



## SSM の設定

---

- [SSM の設定の前提条件](#) (1 ページ)
- [SSM 設定の制約事項](#) (2 ページ)
- [SSM に関する情報](#) (3 ページ)
- [SSM の設定方法](#) (7 ページ)
- [SSM のモニタリング](#) (15 ページ)
- [SSM の次の作業](#) (15 ページ)
- [SSM に関するその他の関連資料](#) (16 ページ)
- [SSM の機能情報](#) (16 ページ)

## SSM の設定の前提条件

次に、Source-Specific Multicast (SSM) および SSM マッピングを設定するための前提条件を示します。

- SSM マッピングを設定する前に、次の作業を実行する必要があります。
  - IP マルチキャスト ルーティングをイネーブルにします。
  - PIM スパース モードをイネーブルにします。
  - SSM を設定します。
- スタティック SSM マッピングを設定する場合は、事前にアクセス コントロール リスト (ACL) を設定して、送信元アドレスにマッピングされるグループ範囲を定義する必要があります。
- SSM マッピングを設定し、DNS ルックアップで使用できるようにするには、稼働中の DNS サーバにレコードを追加する必要があります。稼働中の DNS サーバがない場合は、DNS サーバをインストールする必要があります。



---

(注) 実行中の DNS サーバにレコードを追加するには、*Cisco Network Registrar* などの製品を使用できます。

---

## SSM 設定の制約事項

次に、SSM を設定する際の制約事項を示します。

- IGMPv3 で SSM を使用するには、Cisco IOS 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。
- SSM にまだ対応していない、ネットワーク内の既存のアプリケーションは、(S, G) チャンネル加入をサポートするように変更されないと、SSM 範囲内では機能しません。そのため、既存のアプリケーションが指定の SSM 範囲内のアドレスを使用する場合、ネットワークで SSM をイネーブルにすると問題が発生することがあります。
- IGMP スヌーピング：IGMPv3 で使用される新しいメンバーシップ レポート メッセージは、旧型の IGMP スヌーピングデバイスでは正しく認識されない場合があります。
- SSM をレイヤ 2 スイッチング メカニズムとともに使用する場合は、ある程度のアドレス管理が必要となります。Cisco Group Management Protocol (CGMP)、IGMP スヌーピング、または Router-Port Group Management Protocol (RGMP) でサポートされるのはグループ固有のフィルタリングだけであり、(S, G) チャンネル固有のフィルタリングはサポートされていません。同じスイッチドネットワーク内の異なるレシーバーが異なる (S, G) チャンネルを要求し、これらのチャンネルが同じグループを共有している場合、レシーバーは上記のような既存メカニズムの利点を活用できません。どちらのレシーバーも、すべての (S, G) チャンネルトラフィックを受信し、不要なトラフィックを入力から除外します。SSM は、独立した多くのアプリケーションに SSM 範囲のグループアドレスを再利用できるので、このような状況では、スイッチドネットワークのトラフィック フィルタリング機能が低下する可能性があります。そのため、アプリケーションに対して SSM 範囲の IP アドレスをランダムに使用し、SSM 範囲内の 1 つのアドレスがさまざまなアプリケーションに再利用される可能性を小さくすることが重要です。たとえば、TV チャンネルセットを提供するアプリケーションサービスで、SSM を使用する場合は、各 TV (S, G) チャンネルに異なるグループを使用する必要があります。このようにすれば、同じアプリケーションサービス内の異なるチャンネルに複数のレシーバが接続されていても、レイヤ 2 デバイスを含むネットワークでトラフィック エイリアシングが発生しなくなります。
- PIM-SSM では、ラストホップルータは、そのインターフェイス上に適切な (S, G) 加入登録があると、定期的に (S, G) Join メッセージを送信し続けます。このため、レシーバが (S, G) 加入を送信する限り、ソースが長時間（または二度と）トラフィックを送信しなくてもレシーバからソースへの最短パス ツリー (SPT) 状態が維持されます。

