空の場合、デフォルト設定を使用して、ブリッジ ドメインおよびブリッジに属するすべてのポートに IGMP スヌーピングが設定されます。
- ブリッジ ドメインに（ブリッジ ドメイン レベルで）適用できる IGMP スヌーピング プロファイルは常に 1 つだけです。プロファイルはブリッジに属するポートに適用でき、ポートあたり 1 つのプロファイルが適用できます。
- ポート プロファイルは、ブリッジ ドメインにプロファイルが適用されていない場合は有効になりません。
- ポート固有の設定を有効にするには、ブリッジ ドメインで IGMP スヌーピングがイネーブルになっている必要があります。
- ブリッジ ドメインに適用されたプロファイルにポート固有の設定オプションが含まれている場合は、別のポート固有プロファイルがポートに適用されていない限り、値はそのブリッジに属する mrouter ポートおよびホスト ポートを含むすべてのポートに適用されます。
- ポートにプロファイルが対応付けられていると、IGMP スヌーピングは、ブリッジ レベルのプロファイルに存在するポート設定に関係なく、そのポートを再設定します。

プロファイルの作成

プロファイルを作成するには、グローバル コンフィギュレーション モードで **igmp snooping profile** コマンドを使用します。

プロファイルの適用と解除

ブリッジ ドメインにプロファイルを適用するには、l2vpn ブリッジ グループ ブリッジ ドメイン コンフィギュレーション モードで **igmp snooping profile** コマンドを使用します。ポートにプロファイルを適用するには、ブリッジドメインに属するインターフェイス コンフィギュレーション モードで **igmp snooping profile** コマンドを使用します。プロファイルの適用を解除するには、適切なコンフィギュレーション モードでこのコマンドの **no** 形式を使用します。

ブリッジドメインまたはポートとプロファイルの対応付けを解除しても、プロファイルはそのまま存在し、後で使用できます。プロファイルの対応付けを解除すると、次の処理が行われます。

- ブリッジ ドメインとプロファイルの対応付けを解除すると、ブリッジ ドメインで IGMP スヌーピングが非アクティブになります。
- ポートとプロファイルの対応付けを解除すると、そのポートの IGMP スヌーピング設定値は、ブリッジ ドメイン プロファイルからインスタンス化されます。

プロファイルの変更

アクティブなプロファイルは変更を加えることはできません。アクティブなプロファイルとは、現在対応付けられているプロファイルです。

アクティブなプロファイルを変更する必要がある場合は、すべてのブリッジまたはポートとの対応付けを解除して、変更し、もう一度対応付ける必要があります。

アクティブなプロファイルを変更するもう 1 つの方法は、必要な変更を含む新しいプロファイルを作成し、ブリッジまたはポートに適用することで既存のプロファイルを置き換える方法です。これにより、IGMP スヌーピングは無効になり、新しいプロファイルのパラメータを使用して再びアクティブになります。

IGMP スヌーピングのデフォルト設定

Table 3: IGMP スヌーピングのデフォルト設定値

スコープ	機能	デフォルト値
ブリッジ ドメイン	IGMP snooping	イネーブル化する IGMP プロファイルはブリッジ ドメインに適用されるまで、ブリッジ ドメインではディセーブルです。
	internal querier	未設定
	last-member-query-count	2
	last-member-query-interval	1000 ミリ秒
	minimum-version	2（IGMPv2 と IGMPv3 をサポート）
	querier query-interval	60（秒） **Note** これは、非標準デフォルト値です。
	report-suppression	イネーブル（IGMPv2 のレポート抑制機能と、IGMPv3 のプロキシ レポート機能をイネーブルにします）
	querier robustness-variable	2
	router alert check	イネーブル
	tcn query solicit	ディセーブル
	tcn flood	イネーブル
	ttl-check	イネーブル
	unsolicited-report-timer	1000 ミリ秒
ポート	immediate-leave	ディセーブル
	mrouter	スタティック mrouter は設定されていません。デフォルトで動的な検出が実行されます。
	router guard	ディセーブル
	static group	未設定

