

# 安全IP组播部署

## 目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[术语](#)

[任意源组播](#)

[源特定组播](#)

[相关组播协议/数据包类型](#)

[IGMP/MLD数据包](#)

[PIM控制数据包](#)

[组播PIM控制数据包](#)

[单播PIM控制数据包](#)

[自动RP数据包](#)

[组播服务发现协议\(MSDP\)数据包](#)

[组播环境中的威胁](#)

[信任区域和信任边界](#)

[威胁概述](#)

[路由器面临的基本威胁](#)

[来自源端的威胁](#)

[来自接收方的威胁](#)

[对交汇点和BSR的威胁](#)

[组播和单播安全 \(对比\)](#)

[状态注意事项/过滤器](#)

[来自组播源的攻击](#)

[状态攻击](#)

[接收器发起的攻击](#)

[组播网络中的安全性](#)

[网元安全](#)

[控制层面策略 \(CoPP\)](#)

[本地数据包传输服务\(LPTS\)](#)

[组播特定的安全](#)

[Mroute限制](#)

[网络安全](#)

[禁用组播组](#)

[PIM安全](#)

[PIM邻居控制](#)

[RP/PIM-SM相关过滤器](#)

[自动RP过滤器](#)

[域间过滤器和MSDP](#)

[发件人/源问题](#)

[基于数据包过滤器的访问控制 — 控制源](#)

[PIM-SM源控制](#)

[接收器问题 — 控制IGMP/MLD](#)

[准入控制](#)

[全局和每个接口的IGMP限制](#)

[每个接口的mroute限制](#)

[组播和IPSec](#)

[GET VPN简介](#)

[使用GET VPN加密组播数据平面流量](#)

[使用GET VPN验证控制平面流量](#)

[结论](#)

[相关信息](#)

## 简介

本文档介绍有关保护IP组播网络基础设施的最佳实践的一般指南。

## 先决条件

### 要求

Cisco 建议您了解以下主题：

- IP 组播

### 使用的组件

本文档不限于特定的软件和硬件版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

## 背景信息

本文档介绍一些基本概念和术语，并讨论下列主题：

- 保护特定平台和整个网络的机制。
- 任何源组播(ASM)和源特定组播(SSM)模型。
- 组播虚拟专用网络(MVPN)安全。
- 组加密传输(GET)虚拟专用网络(VPN)架构，为组播数据平面或控制平面流量提供机密性和完整性。

### 术语

在IP组播中有两种典型的服务模型：

- 1.任意源组播(ASM)
- 2.源特定组播(SSM)

在ASM中，接收方通过互联网组成员协议(IGMP)或组播侦听程序发现(MLD)成员身份报告加入组G以指示该组。此报告请求任何源发送到组G的流量，因此名称为“any source”。相反，在SSM中，接收方加入由源S定义的特定信道，源S向组G发送该信道。以下详细介绍每种服务模型。

## 任意源组播

ASM模型的特征在于有两种协议：“密集模式泛洪和修剪”和“稀疏模式显式连接”：

### i)密集模式泛洪和修剪协议(DVMRP/MOSPF/PIM-DM)

在密集模式协议中，网络中的所有路由器都知道所有树、它们的源和接收器。距离矢量组播路由协议(DVMRP)和协议无关组播(PIM)等协议密集模式通过创建“修剪状态”在整个网络中泛洪“活动源”信息，并在不需要特定树流量的部分拓扑中构建树。它们也称为泛洪和修剪协议。在组播开放最短路径优先(MOSPF)中，有关接收器的信息在整个网络中泛洪以支持树构建。

不需要使用密集模式协议，因为网络某些部分中构建的每棵树都可能始终导致网络中所有路由器（或管理范围内，如果已配置）的资源利用率（具有收敛影响）。这些协议在本文的其余部分中不再讨论。

### ii)稀疏模式显式连接协议(PIM-SM/PIM-BiDir)

使用稀疏模式显式加入协议时，设备不会在网络中创建组特定状态，除非接收方已发送组的显式IGMP/MLD成员身份报告（或“加入”）。众所周知，ASM的这种变体能够很好地扩展，是重点的组播模式。

这是PIM稀疏模式的基础，大多数组播部署已使用到这一点。这也是双向PIM(PIM-BiDir)的基础，PIM-BiDir正越来越多地用于多个（源）到多个（接收器）应用。

这些协议称为稀疏模式，因为它们有效支持具有“稀疏”接收器群体的IP组播传输树，并仅在源和接收器之间的路径以及PIM-SM/BiDir中交汇点(RP)的路由器上创建控制平面状态。它们不会在网络的其它部分创建状态。只有在路由器收到来自下游路由器或接收方的加入时，才会明确建立其状态，因此命名为“显式加入协议”。

PIM-SM和PIM-BiDir都采用“共享树”，允许将来自任何源的流量转发到接收方。共享树上的组播状态称为(\*,G)状态，其中\*是ANY SOURCE的通配符。此外，PIM-SM还支持创建与来自特定源的流量相关的状态。这些状态称为源树，相关联的状态称为(S, G)状态。