送信元がトラフィックを送信し、レシーバーがグループに加入している場合にだけ (S, G) ステートが維持される PIM-SM では、これとは対照的な状況が発生します。PIM-SM では、送信元がトラフィックの送信を 3 分以上停止すると、(S, G) ステートは削除され、その送信元からのパケットが RPT を通じて再度到達した場合のみに再確立されます。PI-SSM では、送信元がアクティブであることをレシーバに通知するメカニズムがないので、レシーバが (S, G) チャンネルの受信を要求している限り、(S, G) ステートを維持する必要があります。

次に、SSM マッピングを設定する際の制約事項を示します。

- SSM マッピング機能で、SSM の利点をすべて共有できるわけではありません。SSM マッピングでは、ホストからグループ G の加入が取得され、1つまたは複数のソースに関連付けられているアプリケーションでこのグループを指定できるため、グループ G ごとにこのようなアプリケーション1つのみをサポートできます。それにもかかわらず、完全な SSM アプリケーションは、SSM マッピングにも使用される同じグループを共有することができます。
- 完全な SSM への移行ソリューションとして SSM マッピングだけを使用する場合は、ラストホップルータの IGMPv3 をイネーブルにする際に十分に注意してください。SSM マッピングと IGMPv3 を両方イネーブルにした場合、すでに IGMPv3 をサポートしている (SSM はサポートしていない) ホストは IGMPv3 グループ レポートを送信します。SSM マッピングは、このような IGMPv3 グループ レポートをサポートしていないので、ルータは送信元をこれらのレポートと正しく関連付けることができません。

## SSM に関する情報

Source-Specific Multicast (SSM; 送信元特定マルチキャスト) 機能は、IP マルチキャストの拡張機能であり、この機能を使用すると、受信者に転送されるデータグラムトラフィックは、その受信者が明示的に加入しているマルチキャスト送信元からのトラフィックだけになります。SSM 用にマルチキャスト グループを設定する場合、SSM 配信ツリー (共有ツリーはない) だけが作成されます。

ここでは、Source-Specific Multicast (SSM) の設定方法を説明します。この項の SSM コマンドの詳細な説明については、『*IP Multicast Command Reference*』を参照してください。

## SSM コンポーネントの概要

SSM は、1対多のアプリケーション (ブロードキャストアプリケーション) に最適なデータグラム配信モデルです。SSM は、オーディオおよびビデオのブロードキャスト アプリケーション環境を対象としたシスコの IP マルチキャスト ソリューションの中核的なネットワークングテクノロジーです。このデバイスは、次のコンポーネントをサポートしているため、SSM の実装が可能です。

- Protocol Independent Multicast Source-Specific Mode (PIM-SSM)

PIM-SSM は、SSM の実装をサポートするルーティング プロトコルで、PIM Sparse Mode (PIM-SM) に基づいています。

- Internet Group Management Protocol version 3 (IGMPv3)

## SSM および Internet Standard Multicast (ISM)

インターネットの現行の IP マルチキャスト インフラストラクチャや多くの企業のイントラネットは、PIM-SM プロトコルと Multicast Source Discovery Protocol (MSDP) に基づいています。これらのプロトコルには、Internet Standard Multicast (ISM) サービス モデルの限界がありま

す。たとえば、ISM では、ネットワークは、実際にマルチキャストトラフィックを送信しているホストについての情報を維持する必要があります。

ISM サービスは、任意の送信元からマルチキャストホストグループと呼ばれるレシーバーグループへの IP データグラムの配信でなりたっています。マルチキャストホストグループのデータグラムトラフィックは、任意の IP ユニキャスト送信元アドレス (S) と IP 宛先アドレスとしてのマルチキャストグループアドレス (G) のデータグラムで構成されます。システムは、ホストグループのメンバーになることによって、このトラフィックを受信します。ホストグループのメンバーシップには IGMP バージョン 1、2、または 3 によるホストグループのシグナリングが必要です。