ブリッジ ドメイン レベルでの IGMP スヌーピング設定

IGMP の最小バージョン

minimum-version コマンドは、ブリッジ ドメインの IGMP スヌーピングでサポートされる IGMP バージョンを決定します。

- minimum-version が 2 の場合、IGMP スヌーピングは IGMPv2 および IGMPv3 メッセージを受信します。これはデフォルト値です。
- minimum-version が 3 の場合、IGMP スヌーピングは IGMPv3 メッセージだけを受信し、IGMPv2 メッセージをすべてドロップします。

IGMPv1 はサポートされていません。このコマンドのスコープは、ブリッジ ドメインです。コマンドは、ポートに適用されているプロファイルでは無視されます。

グループ メンバーシップ インターバル、ロバストネス変数、およびクエリー間隔

グループ メンバーシップ インターバル（GMI）は、IGMP スヌーピングが古いグループ メンバーシップ状態を失効させるタイミングを制御します。**show igmp snooping group** コマンドは、次のクエリ インターバルの後に古い状態が消去されるまで、有効期間 0 のグループを表示します。

GMI は次のように計算されます。

GMI = (robustness-variable * query-interval) + maximum-response-time

値は次のとおりです。

- maximum-response-time（MRT）は時間を表します。受信先はこの時間中にメンバーシップ状態を報告する必要があります。
- robustness-variable は、GMI の計算に影響を与える整数です。
- query-interval は一般クエリーの送信間隔を表します。

GMI のコンポーネントの値は、次のように取得されます。

- MRT は IGMPv2 および IGMPv3 両方の一般クエリーでアドバタイズされます。
- クエリアが IGMPv2 を実行している場合、IGMP スヌーピングは、robustness-variable と query-interval に IGMP スヌーピングで設定された値を使用します。これらのパラメータ値は、クエリアに設定された値と一致している必要があります。ほとんどの場合、他のシスコ ルータと対話する場合、これらの値を明示的に設定する必要はありません。通常、IGMP スヌーピングのデフォルト値は、クエリアのデフォルト値と一致しています。一致していない場合は、**querier robustness-variable** および **querier query-interval** コマンドを使用して、一致する値を設定する必要があります。
- IGMPv3 の一般クエリーは、robustness-variable と query-interval の値（それぞれ QRV と QQI）を伝えます。IGMP スヌーピングは、クエリーからの値を使用して、IGMP スヌーピングの GMI をクエリアの GMI と一致させます。

統合ルーティング ブリッジング アクティブ/アクティブ マルチホーム上のマルチキャスト

統合ルーティング ブリッジングのアクティブ/アクティブ マルチホーム機能を介したマルチキャストにより、ルータは、障害が発生しても、トラフィックを損失することなく、ルータ間のトラフィックを迅速かつ安全に切り替えることができます。この機能は、ソリューションとして連携する次の 4 つのサブ機能で構成されています。

- 最初に、ピア ルータに対して IGMPv2 スヌーピングが有効になり、どのレイヤ 2 インターフェイスの受信者が特定グループに関与しているかが分かります。
- スヌーピングの後、この情報は、レイヤ 2 EVPN 同期機能を使用してピアルータに同期されます。
- 両方のピア ルータが同期されると、最後のホップ ルータのように動作し、PIM join アップストリームを送信します。
- トラフィックが両方のピア ルータに到着すると、1 つのピア ルータだけが、指定されたフォワーダ選択機能を使用してトラフィックを受信者に転送します。

IGMP スヌーピングを設定する方法

最初の 2 つの作業は、基本的な IGMP スヌーピングの設定に必須です。

IGMP スヌーピング プロファイルの作成

Procedure

	Command or Action	Purpose
ステップ 1	**configure**	
ステップ 2	**igmp snooping profile** *profile-name* **Example:** `RP/0/RP0/cpu 0: router(config)# igmp snooping profile default-bd-profile`	IGMP スヌーピング プロファイル コンフィギュレーション モードを開始し、名前付きプロファイルを作成します。 デフォルト プロファイルは、IGMP スヌーピングをイネーブルにします。追加の設定をせずに新しいプロファイルをコミットするか、プロファイルに追加の設定オプションを含めることができます。後でプロファイルに戻って、このモジュールの他の作業で記載されている手