## 源特定组播

SSM是接收器（或某些代理）发送(S, G)“加入”以指示其希望接收由源S发送到组G的流量时使用的模型。这可以通过IGMPv3/MLDv2“INCLUDE”模式成员身份报告实现。此模型称为源特定组播(SSM)模型。SSM要求在路由器之间使用显式连接协议。其标准协议是PIM-SSM，它只是用于创建(S, G)树的PIM-SM的子集。SSM中没有共享树(\*,G)状态。

组播接收器因此可以“加入”ASM组G，或“加入”（或更准确地“订阅”到）SSM(S, G)信道。为了避免重复术语“ASM组或SSM通道”，使用术语（组播）流，这意味着流可以是ASM组或SSM通道。

## 相关组播协议/数据包类型

要保护组播网络，必须了解常见的数据包类型以及如何防范它们。需要考虑的主要协议有三种：

1. IGMP/MLD
2. PIM
3. MSDP

下一节将分别讨论这些协议的每种以及每种协议可能产生的问题。

## IGMP/MLD数据包

IGMP/MLD是组播接收器使用的协议，用于向路由器发出信号，表示他们希望接收特定组播组的内容。互联网组成员协议(IGMP)是IPv4中使用的协议，组播侦听程序发现(MLD)是IPv6中使用的协议。

通常部署的IGMP有两个版本：IGMPv2和IGMPv3。一般部署的MLD也有两个版本：MLDv1和MLDv2。

IGMPv2和MLDv1在功能上是等价的，而IGMPv3和MLDv2在功能上是等价的。

这些协议在以下链接中指定：

IGMPv2:[RFC 2236](#)

MLDv1:[RFC 3590](#)

IGMPv3和MLDv2:[RFC 4604](#)

IGMPv2和IGMPv3不仅是协议，也是IPv4 IP协议（具体来说，是协议号2）。它不仅按照这些RFC中的说明用于报告组播组成员身份，还用于其他IPv4组播协议，例如DVMRP、PIM版本1、mtrace和mrinfo。当您尝试过滤IGMP(例如通过Cisco IOS® ACL)时,记住这一点很重要。在IPv6中，MLD不是IPv6协议；而是使用ICMPv6传输MLD数据包。PIM版本2是IPv4和IPv6中的相同协议类型（协议号103）。

## PIM控制数据包

本节讨论组播和单播PIM控制数据包。讨论了在PIM-SM网络中选择交汇点和控制组到RP分配的自动RP和引导路由器(BSR)。

## 组播PIM控制数据包

组播PIM控制数据包包括：

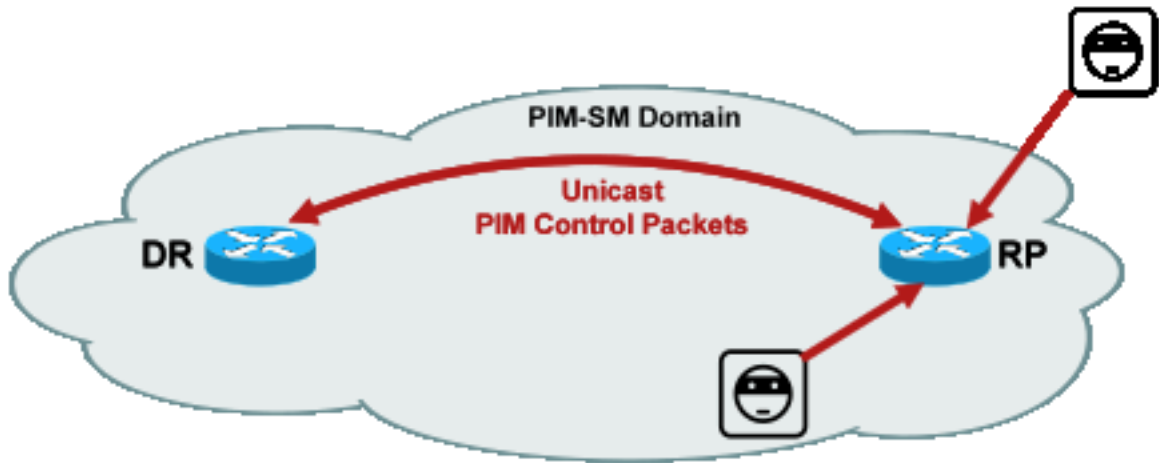
- **PIM Hello** - PIM Hello数据包是本地链路IP组播数据包，发送到连接到同一网络的路由器以建立PIM邻居。
- **PIM加入/修剪** — PIM加入/修剪是本地链路范围IP组播数据包，发送到创建/删除组播状态，并且仅发送到PIM邻居。它们在LAN内进行组播以促进断言、报告抑制和其他PIM协议详细信息，但它们始终指向特定邻居。
- **PIM DF-elect** - PIM Designated Forwarder是Bi-Dir PIM路由器，负责代表连接的接收器或下游PIM邻居向RP发送(\*,G)加入。如果PIM路由器检测到另一台路由器在同一网段上为同一组G发送(\*,G)加入，则会进行选择以确定具有通向RP的最佳路径的路由器。
- **PIM Assert** - PIM Assertion是当连接到网段的PIM路由器开始在转发数据包的同一接口上接收来自特定接口的特定(S, G)数据包时发送的本地链路IP组播数据包。此事件表示有另一台路由器认为自己是此(S, G)的单一转发器(SF)。Assert机制为该(S, G)选择唯一SF。选择PIM SF路由器为特定(S, G)流转发数据包。PIM允许不同的路由器代表不同的(S, G)执行SF角色，理想情况下，每个(S, G)只有一个SF。请勿将SF与指定路由器混淆。PIM指定路由器负责发送到PIM-SM网络中RP的加入/修剪或源寄存器。
- **PIM Bootstrap** - PIM Bootstrap消息在PIMv2网络中发送，以便于为特定组G动态选择交汇点。