SSM では、データグラムは (S, G) チャンネルに基づいて配信されます。SSM と ISM のどちらでも、ソースになるためにシグナリングは必要ありません。ただし、SSM では、レシーバーは特定の送信元からのトラフィックの受信または非受信を決めるために (S, G) への加入または脱退を行う必要があります。つまり、レシーバーは加入した (S, G) チャンネルからだけトラフィックを受信できます。一方、ISM では、レシーバーは受信するトラフィックの送信元の IP アドレスを知る必要はありません。チャンネル加入シグナリングの標準的な方法として、IGMP を使用してモードメンバーシップレポートを包含することが提案されていますが、この手法をサポートしているのは IGMP version 3 だけです。

## SSM IP アドレスの範囲

IP マルチキャストグループアドレス範囲の設定済みのサブセットに SSM 配信モデルを適用することにより、SSM と ISM サービスを一緒に使用できます。Cisco IOS 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 SSM 設定が可能です。SSM 範囲が定義されている場合、既存の IP マルチキャスト受信アプリケーションが SSM 範囲のアドレスの使用を試行しても、トラフィックを受信できません。

## SSM の動作

確立されているネットワークは、IP マルチキャストサービスが PIM SSM に基づいているので、SSM サービスをサポートできます。SSM サービスだけが必要な場合は、ドメイン間の PIM-SM に必要な全プロトコル範囲 (MSDP、Auto-RP、またはブートストラップルータ (BSR)) ではなく、SSM を単独でネットワークに配置することもできます。

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、SSM をサポートするのはラストホップルータだけです。レシーバーに直接接続されていないルータは SSM をサポートする必要はありません。一般的に、ラストホップ以外のルータに必要なのは、SSM 範囲内の PIM-SM だけです。このようなルータは SSM 範囲内での MSDP シグナリング、登録、PIM-SM 共有ツリー操作を抑制するために、ほかのアクセスコントロール設定が必要になる場合もあります。

SSM の範囲を設定し SSM をイネーブルにするには、`ip pim ssm` グローバル コンフィギュレーション コマンドを使用します。この設定による影響は次のとおりです。

- SSM 範囲内のグループは、IGMPv3 include モードメンバーシップレポートを通じて、(S, G) チャンネルに加入できます。

- SSM 範囲のアドレスの PIM 動作は、PIM-SM の派生モードである PIM-SSM に変更されます。このモードでは、ルータで生成されるのは PIM (S, G) の join と prune のメッセージだけであり、(S, G) の Rendezvous Point Tree (RPT) や (\*, G) の RPT メッセージは生成されません。RPT 動作に関連する着信メッセージは無視されるか拒否されます。着信 PIM 登録メッセージに対しては即座に register-stop メッセージで応答が行われます。ラストホップルータ以外のルータでは、PIM-SSM は PIM-SM と下位互換性を保ちます。したがって、ラストホップルータ以外のルータは SSM グループに PIM-SM を使用できません (SSM をサポートしていない場合など)。
- SSM 範囲内の Source-Active (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 マッピング

典型的なセットトップボックス (STB) 配置では、各 TV チャンネルは独立した 1 つの IP マルチキャストグループを使用し、その TV チャンネルの送信を行うアクティブなサーバは 1 つです。1 つのサーバから複数の TV チャンネルへの送信は可能ですが、各チャンネルのグループはそれぞれ異なります。このようなネットワーク環境で、ルータが特定のグループの IGMPv1 または IGMPv2 のメンバーシップレポートを受信した場合、レポートの宛先は、そのマルチキャストグループに関連付けられている TV チャンネルの well-known TV サーバになります。

SSM マッピングが設定されている場合、特定グループの IGMPv1 または IGMPv2 のメンバーシップレポートを受信したルータは、レポートを、このグループに関連付けられている well-known 送信元の 1 つ以上のチャンネルメンバーシップに変換します。