	Command or Action	Purpose
		順に従って、設定を追加することもできます。
ステップ 3	オプションで、デフォルト設定値を上書きするコマンドを追加します。	ブリッジ ドメイン プロファイルを作成する場合は、次の点を考慮します。 • 空のプロファイルは、ブリッジ ドメインへの適用に適しています。空のプロファイルは、デフォルト設定値でIGMP スヌーピングをイネーブルにします。 • オプションで、デフォルト設定値を上書きするコマンドをプロファイルに追加できます。 • ブリッジ ドメイン プロファイルにポート固有の設定を含める場合、別のプロファイルがポートに適用されていない限り、設定はそのブリッジに属するすべてのポートに適用されます。 ポート固有のプロファイルを作成する場合は、次の点を考慮します。 • 空のプロファイルはポートに適用できますが、ポートの設定には影響を与えません。 • ポートにプロファイルを適用する際、IGMP スヌーピングはブリッジ ドメイン プロファイルからの設定値の継承を上書きして、ポートを再設定します。これらの設定を保持する場合は、ポート プロファイルのコマンドを繰り返し実行する必要があります。 後でプロファイルにコマンドを追加するには、プロファイルの適用を解除し、プロファイルを変更してから再適用します。
ステップ 4	**commit**	

次の作業

プロファイルをブリッジ ドメインまたはポートに適用し、プロファイルを有効にする必要があります。次のいずれかの作業を参照してください。

プロファイルの適用およびブリッジ ドメインでの IGMP スヌーピングのアクティブ化

ブリッジ ドメインで IGMP スヌーピングをアクティブにするには、次の手順の説明に従って、ブリッジ ドメインに IGMP スヌーピング プロファイルを適用します。

Procedure

	Command or Action	Purpose
ステップ 1	**configure**	
ステップ 2	**l2vpn** **Example:** `RP/0/RP0/cpu 0: router(config)# l2vpn`	レイヤ 2 VPN 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	**bridge group** *bridge-group-name* **Example:** `RP/0/RP0/cpu 0: router(config-l2vpn)# bridge group GRP1`	名前付きブリッジ グループのレイヤ 2 VPNブリッジ グループ コンフィギュレーション モードを開始します。
ステップ 4	**bridge-domain** *bridge-domain-name* **Example:** `RP/0/RP0/cpu 0: router(config-l2vpn-bg)# bridge-domain ISP1`	名前付きブリッジ ドメインのレイヤ 2 VPNブリッジグループブリッジドメイン コンフィギュレーション モードを開始します。
ステップ 5	**igmp snooping profile** *profile-name* **Example:** `RP/0/RP0/cpu 0: router(config-l2vpn-bg-bd)# igmp snooping profile default-bd-profile`	ブリッジ ドメインに名前付き IGMP スヌーピング プロファイルを適用し、ブリッジ ドメインで IGMP スヌーピングをイネーブルにします。
ステップ 6	**commit**	
ステップ 7	**show igmp snooping bridge-domain detail** **Example:**	（任意）IGMP スヌーピングがブリッジ ドメインでイネーブルであることを確認し、ブリッジ ドメインおよびポートに

	Command or Action	Purpose
	`RP/0/RP0/cpu 0: router# show igmp snooping bridge-domain detail`	適用されるIGMPスヌーピングプロファイルの名前を表示します。
ステップ 8	**show l2vpn bridge-domain detail** **Example:** `RP/0/RP0/cpu 0: router# show l2vpn bridge-domain`	（任意）IGMPスヌーピングがブリッジドメインのフォワーディング プレーン（レイヤ2）に実装されていることを確認します。