## 单播PIM控制数据包

单播PIM控制数据包定向到RP或从RP传出，包括：

- **源注册数据包** — 发送PIM源注册数据包以向交汇点注册新的组播源。一旦源开始发送组播数据包，连接到源网络的指定路由器就会向RP发送单播注册流，以指示存在活动源，用于由RP负责的组播组。  
源寄存器数据包作为原始组播流的单播封装发送。  
PIM注册消息是进程级交换的，并且只在RP发送注册停止消息之前发送。这些数据包的性能影响与源速率(每(S, G)流成正比)。
- **注册停止数据包** — PIM注册停止数据包从交汇点发送到发送注册消息的PIM DR。当RP开始从源本地接收组播数据包时，会立即发送注册停止消息。
- **BSR候选 — 交汇点通告数据包** - PIM BSR C-RP — 通告数据包被发送到BSR，以便在选择BSR后通告候选RP。

图1:PIM单播数据包



图

1\_PIM\_unicast

利用这些数据包的攻击可能来自任何地方，因为这些数据包是单播数据包。

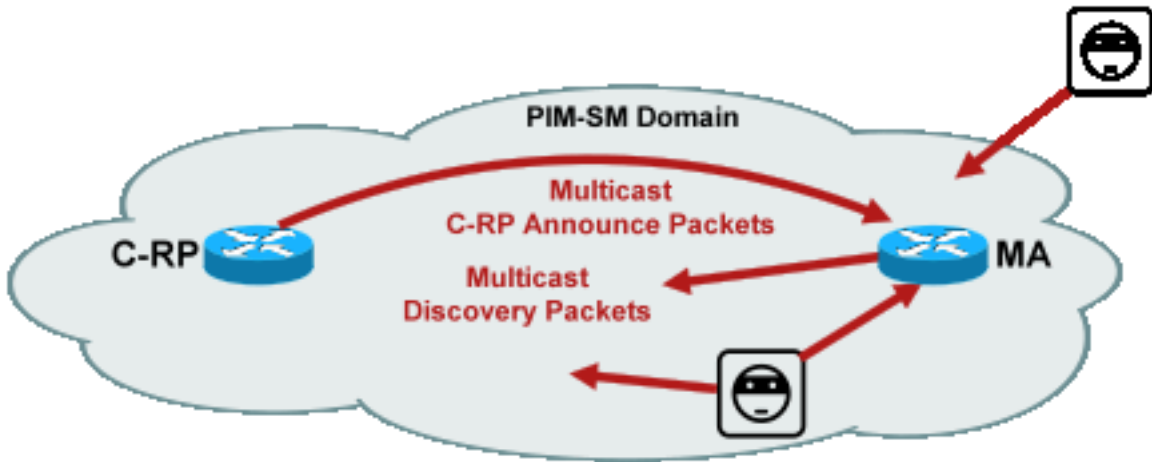
### 自动RP数据包

自动RP是思科开发的协议，其用途与PIMv2 BSR相同。自动RP是在BSR之前开发的，只支持IPv4，支持IPv4和IPv6，自动RP中的映射代理与BSR中的引导路由器功能相同。在BSR中，来自C-RP的消息单播到引导路由器。在自动RP中，消息通过组播发送到映射代理，这样边界处的过滤更加简单，如后所述。自动RP在此链接中详细介绍

: [https://www.cisco.com/c/en/us/td/docs/ios/solutions\\_docs/ip\\_multicast/White\\_papers/rps.html](https://www.cisco.com/c/en/us/td/docs/ios/solutions_docs/ip_multicast/White_papers/rps.html)

在Cisco IOS中，AutoRP/BSR数据包始终被转发，并且当前未被禁用。在自动RP的情况下，这可能带来特定的安全风险。

图2:自动RP数据包



图

2\_AutoRP\_packets

**注意：**即使自动RP用作PIM-SM RP通告和发现的机制，它也不使用PIM数据包（IP协议

103 ) ; 而是使用用户数据报协议(UDP)端口496数据包和组播地址。

自动RP使用两种数据包类型 :