ルータは、IGMPv1 または IGMPv2 のメンバーシップレポートを受信すると、SSM マッピングを使用して、そのグループに 1 つ以上の送信元 IP アドレスを決定します。その後、SSM マッピングによって、そのメンバーシップレポートが IGMPv3 レポートに変換され、IGMPv3 レポートを受信した場合と同様に処理が続行されます。IGMPv1 または IGMPv2 メンバーシップレポートの受信が続き、そのグループの SSM マッピングが同じである限り、ルータは PIM join を送信し、グループに加入し続けます。

SSM マッピング機能を使用すると、ラストホップルータはスタティックに設定されたルータ上のテーブルまたは DNS サーバを通じて、送信元アドレスを決定できます。スタティックに設定されたテーブルまたは DNS マッピングが変更された場合、ルータは加入しているグループに関連付けられている現在の送信元から脱退します。

## スタティック SSM マッピング

スタティック SSM マッピングでは、ラストホップルータは、グループへの送信を行う送信元を決定するために、継続的にスタティック マップを使用します。スタティック SSM マッピングを使用するには、グループ範囲を定義した ACL を設定する必要があります。グループ範囲を定義する ACL を設定した後、**ip igmp ssm-map static** グローバル コンフィギュレーション コマンドを使用して、ACL で許可されたグループを送信元にマッピングできます。

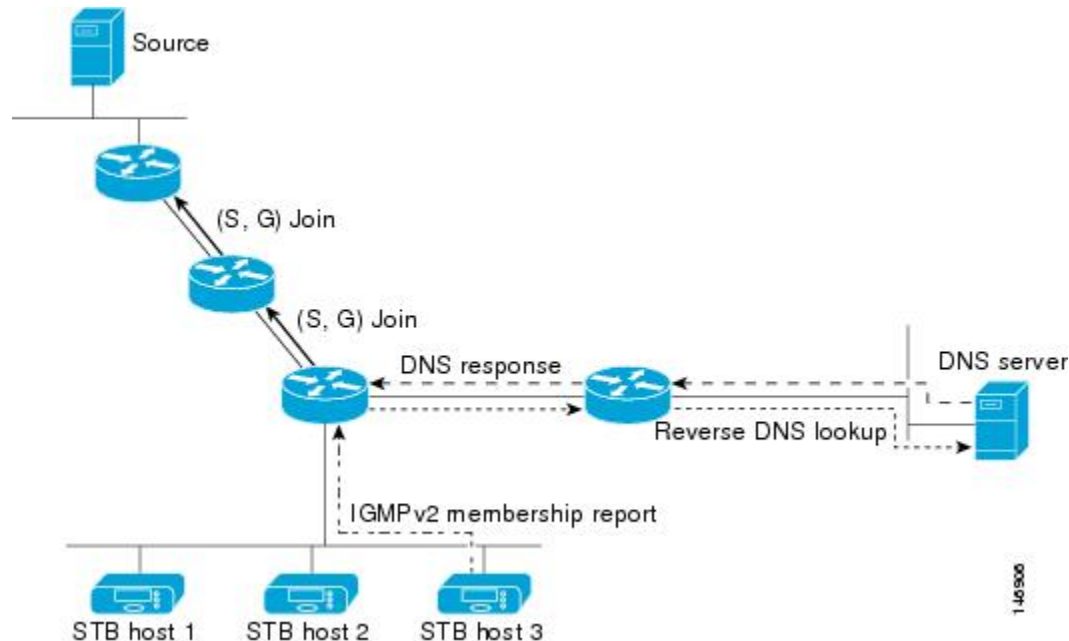
DNSが必要とされないか、またはローカルでDNSマッピングが変更される場合、小規模なネットワークではスタティック SSM マッピングを設定できます。設定されたスタティック SSM マッピングは、DNS マッピングよりも優先されます。