プロファイルの適用解除とブリッジ ドメインでの IGMP スヌーピングの非アクティブ化

ブリッジドメインでIGMPスヌーピングを非アクティブ化するには、次の手順を使用して、ブリッジ ドメインからプロファイルを削除します。

Note ブリッジ ドメインに一度に適用できるプロファイルは 1 つだけです。

Procedure

	Command or Action	Purpose
ステップ 1	**configure**	
ステップ 2	**l2vpn** **Example:** `RP/0/RP0/cpu 0: router(config)# l2vpn`	レイヤ 2 VPN 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	**bridge group** *bridge-group-name* **Example:** `RP/0/RP0/cpu 0: router(config-l2vpn)# bridge group GRP1`	名前付きブリッジ グループのレイヤ 2 VPNブリッジ グループ コンフィギュレーション モードを開始します。
ステップ 4	**bridge-domain** *bridge-domain-name* **Example:** `RP/0/RP0/cpu 0: router(config-l2vpn-bg)# bridge-domain ISP1`	名前付きブリッジ ドメインのレイヤ 2 VPNブリッジグループブリッジドメイン コンフィギュレーション モードを開始します。

	Command or Action	Purpose
ステップ 5	**no igmp snooping** **Example:** `RP/0/RP0/cpu 0: router(config-l2vpn-bg-bd)# no igmp snooping`	ブリッジ ドメインから IGMP スヌーピング プロファイルの適用を解除し、ブリッジ ドメインで IGMP スヌーピングをディセーブルにします。 **Note** 同時にブリッジ ドメインに適用できるプロファイルは 1 つだけです。プロファイルが適用されている場合、IGMP スヌーピングはイネーブルです。プロファイルが適用されていない場合、IGMP スヌーピングはディセーブルです。
ステップ 6	**commit**	
ステップ 7	**show igmp snooping bridge-domain detail** **Example:** `RP/0/RP0/cpu 0: router# show igmp snooping bridge-domain detail`	（任意）IGMP スヌーピングがブリッジ ドメインでディセーブルであることを確認します。
ステップ 8	**show l2vpn bridge-domain detail** **Example:** `RP/0/RP0/cpu 0: router# show l2vpn bridge-domain`	（任意）IGMP スヌーピングがブリッジ ドメインのフォワーディング プレーン（レイヤ 2）でディセーブルであることを確認します。

ブリッジに属するポートへのプロファイルの適用と解除

Before you begin

ポート固有のプロファイルが IGMP スヌーピングの動作に影響を与えるようにするには、ブリッジ ドメインで IGMP スヌーピングがイネーブルになっている必要があります。

Procedure

	Command or Action	Purpose
ステップ 1	**configure**	
ステップ 2	**l2vpn** **Example:** `RP/0/RP0/cpu 0: router(config)# l2vpn`	レイヤ 2 VPN コンフィギュレーション モードを開始します。

	Command or Action	Purpose
ステップ 3	**bridge group** *bridge-group-name* **Example:** `RP/0/RP0/cpu 0: router(config-l2vpn)# bridge group GRP1`	名前付きブリッジ グループのレイヤ 2 VPN ブリッジ グループ コンフィギュレーション モードを開始します。
ステップ 4	**bridge-domain** *bridge-domain-name* **Example:** `RP/0/RP0/cpu 0: router(config-l2vpn-bg)# bridge-domain ISP1`	名前付きブリッジ ドメインのレイヤ 2 VPN ブリッジ グループ ブリッジ ドメイン コンフィギュレーション モードを開始します。
ステップ 5	**interface** *interface-type interface-number* **Example:** `RP/0/RP0/cpu 0: router(config-l2vpn-bg-bd)# interface gig 1/1/1/1`	名前付きインターフェイスまたは PW のレイヤ 2 VPN ブリッジ グループ ブリッジ ドメイン インターフェイス コンフィギュレーション モードを開始します。
ステップ 6	次のいずれかを実行します。 • **igmp snooping profile** *profile-name* • **no igmp snooping** **Example:** `RP/0/RP0/cpu 0: router(config-l2vpn-bg-bd-if)# igmp snooping profile mrouter-port-profile`	名前付き IGMP スヌーピング プロファイルをポートに適用します。 **Note** ポートのプロファイルは、ブリッジに他のプロファイルが適用されていない限り、無効です。 コマンドの **no** 形式を使用して、ポートからプロファイルの適用を解除します。ポートに適用できるプロファイルは 1 つだけです。
ステップ 7	**routed interface BVI** *BVI 番号* **Example:** `RP/0/(config-l2vpn-bg-bd-if)# routed interface bvi 2`	BVI をブリッジ ドメインに接続します。 *BVI 番号*には任意の番号を指定できます。
ステップ 8	**commit**	
ステップ 9	**show igmp snooping bridge-domain detail** **Example:** `RP/0/RP0/cpu 0: router# show igmp`	（任意）IGMP スヌーピングがブリッジドメインでイネーブルであることを確認し、ブリッジドメインおよびポー