- C-RP-Announce数据包 : 这些数据包组播到所有映射代理 , 并使用互联网编号指派机构 (IANA)保留的“公认”地址(224.0.1.39)。 它们由C-RP发送 , 以通告RP能够充当RP的RP地址和组范围。
- C-RP发现数据包 : 这些数据包组播到所有PIM路由器 , 并使用IANA保留的“公认”地址 (224.0.1.40)。 它们由自动RP映射代理发送 , 以通告选择为特定组范围RP的特定C-RP。

这些数据包类型中的每一种都旨在通过网络泛洪。

在Cisco IOS中 , 224.0.1.39和224.0.1.40都以PIM密集模式转发 , 以避免当组用于分发RP信息时 , 组的RP事先没有信息的问题。这是PIM密集模式的唯一推荐用法。

在Cisco IOS XR中 , 自动RP消息是从邻居到邻居的逐跳反向路径转发(RPF)泛洪消息。因此 , 无需创建PIM DM mroute状态来支持思科IOS XR中的自动RP。事实上 , Cisco IOS XR根本不支持PIM-DM。

## 组播服务发现协议(MSDP)数据包

MSDP是一种IPv4协议 , 它允许一个域中的源通过其各自的交汇点通告给另一个域中的接收器。[RFC 3618](#)中指定了MSDP。

为了在PIM域之间共享有关活动源的信息 , 使用MSDP。如果源在一个域中变为活动状态 , 则MSDP确保所有对等域及时了解此新源 , 这允许其他域中的接收器快速联系此新源 , 如果它恰好被发送到接收器感兴趣的组。ASM/PIM-SM组播通信需要MSDP , 它通过各个域中的交汇点之间配置的单播传输控制协议(TCP)连接运行。

## 组播环境中的威胁

### 信任区域和信任边界

文档的此部分按网络中的功能实体组织。所讨论的威胁模型围绕这些实体形成。例如 , 本文档说明如何保护组播网络中的路由器 ( 从组播的角度而言 ) , 而与路由器的部署位置无关。同样 , 对于如何在指定路由器、交汇点等上部署网络范围的安全措施 , 也有一些注意事项

此处描述的威胁也遵循此逻辑 , 并按网络中的逻辑功能组织。

### 威胁概述

在抽象层上 , 任何组播部署都可能受到各种安全方面的威胁。安全的关键方面是机密性、完整性和可用性。

- **机密性威胁:**在大多数应用中，组播流量不加密，因此任何人都可以侦听或捕获路径中的任何线路或网络元素。在“GET VPN加密组播流量以防止此类攻击的方法”一节中，将会进行讨论。
- **对流量完整性的威胁:**如果没有应用级安全或基于网络的安全性（例如GET VPN），组播流量在传输过程中很容易被修改。这对于使用组播（例如OSPF、PIM和许多其他协议）的控制平面流量尤为重要。
- **网络完整性面临的威胁：**如果没有本文中描述的安全机制，未经授权的发送方、接收方或受感染的网络元素可以访问组播网络、未经授权发送和接收流量（窃取服务）或过载网络资源。
- **可用性威胁:**许多拒绝服务攻击可能使合法用户无法使用资源。

接下来的部分将讨论网络中每个逻辑功能的威胁。

## 路由器面临的基本威胁

路由器面临许多基本威胁，这些威胁与路由器是否支持组播以及攻击是否涉及组播流量或协议无关。

拒绝服务(DoS)攻击是网络中最重要的通用攻击媒介。原则上，每个网络元素都可能遭受DoS攻击，这可能使元素过载，并可能导致合法用户的服务随后丢失或降级。请务必遵循适用于单播的基本网络安全建议。

值得注意的是，组播攻击并非总是故意的，而往往是偶然的。例如，首次在2004年3月观察到的Witty蠕虫就是一种通过对IP地址的随机攻击传播的蠕虫。由于地址空间的完全随机化，多播IP目标也受到蠕虫的影响。在许多组织中，由于蠕虫将数据包发送到许多不同的组播目的地址，许多第一跳路由器崩溃。但是，路由器在相关状态创建时没有针对此类组播流量负载设定范围，并且实际上经历了资源耗尽。这说明即使企业不使用组播，也需要保护组播流量。

针对路由器的常见威胁包括：

- 任何类型的数据包泛洪；例如，针对硬件路径(例如慢速(punt)路径和软件路径（例如管理或控制平面端口），包括安全外壳(SSH)、Telnet、边界网关协议(BGP)、OSPF、网络时间协议(NTP)等
- 入侵路由器，随后利用路由器的功能；弱Telnet或SSH密码和弱简单网络管理协议(SNMP)社区字符串是现代网络中常见的问题。
- 配置错误或内部攻击等操作问题可能会危及整个网络及其流量的安全。

在路由器上启用组播时，除了单播之外，还必须保护组播。使用IP组播不会改变基本的威胁模型；但是，它支持可能受到攻击的其他协议(PIM、IGMP、MLD、MSDP)，这些攻击需要特别保护。当在这些协议中使用单播流量时，威胁模型与路由器运行的其他协议相同。