## DNS ベースの SSM マッピング

DNSベースのSSMマッピングを使用して、ラストホップルータが継続的に逆DNSルックアップを実行し、グループに送信する送信元を決定するようにすることも可能です。DNSベースのSSMマッピングが設定されると、ルータはグループ名を含むドメイン名を構築し、DNSへの逆ルックアップを実行します。ルータはIPアドレスリソースを検索し、それらをグループに関連付けられた送信元アドレスとして使用します。SSMマッピングでサポートできる送信元数は、グループごとに最大20です。ルータは各グループに設定されているすべてのソースに加入します。

図 1: DNS ベースの SSM マッピング

次の図は、DNS ベースの SSM マッピングを示します。



ラストホップルータが1つのグループの複数の送信元に加入できるようにするSSMマッピングメカニズムによって、TVブロードキャストの送信元に冗長性を持たせることができます。この場合、ラストホップルータは、SSMマッピングを使用し、同じTVチャンネルに対して2つのビデオ送信元に同時に加入することにより冗長性を提供します。ただし、ラストホップルータでのビデオトラフィックの重複を防ぐため、ビデオ送信元がサーバ側でスイッチオーバーメカニズムを使用する必要があります。一方のビデオ送信元はアクティブ、もう一方のバックアップビデオ送信元はパッシブになります。パッシブの送信元は待機状態になり、アクティブな送信元の障害が検出された場合に、そのTVチャンネルにビデオトラフィックを送信します。サーバ側のスイッチオーバーメカニズムによって、実際にそのTVチャンネルにビデオトラフィックを送信するサーバは1つだけになります。

G1、G2、G3、G4 を含むグループの 1 つ以上の送信元アドレスを検索するには、DNS サーバに次のような DNS レコードを設定する必要があります。

```
G4.G3.G2.G1 [multicast-domain] [timeout] IN A source-address-1
IN A source-address-2
IN A source-address-n
```

DNS リソース レコードの設定の詳細については、DNS サーバのマニュアルを参照してください。

## SSM の設定方法

### SSM の設定

SSM を設定するには、次の手順を実行します。

この手順は任意です。

#### 始める前に

Source Specific Multicast (SSM) 範囲の定義にアクセスリストを使用する場合、**ip pim ssm** コマンドでアクセスリストを参照する前にアクセスリストを設定します。

#### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例： Device> <b>enable</b>	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	<b>configure terminal</b> 例： Device# <b>configure terminal</b>	グローバル コンフィギュレーション モードを開始します。
ステップ 3	<b>ip pim ssm [default   range access-list]</b> 例： Device(config)# <b>ip pim ssm range 20</b>	IP マルチキャストアドレスの SSM 範囲を定義します。
ステップ 4	<b>interface type number</b> 例：	IGMPv3 をイネーブルに設定可能なホストに接続されているインターフェイスを

	コマンドまたはアクション	目的
	<pre>Device(config)# interface gigabitethernet 1/0/1</pre>	<p>選択し、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。</p> <p>次のいずれかのインターフェイスを指定する必要があります。</p> <ul style="list-style-type: none"> <li>• ルーテッドポート：レイヤ3ポートとして <b>no switchport</b> インターフェイスコンフィギュレーションコマンドを入力して設定された物理ポートです。</li> <li>• SVI： <b>interface vlan vlan-id</b> グローバルコンフィギュレーションコマンドを使用して作成された VLAN インターフェイスです。</li> </ul> <p>これらのインターフェイスには、IP アドレスを割り当てる必要があります。</p>
ステップ 5	<pre>ip pim {sparse-mode }</pre> <p>例：</p> <pre>Device(config-if)# ip pim sparse-mode</pre>	<p>インターフェイスに対して PIM をイネーブルにします。</p>
ステップ 6	<pre>ip igmp version 3</pre> <p>例：</p> <pre>Device(config-if)# ip igmp version 3</pre>	<p>このインターフェイス上で IGMPv3 をイネーブルにします。デフォルトでは、IGMP のバージョン 2 が設定されます。</p>
ステップ 7	<pre>end</pre> <p>例：</p> <pre>Device(config)# end</pre>	<p>特権 EXEC モードに戻ります。</p>
ステップ 8	<pre>show running-config</pre> <p>例：</p> <pre>Device# show running-config</pre>	<p>入力を確認します。</p>
ステップ 9	<pre>copy running-config startup-config</pre> <p>例：</p> <pre>Device# copy running-config</pre>	<p>(任意) コンフィギュレーションファイルに設定を保存します。</p>



