CHAPTER 15

マルチキャスト IGMP

この章では、マルチキャスト インターネット グループ管理プロトコル（IGMP）スヌーピングに関する問題を識別して解決する方法について説明します。

この章で説明する内容は、次のとおりです。

マルチキャストについて

IP マルチキャストは、同一セットの IP パケットをネットワーク上の複数のホストに転送する手法です。マルチキャストは、IPv4 ネットワークと IPv6 ネットワークの両方で使用でき、複数の宛先への効率のよいデータ配信を実現します。

マルチキャストには、グループと呼ばれる IP マルチキャスト アドレスに送信されたマルチキャスト データの送信側と受信側の配信と検出の両方の手法が含まれます。グループと送信元 IP アドレスが入ったマルチキャスト アドレスは、しばしばチャネルと呼ばれます。

マルチキャスト IGMP スヌーピング

IGMP スヌーピング ソフトウェアは、VLAN 内のレイヤ 2 IP マルチキャスト トラフィックを調べて、該当する受信側が入っているポートを検出します。IGMP スヌーピングは、VLAN 全体でのフラッディングを避けるために、ポート情報を使用してマルチアクセス LAN 環境での帯域幅消費を低減させることができます。IGMP スヌーピング機能は、ルータによる IGMP メンバーシップ レポートの転送を支援するために、どのポートがマルチキャスト機能を持つルータに接続されているかを追跡します。IGMP スヌーピング ソフトウェアは、トポロジ変更通知に応答します。

基本的に、IGMP スヌーピングは次のように機能します。

- イーサネット スイッチ（Cisco Catalyst 6000 スイッチなど）が、すべての IGMP パケットを解析および傍受し、プロトコル処理のために CPU（スーパーバイザ モジュールなど）に転送します。
- ルータのポートが、IGMP クエリーを使用して学習されます。スイッチは、IGMP クエリーを返し、クエリーがどのポートから送られてきたかを記憶し、そのポートをルータ ポートとしてマークします。
- IGMP メンバーシップが、IGMP レポートを使用して学習されます。スイッチが、IGMP メンバーシップを追跡するために、IGMP レポート パケットを解析し、パケットを報告し、そのマルチキャスト転送テーブルを更新します。

- スイッチは、マルチキャスト トラフィックを受信したら、そのマルチキャスト テーブルをチェックし、そのトラフィックを受け取るべきポートだけにトラフィックを転送します。
- IGMP クエリーは、全 VLAN にフラッディングされます。
- IGMP レポートは、アップリンク ポート（ルータ ポート）に転送されます。
- マルチキャスト データ トラフィックは、アップリンク ポート（ルータ ポート）に転送されます。

マルチキャスト IGMP スヌーピングの問題

マルチキャスト IGMP スヌーピングの操作は、アップリンク スイッチが正しく設定されていないとうまく機能しません。IGMP プロセスは、IGMP ルーティングをサポートするルータにどのアップストリーム ポートが接続されているかを知る必要があるため、**ip multicast-routing** コマンドを発行して、アップストリーム スイッチで IP マルチキャスト ルーティングを有効にしておく必要があります。

次の例は、グローバルなマルチキャスト ルーティングを有効にし、SVI インターフェイスを設定し、PIM ルーティング プロトコルを有効にする方法を示します。

```
switch#conf terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)#ip multicast-routing
switch(config)#end

switch#conf terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)#int vlan159
switch(config-if)#ip pim dense-mode
switch(config-if)#end
```

トラブルシューティングのガイドライン

マルチキャスト IGMP の問題をトラブルシューティングする際には、次のガイドラインに従ってください。

- **show ip igmp snooping** コマンドを使用して、IGMP スヌーピングがイネーブルになっていることを確認します。
- アップストリーム スイッチの IGMP が設定されていることを確認します。
- **show ip igmp snooping groups** コマンドを使用して、スイッチが正しく設定され、マルチキャスト トラフィックを転送できる状態になっていることを確認します。コマンド出力のポート見出しの下で、R という文字を探します。R は、VSM がアップストリーム スイッチによって送信された IGMP クエリーからアップリンク ルータ ポートを学習したということを示しており、マルチキャスト トラフィックを転送できる状態になっています。

トラブルシューティング コマンド

マルチキャスト IGMP スヌーピングに関する問題をトラブルシューティングするには、次のコマンドを使用できます。

- **show cdp neighbor**

  IGMP はパケット VLAN を使用して IGMP パケットを VSM に転送していますが、これは Cisco Discovery Protocol（CDP; シスコ検出プロトコル）が使用するメカニズムと同じであるため、このトラブルシューティングにも **show cdp neighbor** コマンドを使用できます。ただし、アップストリーム スイッチで **no cdp enable** コマンドを使用して CDP プロトコルをディセーブルにしていた場合は、**show cdp neighbor** コマンドを実行しても何も情報は表示されません。