请注意，组播流量不能以与单播流量相同的方式用于攻击路由器，因为组播流量从根本上来说是“接收器驱动的”，不能以远程目标为目标。攻击目标需要明确“加入”到组播流。在大多数情况下（主要例外是自动RP），路由器仅侦听和接收“本地链路”组播流量。本地链路流量从不转发。因此，对带有组播数据包的路由器的攻击只能来自直接连接的攻击者。



## 来自源端的威胁

组播源（无论是PC还是视频服务器）有时与网络不在相同的管理控制之下。因此，从网络运营商的角度来看，大部分发件人被视为不受信任。考虑到PC和服务器的强大功能及其复杂的安全设置（这些设置往往不完整），发送方对任何网络（包括组播）都构成了严重威胁。这些威胁包括：

- **第2层攻击**：第2层上有多种攻击形式来执行各种类型的攻击。这些适用于单播和组播。由于这些攻击形式并不特定于组播，因此本文档不会更详细地讨论它们。有关详细信息，请参阅Cisco出版社出版的《LAN交换机安全》，ISBN-10:1-58705-467-1的多播地址发送一次邻居消息。
- **使用组播流量的攻击**：如前所述，由于第一跳路由器不会转发组播流量，因此很难使用组播流量进行攻击，除非组具有侦听程序。但是，第一跳可以通过组播数据包以多种方式受到攻击：
- **网络饱和攻击**：攻击者可以过度利用可用带宽，向分段发送组播数据包，从而导致DoS情况。
- **组播状态攻击**：第一跳路由器被组播数据包泛洪，这可能造成过多的状态，从而导致DoS攻击情况。
- 发送方可以通过发送的PIM hello尝试成为PIM DR。在这种情况下，任何流量都不会转发到或来自LAN。
- 可以伪装BiDir-PIM DF的PIM DF选举数据包。在这种情况下，任何流量都不会转发到或来自LAN。
- 发送方可以伪装AutoRP RP发现或BSR引导消息。这将有效通告虚假RP，并关闭或中断PIM-SM/BiDir服务。
- 发送方可能发起单播攻击，例如PIM源注册/注册 — 停止消息，也可能发送BSR通告数据包和通告虚假BSR。
- 发送方可以发送到任何有效的组播组，除非已过滤此组播组。如果源地址在边缘被伪装且未被阻止，则发送方可以使用合法发送方的源IP地址，并覆盖部分网络中的内容。
- **针对控制平面协议的组播攻击**：许多与组播无关的协议（例如OSPF和动态主机配置协议 [DHCP]）使用组播数据包，它们可用于攻击这些协议
- **伪装**：发送方可以伪装成其他发送方的许多攻击形式。欺骗源IP地址就是这种攻击形式。
- **服务失窃**：除非发件人受到控制，否则有可能从发件人非法使用组播服务。

**注意**：主机通常不发送或接收PIM数据包。执行此操作的主机可能会尝试发起攻击。

## 来自接收方的威胁

接收方通常也是具有大量CPU功率和带宽的平台，并且支持多种攻击形式。这些威胁与发送方威胁大致相同。第2层攻击仍然是重要的攻击媒介。在接收端也可能出现假接收器和窃取服务的情况，但攻击矢量通常是IGMP（或如前所述，第2层攻击）。

## 对交汇点和BSR的威胁

PIM-SM RP和PIM-BSR是组播网络中的关键点，因此是攻击者的重要目标。如果第一跳路由器也不是，则仅单播攻击形式（包括PIM单播）可以直接针对这些元素。针对RP和BSR的威胁包括：

- 所有通用攻击形式，如“对路由器的基本威胁”一节所述。

- PIM单播攻击（可能包含伪造的源IP地址）允许DoS攻击，但PIM注册或注册停止消息由恶意设备发送。

## 组播和单播安全（对比）

### 状态注意事项/过滤器

考虑图3中的拓扑，其中显示一个源、三个接收器(A、B、C)、一个交换机(S1)和两个路由器 (R1和R2)。蓝线代表单播流，红线代表组播流。所有三个接收器都是组播流的成员。