	コマンドまたはアクション	目的
	<code>startup-config</code>	

## Source-Specific Multicast (SSM) マッピングの設定

Source Specific Multicast (SSM) マッピング機能は、管理上または技術上の理由からエンドシステムで SSM をサポートできないかまたはサポートが望ましくない場合に SSM 移行手段として使用できます。SSM マッピングを使用すると、IGMPv3 をサポートしないレガシー STB へのビデオ配信や、IGMPv3 ホストスタックを使用しないアプリケーションに SSM を活用できます。

### スタティック SSM マッピングの設定

スタティック SSM マッピングを設定するには、次の手順を実行します。

#### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例： <code>Device&gt; enable</code>	特権 EXEC モードを有効にします。 <ul style="list-style-type: none"><li>パスワードを入力します（要求された場合）。</li></ul>
ステップ 2	<b>configure terminal</b> 例： <code>Device# configure terminal</code>	グローバル コンフィギュレーションモードを開始します。
ステップ 3	<b>ip igmp ssm-map enable</b> 例： <code>Device(config)# ip igmp ssm-map enable</code>	設定されている SSM 範囲で、グループの SSM マッピングをイネーブルにします。  (注) このコマンドでは、デフォルトで、DNS ベースの SSM マッピングがイネーブルにされます。
ステップ 4	<b>no ip igmp ssm-map query dns</b> 例：	(任意) DNS ベースの SSM マッピングをディセーブルにします。

	コマンドまたはアクション	目的
	<pre>Device(config)# no ip igmp ssm-map query dns</pre>	<p>(注) スタティック SSM マッピングだけを使用する場合は、DNS ベースの SSM マッピングをディセーブルにします。デフォルトでは、<b>ip igmp ssm-map</b> コマンドによって DNS ベースの SSM マッピングがイネーブルになります。</p>
ステップ 5	<p><b>ip igmp ssm-map static</b> <i>access-list</i> <i>source-address</i></p> <p>例 :</p> <pre>Device(config)# ip igmp ssm-map static 11 172.16.8.11</pre>	<p>スタティック SSM マッピングを設定します。</p> <ul style="list-style-type: none"> <li>• <i>access-list</i> 引数に入力した ACL によって、<i>source-address</i> 引数に入力したソース IP アドレスにマッピングされるグループが決まります。</li> </ul> <p>(注) 追加のスタティック SSM マッピングを設定することもできます。SSM マッピングを追加設定した場合、ルータが SSM 範囲のグループの IGMPv1 または IGMPv2 のメンバーシップレポートを受信すると、デバイスは、設定されている各 <b>ip igmp ssm-map static</b> コマンドに基づいて、そのグループに関連付けられている送信元アドレスを特定します。デバイスは各グループに最大 20 の送信元を関連付けます。</p> <p>必要な場合は、ステップを繰り返して、追加のスタティック SSM マッピングを設定します。</p>
ステップ 6	<p><b>end</b></p> <p>例 :</p> <pre>Device(config)# end</pre>	<p>特権 EXEC モードに戻ります。</p>
ステップ 7	<p><b>show running-config</b></p> <p>例 :</p>	<p>入力を確認します。</p>

	コマンドまたはアクション	目的
	Device# <code>show running-config</code>	
ステップ 8	<b>copy running-config startup-config</b> 例 : Device# <code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

## DNS ベースの SSM マッピングの設定

DNS ベースの SSM マッピングを設定するには、DNS サーバゾーンを作成するか、または既存のゾーンにレコードを追加する必要があります。DNS ベースの SSM マッピングを使用するルータが他の目的にも DNS を使用している場合は、通常の設定の DNS サーバを使用する必要があります。そのルータで使用されている DNS 実装が DNS ベースの SSM マッピングだけの場合は、ルートゾーンが空であるか、またはそれ自身を指すようなフォールス DNS セットアップが可能です。