例 15-1　show cdp neighbor コマンド

```
n1000V# show cdp neighbor
Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater,
                  V - VoIP-Phone, D - Remotely-Managed-Device,
                  s - Supports-STP-Dispute

Device ID              Local Intrfce   Hldtme  Capability  Platform    Port ID
n1000V         Eth3/2            179    R S I       WS-C6506-E    Gig5/16
n1000V         Eth3/4            179    R S I       WS-C6506-E    Gig5/23
```

- **show ip igmp groups**

  show ip igmp groups コマンドでは、VLAN 上で IGMP スヌーピングがイネーブルになっていることを確認できます。

例 15-2　show ip igmp snooping vlan コマンド

```
n1000V# show ip igmp snooping vlan 159
IGMP Snooping information for vlan 159
  IGMP snooping enabled     <-- IGMP SNOOPING is enabled for vlan 159
  IGMP querier none
  Switch-querier disabled
  IGMPv3 Explicit tracking enabled (initializing, time-left: 00:03:20)
  IGMPv2 Fast leave disabled
  IGMPv1/v2 Report suppression enabled
  IGMPv3 Report suppression disabled
  Router port detection using PIM Hellos, IGMP Queries
  Number of router-ports: 0
  Number of groups: 0show ip igmp snooping
```

- **show ip igmp snooping groups**
- **debug ip igmp snooping vlan**

例 15-3　debug ip igmp snooping vlan コマンド

```
n1000V(config)# debug ip igmp snooping vlan
2008 Sep  2 13:29:36.125661 igmp: SNOOP: <vlan 159> Process a valid IGMP packet
2008 Sep  2 13:29:36.126005 igmp: SNOOP: <vlan 159> Received v2 report: group
224.0.0.251 fro 7.159.159.54 on Vethernet3
2008 Sep  2 13:29:36.126086 igmp: SNOOP: <vlan 159> Added oif Vethernet3 for (*,
224.0.0.251) entry
2008 Sep  2 13:29:36.126157 igmp: SNOOP: <vlan 159> Forwarding report for (*,
224.0.0.251) came on Vethernet3
```

```
2008 Sep  2 13:29:36.126225 igmp: SNOOP: <vlan 159> Forwarding the packet to
router-ports
2008 Sep  2 13:29:36.126323 igmp: SNOOP: <vlan 159> Forwarding packet to router-port
Ethernet3/6 (iod 42)
```

VSM 上で、次のコマンドを使用します。

- **module vem** *module-number* **execute vemcmd show vlan**

  例 15-4 の出力では、LTL 18 が vmnic3 に対応し、LTL 47 が VM fedora8, interface eth0 に対応することがわかります。

  224.1.2.3 のマルチキャスト グループ テーブルは、VEM がグループ 224.1.2.3 のマルチキャスト トラフィックを受信したときに転送先とするインターフェイスを示します。fedora8 がその eth0 インターフェイス上にマルチキャスト グループ 224.1.2.3 を持つ場合、LTL 47 が 224.1.2.3 のマルチキャスト グループ テーブルに入っている必要があります。

  LTL 18 は、マルチキャスト グループ 224.1.2.3 内にもあります。これは、LTL 18 が VM であり、224.1.2.3 へのマルチキャスト トラフィックを生成するということを意味します。トラフィックは、アップストリーム スイッチへのアップリンクである vmnic3 に転送されます。

  0.0.0.0 のマルチキャスト グループ テーブル エントリは、デフォルト ルートを提供します。どのマルチキャスト グループにも一致しないマルチキャスト グループ トラフィックがあった場合、そのアドレスにはデフォルト ルートが使用されます。つまり、この場合、トラフィックは vmnic3 を介してアップストリーム スイッチに転送されます。

例 15-4　　module vem *module-number execute* **vemcmd show vlan コマンド**

```
n1000V# module vem 3 execute vemcmd show vlan 159
BD 159, vdc 1, vlan 159, 3 ports
Portlist:
     18  vmnic3
     47  fedora8.eth0

Multicast Group Table:
Group 224.1.2.3 RID 1 Multicast LTL 4408
    47
    18
Group 0.0.0.0 RID 2 Multicast LTL 4407
    18
```

現象、原因、および解決方法

現象	考えられる原因	解決方法
VM がマルチキャスト トラフィックを受け取る必要があるのに、マルチキャスト トラフィックを受信していない。	—	**debug ip igmp snooping vlan** コマンドを使用して、IGMP スヌーピングが期待されるとおりに機能しているかどうかを調べます。出力を見て、ポートが IGMP レポートを受信しているか、およびインターフェイスが VM のマルチキャスト トラフィック インターフェイス リストに追加されているかを調べます。
	—	**module vem** *module-number* **execute vemcmd show vlan** コマンドを使用して、VEM 内のマルチキャスト分散テーブルに正しい情報が格納されていることを確認します。
	—	**module vem** *module-number* **execute vemcmd show port** コマンドを使用して、ポート テーブルを見ます。テーブルに正しい情報が格納されていることを確認します。トランク ポートとアクセス ポートの状態が UP/UP になっていることを確認します。