图3:路由器和交换机中的复制

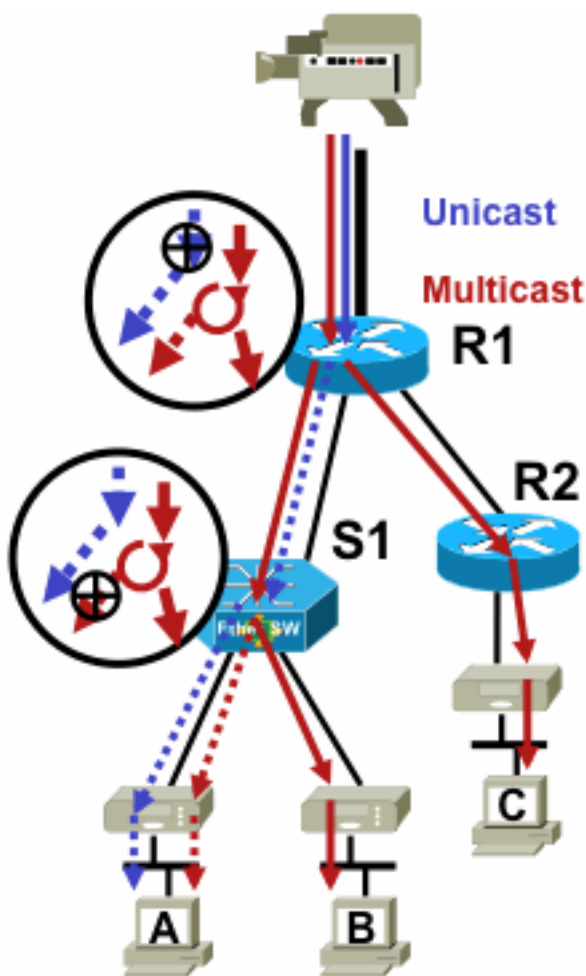


图3\_replication\_RS

要禁止从特定源到特定接收方的流量，请执行以下操作：

- 对于单播流，在从发送方到接收方的路径上的任意位置安装过滤器。
- 但是，对于组播流，管理员需要对安装过滤器的位置进行更详细的规定：在接收端经过最后复制点后的过滤器在接收端之前；在源端过滤源之后的第一个复制点之前。

### 来自组播源的攻击

本节适用于ASM和SSM服务模型，其中根据接收方端显式联接的接收来转发流量。

对于单播流，没有隐式接收器保护。单播源可以将流量发送到目的地，即使该目的地没有请求流量。因此，防火墙等防御机制通常用于保护端点。另一方面，组播具有一些内置于协议中的隐式保护。理想情况下，流量只能到达已加入相关流量的接收器。

使用ASM，源可以通过向活动RP所支持的任何组传输组播流量，从而发起流量插入或DoS攻击。理想情况下，此流量不会到达接收方，但至少可以到达路径中的第一跳路由器，也可以到达RP（允许有限攻击）。但是，如果恶意源知道目标接收方感兴趣的组，并且如果没有适当的过滤器，则可以将流量发送到该组。只要接收方监听的组，就会收到此流量。

使用SSM时，不需要的源发起攻击只能在第一跳路由器上发生，如果没有接收方加入该(S, G)信道，流量会在第一跳路由器上停止。这不会导致第一跳路由器受到任何状态攻击，因为它会丢弃接收器中不存在显式加入状态的所有SSM流量。在此模型中，恶意源仅知道目标对哪个组感兴趣是不够的，因为“联合”是源特定的。在这里，需要伪装的IP源地址加上潜在的路由攻击才能成功。

## 状态攻击

即使网络中没有接收器，PIM-SM也会在最靠近源的第一跳路由器以及交汇点上创建(S, G)和(\*,G)状态。因此，可能存在对源第一跳路由器和PIM-SM RP上的网络的状态攻击。