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例 : Device> <code>enable</code>	特権 EXEC モードを有効にします。 <ul style="list-style-type: none"> <li>パスワードを入力します (要求された場合)。</li> </ul>
ステップ 2	<b>configure terminal</b> 例 : Device# <code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 3	<b>ip igmp ssm-map enable</b> 例 : Device(config)# <code>ip igmp ssm-map enable</code>	設定されている SSM 範囲で、グループの SSM マッピングをイネーブルにします。
ステップ 4	<b>ip igmp ssm-map query dns</b> 例 : Device(config)# <code>ip igmp ssm-map query dns</code>	(任意) DNS ベースの SSM マッピングをイネーブルにします。 <ul style="list-style-type: none"> <li>デフォルトでは、<code>ip igmp ssm-map</code> コマンドによって DNS ベースの SSM マッピングがイネーブルになります。実行コンフィギュレー</li> </ul>

	コマンドまたはアクション	目的
		<p>ションに保存されるのは、このコマンドを <b>no</b> 形式で使用した場合だけです。</p> <p>(注) DNS ベースの SSM マッピングがディセーブルの場合、このコマンドを使用して DNS ベースの SSM マッピングを再度イネーブルにします。</p>
ステップ 5	<p><b>ip domain multicast</b> <i>domain-prefix</i></p> <p>例 :</p> <pre>Device(config)# ip domain multicast ssm-map.cisco.com</pre>	<p>(任意) DNS ベースの SSM マッピングに使用するドメインプレフィックスを変更します。</p> <ul style="list-style-type: none"> <li>• デフォルトでは、<b>ip-addr.arpa</b> ドメインプレフィックスが使用されます。</li> </ul>
ステップ 6	<p><b>ip name-server</b> <i>server-address1</i> [<i>server-address2...server-address6</i>]</p> <p>例 :</p> <pre>Device(config)# ip name-server 10.48.81.21</pre>	<p>名前とアドレスの解決に使用する 1 つまたは複数のネームサーバのアドレスを指定します。</p>
ステップ 7	冗長性のために追加の DNS サーバを設定する場合は、必要に応じて、ステップ 6 を繰り返します。	
ステップ 8	<p><b>end</b></p> <p>例 :</p> <pre>Device(config)# end</pre>	特権 EXEC モードに戻ります。
ステップ 9	<p><b>show running-config</b></p> <p>例 :</p> <pre>Device# show running-config</pre>	入力を確認します。
ステップ 10	<p><b>copy running-config startup-config</b></p> <p>例 :</p> <pre>Device# copy running-config startup-config</pre>	(任意) コンフィギュレーションファイルに設定を保存します。

## SSM マッピングを使用したスタティック トラフィック転送の設定

ラスト ホップ ルータ上の SSM マッピングでスタティック トラフィック転送を設定する場合は、次の手順を実行します。

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例 : Device> <b>enable</b>	特権 EXEC モードを有効にします。 <ul style="list-style-type: none"> <li>パスワードを入力します (要求された場合)。</li> </ul>
ステップ 2	<b>configure terminal</b> 例 : Device# <b>configure terminal</b>	グローバル コンフィギュレーション モードを開始します。
ステップ 3	<b>interface interface-id</b> 例 : Device(config)# <b>interface gigabitethernet 1/0/1</b>	SSM マッピングを使用してマルチキャスト グループにスタティックにトラフィックを転送するインターフェイスを選択し、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。 次のいずれかのインターフェイスを指定する必要があります。 <ul style="list-style-type: none"> <li>ルーテッドポート : レイヤ 3 ポートとして <b>no switchport</b> インターフェイス コンフィギュレーション コマンドを入力して設定された物理ポートです。</li> <li>SVI : <b>interface vlan vlan-id</b> グローバル コンフィギュレーション コマンドを使用して作成された VLAN インターフェイスです。</li> </ul> これらのインターフェイスには、IP アドレスを割り当てる必要があります。