	Command or Action	Purpose
	`snooping bridge-domain detail`	トに適用される IGMP スヌーピング プロファイルの名前を表示します。
ステップ 10	**show l2vpn bridge-domain detail** **Example:** `RP/0/RP0/cpu 0: router# show l2vpn bridge-domain`	（任意）IGMP スヌーピングがブリッジ ドメインのフォワーディング プレーン（レイヤ 2）に実装されていることを確認します。

マルチキャスト転送の確認

Procedure

	Command or Action	Purpose
ステップ 1	**configure**	
ステップ 2	**show l2vpn forwarding bridge-domain** [*bridge-group-name*:*bridge-domain-name*] **mroute ipv4** [**detail**] [**hardware** {**ingress** | **egress**}] **location** *node-id* **Example:** `RP/0/RP0/cpu 0: router# show l2vpn forwarding bridge-domain bridgeGroup1:ABC mroute ipv4 detail location 0/3/CPU0`	フォワーディング プレーンの転送テーブルに変換されるマルチキャスト ルートを表示します。特定のブリッジ グループまたはブリッジ ドメインに表示を制限するには、任意の引数を使用します。 これらのルートが期待したルートではない場合は、コントロール プレーンの設定を確認し、対応する IGMP スヌーピング プロファイルを訂正してください。
ステップ 3	**show l2vpn forwarding bridge-domain** [*bridge-group-name*:*bridge-domain-name*] **mroute ipv4 summary location** *node-id* **Example:** `RP/0/RP0/cpu 0: router# show l2vpn forwarding bridge-domain bridgeGroup1:ABC mroute ipv4 summary location 0/3/CPU0`	フォワーディング プレーンの転送テーブルに保存されているマルチキャスト ルートの要約レベルの情報を表示します。特定のブリッジ ドメインに表示を制限するには、任意の引数を使用します。

IGMP スヌーピングの設定例

次に、のレイヤ2ブリッジ ドメインでIGMP スヌーピングをイネーブルにする例を示します。

ブリッジに属する物理インターフェイスでの IGMP スヌーピングの設定：例

1. 2 つのプロファイルを作成します。

```
igmp snooping profile bridge_profile
!
igmp snooping profile port_profile

!
```

2. L2 転送用の 2 つの物理インターフェイスを設定します。

```
interface GigabitEthernet0/8/0/38
   negotiation auto
   l2transport
   no shut
   !
!
interface GigabitEthernet0/8/0/39
   negotiation auto
   l2transport
   no shut
   !
!
```

3. ブリッジ ドメインにインターフェイスを追加します。ブリッジ ドメインに bridge_profile を適用し、イーサネット インターフェイスのいずれかに port_profile を適用します。2 番目のイーサネット インターフェイスは、ブリッジ ドメイン プロファイルから IGMP スヌーピング設定属性を継承します。

```
l2vpn
  bridge group bg1
     bridge-domain bd1
     igmp snooping profile bridge_profile
     interface GigabitEthernet0/8/0/38
       igmp snooping profile port_profile
     interface GigabitEthernet0/8/0/39

!
  !
!
```

4. 設定されたブリッジ ポートを確認します。

```
show igmp snooping port
```

ブリッジに属する VLAN インターフェイスでの IGMP スヌーピングの設定：例

1. 2 つのプロファイルを設定します。

```
igmp snooping profile bridge_profile
igmp snooping profile port_profile

!
```