如果恶意源开始向多个组发送流量，则对于检测到的每个组，处于网络的路由器会在源和RP处创建状态，前提是相关组由RP配置允许。

因此，PIM-SM会受到源和流量攻击。如果源地址在正确的前缀内随机更改其源IP地址，或者换句话说，仅欺骗地址的主机位，则攻击可能加剧。

### 图4:ASM RP攻击



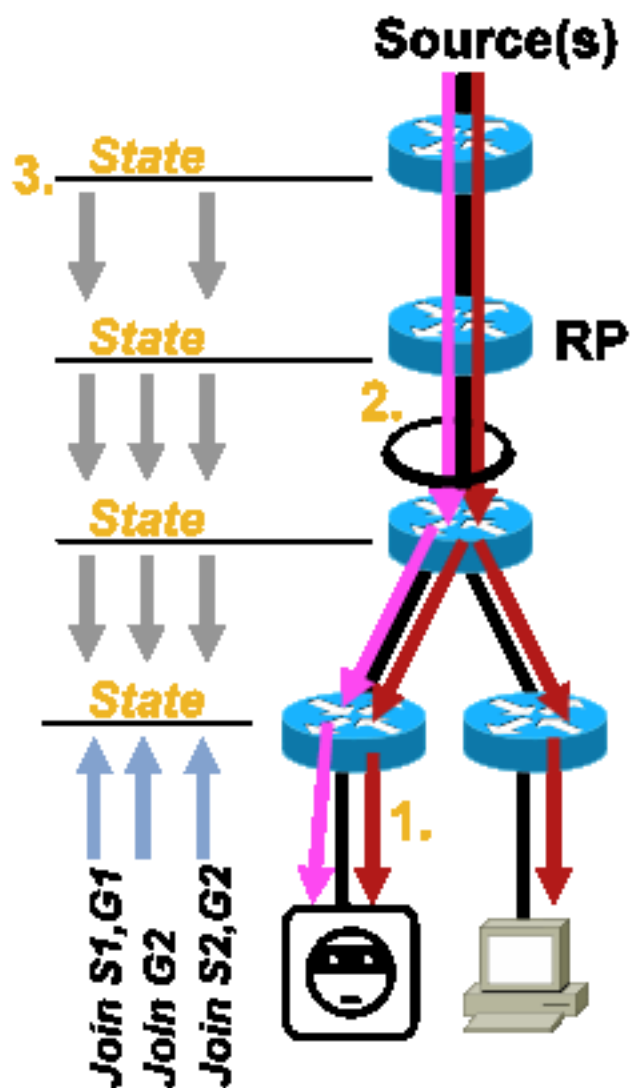


图5\_Receiver\_Explicit\_Join

接收器攻击可以分为三种类型：

1. 组播接收方可以尝试加入其未授权的流，并尝试接收其未授权接收的内容。
2. 组播接收器可能会通过关注许多组或信道来过载可用网络带宽。这种攻击成为针对其他潜在内容接收方的共享带宽攻击。
3. 组播接收器可能会尝试对路由器或交换机发起攻击。可以生成大量IGMP报告，从而产生大量的组播树状态和潜在的路由器过载。这反过来又会导致组播收敛时间延长，或者导致路由器上的DoS增加。

缓解此类攻击的各种方法将在下一节“组播网络中的安全性”中介绍。

## 组播网络中的安全性

### 网元安全

安全不是单点功能，而是每个网络设计的固有部分。因此，必须在网络的每个点考虑安全性。每个网络元素都必须得到适当的保护，这一点至关重要。一种可能的攻击场景是路由器被入侵者破坏

，适用于任何技术。一旦入侵者控制了路由器，攻击者就可以运行许多不同的攻击场景。因此，每个网络元素都必须适当地受到保护，以免受任何形式的基本攻击和特定组播攻击。

## 控制层面策略 (CoPP)

CoPP是路由器ACL(rACL)的发展，在大多数平台上可用。原理是相同的：CoPP仅管制发往路由器的流量。

服务策略使用与任何服务质量策略相同的语法，包括策略映射和类映射。因此，它使用速率限制器扩展了rACL（允许/拒绝）的功能，以限制流向控制平面的特定流量。

**注意：**某些平台（例如Catalyst 9000系列交换机）默认启用了CoPP，且保护不会被取代。有关其他信息，请参阅[CoPP指南](#)。

如果您决定在实际网络中调整、修改或创建rACL或CoPP，请务必小心。由于这两个功能都能过滤到控制平面的所有流量，因此必须明确允许所有所需的控制平面和管理平面协议。所需协议的列表非常庞大，很容易忽略不太明显的协议，例如终端访问控制器访问控制系统(TACACS)。所有非默认rACL和CoPP配置在部署到生产网络之前，必须始终在实验室环境中进行测试。此外，初始部署只需从“允许”策略开始。这允许使用ACL命中计数器验证任何意外命中。

在组播环境中，必须在rACL或CoPP中允许所需的组播协议（PIM、MSDP、IGMP等），组播才能正常工作。请务必记住，来自PIM-SM场景中的源的组播流中的第一个数据包用作控制平面数据包，以帮助创建组播状态（位于设备的控制平面）。因此，在rACL或CoPP中允许相关组播组非常重要。由于存在许多特定于平台的例外，因此在部署之前必须查阅相关文档并测试任何计划的配置。

## 本地数据包传输服务(LPTS)

在Cisco IOS XR上，本地数据包传输服务(LPTS)充当到路由器控制平面的流量的监察器，类似于Cisco IOS上的CoPP。此外，接收流量（包括单播和组播流量）可以过滤并限制速率。

## 组播特定的安全

在启用组播的网络中，每个网络元素都需要使用组播特定的安全功能进行保护。本部分概述了这些功能，用于通用路由器保护。并非每台路由器都要求具备的功能，但仅限于网络中的特定位置，以及需要路由器之间交互（例如PIM身份验证）的功能，将在下一节讨论。

## Mroute限制

mroute limit命令可限制路由器上全局组播路由的数量，并有助于防止DoS攻击。

```
ip multicast route-limit <mroute-limit> <warning-threshold>
```