	コマンドまたはアクション	目的
		(注) SSM マッピングを使用したトラフィックのスタティック転送は、DNS ベースの SSM マッピングとスタティックに設定された SSM マッピングのいずれかで機能します。
ステップ 4	<b>ip igmp static-group group-address source ssm-map</b> 例 : <pre>Device(config-if)# ip igmp static-group 239.1.2.1 source ssm-map</pre>	そのインターフェイスから (S,G) チャネルへのスタティック転送用の SSM マッピングを設定します。 このコマンドは、特定グループに SSM トラフィックをスタティックに転送する場合に使用します。チャネルの送信元アドレスを決定するには DNS ベースの SSM マッピングを使用します。
ステップ 5	<b>end</b> 例 : <pre>Device(config)# end</pre>	特権 EXEC モードに戻ります。
ステップ 6	<b>show running-config</b> 例 : <pre>Device# show running-config</pre>	入力を確認します。
ステップ 7	<b>copy running-config startup-config</b> 例 : <pre>Device# copy running-config startup-config</pre>	(任意) コンフィギュレーション ファイルに設定を保存します。

## SSM のモニタリング

SSM をモニタするには、次の表の特権 EXEC コマンドを使用します。

表 1: SSM のモニタリングコマンド

コマンド	目的
<code>show ip igmp groups detail</code>	IGMPv3 による (S,G) チャンネル加入登録を表示します。
<code>show ip mroute</code>	マルチキャストグループが SSM サービスをサポートしているかどうか、または送信元固有のホスト レポートが受信されたかどうかを表示します。

## SSM マッピングのモニタリング

SSM マッピングをモニタするには、次の表の特権 EXEC コマンドを使用します。

表 2: SSM マッピングをモニタするコマンド

コマンド	目的
<code>show ip igmp ssm-mapping</code>	SSM マッピングについての情報を表示します。
<code>show ip igmp ssm-mapping group-address</code>	SSM マッピングが特定のグループに使用する送信元を表示します。
<code>show ip igmp groups [group-name   group-address   interface-type interface-number] [detail]</code>	ルータに直接接続されているレシーバと IGMP によって学習されたレシーバを持つマルチキャストグループを表示します。
<code>show host</code>	デフォルトのドメイン名、名前ルックアップサービス、ネームサーバホストのリスト、およびホスト名とアドレスのキャッシュされたリストを表示します。
<code>debug ip igmp group-address</code>	送受信された IGMP パケットと IGMP ホスト関連イベントを表示します。

## SSM の次の作業

次の設定を行えます。

- IGMP
- PIM
- IP マルチキャストルーティング
- サービス検出ゲートウェイ

## SSM に関するその他の関連資料

### 関連資料

関連項目	マニュアル タイトル
この章で使用するコマンドの完全な構文および使用方法の詳細。	の「IP マルチキャストルーティングのコマンド」の項を参照してください。 <i>Command Reference (Catalyst 9200 Series Switches)</i>

### 標準および RFC

標準/RFC	タイトル
RFC 4601	『 <i>Protocol-Independent Multicast-Sparse Mode (PIM-SM): Protocol Specification</i> 』

## SSM の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、[www.cisco.com/go/cfn](http://www.cisco.com/go/cfn) に移動します。Cisco.com のアカウントは必要ありません。



表 3: SSM の機能情報

機能名	リリース	機能情報
SSM	Cisco IOS XE Fuji 16.9.2	Source-Specific Multicast (SSM; 送信元特定マルチキャスト) 機能は、IP マルチキャストの拡張機能であり、この機能を使用すると、受信者に転送されるデータグラムトラフィックは、その受信者が明示的に加入しているマルチキャスト送信元からのトラフィックだけになります。SSM用にマルチキャストグループを設定する場合、SSM 配信ツリー (共有ツリーはない) だけが作成されます。