2. L2 転送用の VLAN インターフェイスを設定します。

```
interface GigabitEthernet0/8/0/8
   negotiation auto
   no shut
   !
!
interface GigabitEthernet0/8/0/8.1 l2transport
   encapsulation dot1q 1001
   mtu 1514
   !
!
interface GigabitEthernet0/8/0/8.2 l2transport
   encapsulation dot1q 1002
   mtu 1514
   !
!
```

3. プロファイルを適用し、ブリッジ ドメインにインターフェイスを追加します。インターフェイスのいずれかにプロファイルを適用します。他のインターフェイスは、ブリッジ ドメイン プロファイルから IGMP スヌーピング設定属性を継承します。

```
l2vpn
  bridge group bg1
     bridge-domain bd1
     igmp snooping profile bridge_profile
     interface GigabitEthernet0/8/0/8.1
       igmp snooping profile port_profile
     interface GigabitEthernet0/8/0/8.2

     !
  !
!
```

4. 設定されたブリッジ ポートを確認します。

```
show igmp snooping port
```

ブリッジに属するイーサネット バンドルでの IGMP スヌーピングの設定：例

1. この例では、バンドルのフロントエンドが事前に設定されていることを前提にしています。たとえば、バンドル設定が次の 3 つのスイッチインターフェイスから構成されているとします。

```
    interface Port-channel1
    !
interface GigabitEthernet0/0/0/0
    !
interface GigabitEthernet0/0/0/1
!
    interface GigabitEthernet0/0/0/2
       channel-group 1 mode on
    !
    interface GigabitEthernet0/0/0/3
       channel-group 1 mode on
    !
```

2. 2 つの IGMP スヌーピング プロファイルを設定します。

```
       igmp snooping profile bridge_profile
       !
       igmp snooping profile port_profile

       !
```

3. バンドルのメンバ リンクとしてインターフェイスを設定します。

```
       interface GigabitEthernet0/0/0/0
         bundle id 1 mode on
         negotiation auto
       !
       interface GigabitEthernet0/0/0/1
         bundle id 1 mode on
         negotiation auto
       !
       interface GigabitEthernet0/0/0/2
         bundle id 2 mode on
         negotiation auto
       !
       interface GigabitEthernet0/0/0/3
         bundle id 2 mode on
         negotiation auto
       !
```

4. L2 転送用のバンドル インターフェイスを設定します。

```
interface Bundle-Ether 1
          l2transport
          !
       !
       interface Bundle-Ether 2
          l2transport
```

```
    !
  !
```

5. インターフェイスをブリッジ ドメインに追加し、IGMP スヌーピング プロファイルを適用し。

```
l2vpn
  bridge group bg1
     bridge-domain bd1
     igmp snooping profile bridge_profile
     interface bundle-Ether 1
       igmp snooping profile port_profile
     interface bundle-Ether 2

     !
  !
!
```

6. 設定されたブリッジ ポートを確認します。

```
show igmp snooping port
```

統合ルーティング ブリッジング アクティブ/アクティブ マルチホーム上のマルチキャストの設定

ピア 1 で実行される設定：

1. レイヤ 2 基本設定

```
hostname peer1
!
interface Bundle-Ether2
!
interface Bundle-Ether2.2 l2transport
 encapsulation dot1q 2
 rewrite ingress tag pop 1 symmetric
!
interface TenGigE0/0/0/0
 bundle id 2 mode on
 no shut
!
interface BVI2
 ipv4 address 100.2.0.1 255.255.255.0
 mac-address 1002.1111.2
!
```

2. EVPN 設定

```
hostname peer1
!
router bgp 100
 bgp router-id 1.1.1.1
 bgp graceful-restart
 address-family l2vpn evpn
 !
```

```
 neighbor 3.3.3.3
  remote-as 100
  update-source Loopback0
  address-family l2vpn evpn
  !
 !
!
evpn
 evi 2
  advertise-mac
  !
 !
 interface Bundle-Ether2
  ethernet-segment
   identifier type 0 02.02.02.02.02.02.02.02.02
   bgp route-target 0002.0002.0002
  !
 !
!
```

3. IGMPv2 スヌーピングの設定

```
hostname peer1
!
router igmp
 interface BVI2
  version 2
 !
!
l2vpn
 bridge group VLAN2
  bridge-domain VLAN2
   igmp snooping profile 1
   interface Bundle-Ether2.2
   !
   routed interface BVI2
   !
   evi 2
   !
  !
 !
igmp snooping profile 1
!
```

ピア 2 で実行される設定：

1. レイヤ 2 基本設定

```
hostname peer2
!
interface Bundle-Ether2
!
interface Bundle-Ether2.2 l2transport
 encapsulation dot1q 2
 rewrite ingress tag pop 1 symmetric
!
interface TenGigE0/0/0/0
 bundle id 2 mode on
 no shut
!
interface BVI2
 ipv4 address 100.2.0.1 255.255.255.0
 mac-address 1002.1111.2
!
```

2. EVPN 設定

```
hostname peer2
!
router bgp 100
 bgp router-id 2.2.2.2
 bgp graceful-restart
 address-family l2vpn evpn
 !
 neighbor 3.3.3.3
  remote-as 100
  update-source Loopback0
  address-family l2vpn evpn
  !
 !
!
evpn
 evi 2
  advertise-mac
  !
 !
 interface Bundle-Ether2
  ethernet-segment
   identifier type 0 02.02.02.02.02.02.02.02.02
   bgp route-target 0002.0002.0002
  !
 !
!
```

3. IGMPv2 スヌーピングの設定

```
hostname peer2
!
router igmp
 interface BVI2
  version 2
 !
!
l2vpn
 bridge group VLAN2
  bridge-domain VLAN2
   igmp snooping profile 1
   interface Bundle-Ether2.2
   !
   routed interface BVI2
   !
   evi 2
   !
  !
 !
igmp snooping profile 1
!
```

IGMP スヌーピングおよび EVPN 同期の確認

この例では、受信者はグループ 239.0.0.2 の IGMPv2 join を送信します。ピア 2 では、このグループには D フラグがあります。これは、ピア 1 ではなく、実際の IGMP がピア 2 に join しましたことを示します。ピア 1 では、このグループには B フラグがあります。これは、このグループが EVPN 同期機能を使用して BGP から学習されたことを示します。

```
RP/0/RP0/CPU0:peer1#show igmp snooping group
Fri Aug 31 22:27:46.363 UTC

Key: GM=Group Filter Mode, PM=Port Filter Mode
Flags Key: S=Static, D=Dynamic, B=BGP Learnt, E=Explicit Tracking, R=Replicated

                          Bridge Domain VLAN10:VLAN10

Group           Ver GM Source          PM Port                         Exp   Flgs
-----           --- -- ------          -- ----                         ---   ----
239.0.0.2       V2  -  *               -  BE2.2                        never B


RP/0/RP0/CPU0:peer2#show igmp snooping group
Fri Aug 31 22:27:49.686 UTC

Key: GM=Group Filter Mode, PM=Port Filter Mode
Flags Key: S=Static, D=Dynamic, B=BGP Learnt, E=Explicit Tracking, R=Replicated

                          Bridge Domain VLAN10:VLAN10

Group           Ver GM Source          PM Port                         Exp   Flgs
-----           --- -- ------          -- ----                         ---   ----
239.0.0.2       V2  -  *               -  BE2.2                        74    D
```

デュアル DR PIM アップリンクの確認

この例では、送信元 126.0.0.100 がグループ 239.0.0.2 にトラフィックを送信すると、ピア 1 とピア 2 の両方が PIM join アップストリームを送信していることがわかります。(*, G) と (S, G) の着信インターフェイスは、それぞれ RP と送信元へのインターフェイスである必要があります。ピア 1 とピア 2 の両方については、発信インターフェイスは、受信者側の BVI インターフェイスである必要があります。

```
RP/0/RP0/CPU0:peer1#show mrib route
:
:

(*,239.0.0.2) RPF nbr: 30.0.0.4 Flags: C RPF
  Up: 00:13:41
  Incoming Interface List
    HundredGigE0/0/0/1 Flags: A NS, Up: 00:13:41
  Outgoing Interface List
    BVI2 Flags: F NS LI, Up: 00:13:41

(126.0.0.100,239.0.0.2) RPF nbr: 30.0.0.4 Flags: RPF
  Up: 00:03:34
  Incoming Interface List
    HundredGigE0/0/0/1 Flags: A, Up: 00:03:34
  Outgoing Interface List
    BVI2 Flags: F NS, Up: 00:03:34
:
:

RP/0/RP0/CPU0:peer2#show mrib route
:
:

(*,239.0.0.2) RPF nbr: 50.0.0.4 Flags: C RPF
  Up: 00:13:33
  Incoming Interface List
```

```
    HundredGigE0/0/0/2 Flags: A NS, Up: 00:13:33
  Outgoing Interface List
    BVI2 Flags: F NS LI, Up: 00:13:33

(126.0.0.100,239.0.0.2) RPF nbr: 50.0.0.4 Flags: RPF
  Up: 00:03:24
  Incoming Interface List
    HundredGigE0/0/0/2 Flags: A, Up: 00:03:24
  Outgoing Interface List
    BVI2 Flags: F NS, Up: 00:03:24
:
:
```

指定されたフォワーダ選択の確認

前の例で説明したように、ピア 1 とピア 2 の両方には発信インターフェイスとしての BVI2 があります。ただし、ピアのうち 1 つだけがトラフィックを転送する必要があります。指定されたフォワーダ選択では、転送を実行するためにそのうちの 1 つを選択します。この例では、ピア 2 がフォワーダとして選択されています。ピア 1 には、NDF としてマークされた Bundle-Ether 2.2 があります。

```
RP/0/RP0/CPU0:peer1#show l2vpn forwarding bridge-domain VLAN2:VLAN2 mroute ipv4 hardware
 ingress detail location 0/0/cPU0
Bridge-Domain: VLAN2:VLAN2, ID: 0
:
:

Bridge-Domain: VLAN2:VLAN2, ID: 0
  Prefix: (0.0.0.0,239.0.0.2/32)
  P2MP enabled: N
  IRB platform data: {0x0, 0x2d, 0x0, 0x0}, len: 32
  Bridge Port:
  EVPN, Xconnect id: 0x80000001 NH:2.2.2.2
  Bundle-Ether2.2, Xconnect id: 0xa0000015 (NDF)


RP/0/RP0/CPU0:peer2#show l2vpn forwarding bridge-domain VLAN2:VLAN2 mroute ipv4 hardware
 ingress detail location 0/0/cPU0
:
:

Bridge-Domain: VLAN2:VLAN2, ID: 0
  Prefix: (0.0.0.0,239.0.0.2/32)
  P2MP enabled: N
  IRB platform data: {0x0, 0x30, 0x0, 0x0}, len: 32
  Bridge Port:
  EVPN, Xconnect id: 0x80000001 NH:1.1.1.1
  Bundle-Ether2.2, Xconnect id: 0xa0000029
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
MPLS VPLS ブリッジの設定	*MPLS Configuration Guide for Cisco NCS 560 Series Routers*の「Implementing Virtual Private LAN Services on Cisco IOS XR ソフトウェア」モジュール
スタートアップ情報	
EFP と EFP バンドルの設定	*Interface and Hardware Component Configuration Guide for Cisco NCS 560 Series Routers*

標準

標準[1]	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	—

[1] サポートされている標準がすべて記載されているわけではありません。

MIB

MIB	MIB のリンク
MIB は、IGMP スヌーピングをサポートしません。	Cisco IOS XR ソフトウェアを使用して MIB を特定およびダウンロードするには、次の URL にある Cisco MIB Locator を使用し、[Cisco Access Products] メニュー（http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml）からプラットフォームを選択します。

RFC

RFC	タイトル
RFC-4541	『Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches』

シスコのテクニカル サポート

説明	リンク
シスコのテクニカル サポート Web サイトでは、製品、テクノロジー、ソリューション、技術的なヒント、およびツールへのリンクなどの、数千ページに及ぶ技術情報が検索可能です。Cisco.com に登録済みのユーザは、このページから詳細情報にアクセスできます。	http://www.cisco.com/techsupport