### 图6:Mroute限制

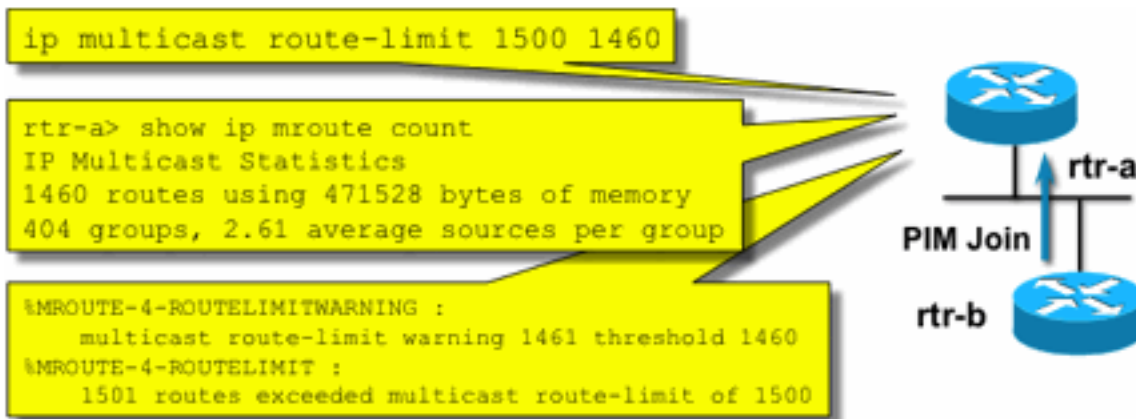


图6\_Mroute\_Limits

Mroute限制允许设置组播路由表中允许的路由数量的阈值。如果启用了组播路由限制，则不会创建超出配置限制的组播状态。还有一个警告阈值。当路由数量超过警告阈值时，系统会触发系统日志警告消息。在mroute limit处，会丢弃任何会触发状态的其他数据包。

ip multicast route-limit命令也可用于每个MVRP。

### 禁用SAP侦听：no ip sap listen

sap listen命令使路由器接收会话通告协议/会话描述协议(SAP/SDP)消息。SAP/SDP是一种传统协议，从组播主干(MBONE)的日期起生效。这些消息指示未来或当前可用的有关组播内容的目录信息。这可能是针对路由器CPU和内存资源的DoS源，因此需要禁用此功能。

### 控制对mrinfo信息的访问 — “ip multicast mrinfo-filter”命令

mrinfo命令（在Cisco IOS以及Microsoft Windows和Linux的某些版本上提供）使用各种消息查询组播路由器以获取信息。ip multicast mrinfo-filter全局配置命令可用于限制对源子集的此信息的访问，或者完全禁用此信息。

此示例拒绝来自192.168.1.1的查询，而允许来自任何其他来源的查询：

```
ip multicast mrinfo-filter 51

access-list 51 deny 192.168.1.1
access-list 51 permit any
```

此示例拒绝 mrinfo 来自任何来源的请求：

```
ip multicast mrinfo-filter 52

access-list 52 deny any
```

**注意：**与任何ACL的预期一样，deny表示过滤数据包，permit表示允许该数据包。

如果将mrinfo命令用于诊断目的，则强烈建议使用适当的ACL配置ip multicast mrinfo-filter命令，以便仅允许从源地址的子集进行查询。mrinfo命令提供的信息也可以通过SNMP检索。强烈建议使用完整的mrinfo请求块（阻止来自设备查询的任何源）。

# 网络安全

本节讨论保护PIM组播和单播控制数据包以及自动RP和BSR的各种方法。

## 禁用组播组

`ip multicast group-range/ipv6 multicast group range`命令可用于禁用被ACL拒绝的组的所有操作：

```
ip multicast group-range <std-acl>
ipv6 multicast group-range <std-acl>
```

如果ACL拒绝的任何组显示数据包，则这些数据包在所有控制协议（包括PIM、IGMP、MLD和MSDP）中都会被丢弃，并且也会被丢弃在数据平面上。因此，不会为这些组范围创建IGMP/MLD缓存条目、PIM、组播路由信息库/组播转发信息库(MRIB/MFIB)状态，并且所有数据包都会立即丢弃。

这些命令在设备的全局配置中输入。

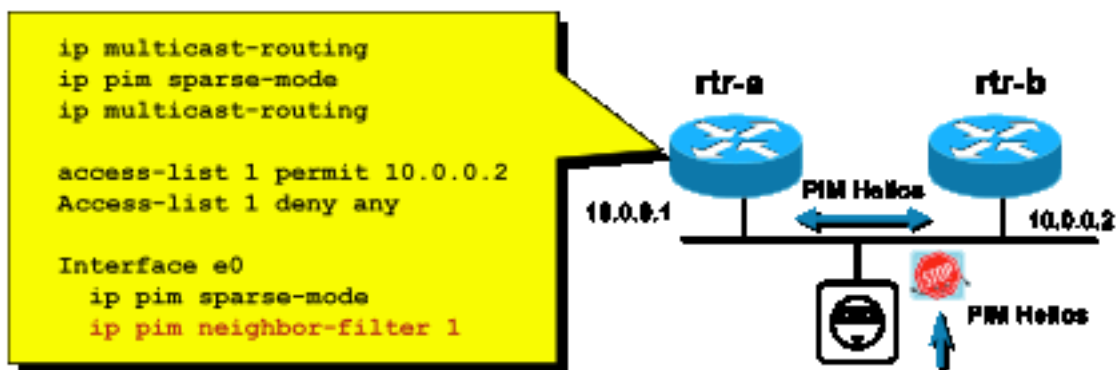
建议在网络中的所有路由器上部署此命令，以便控制源自网络外部的所有组播流量。请注意，这些命令会影响数据平面和控制平面。如果可用，此命令提供的覆盖范围比标准ACL更广泛，因此是首选命令。

## PIM安全

### PIM邻居控制

PIM路由器必须收到PIM Hello才能建立PIM邻居关系。PIM邻居关系也是指定路由器(DR)选举和DR故障切换以及发送/接收PIM加入/修剪/断言消息的基础。

图7:PIM邻居控制



图

7\_PIM\_neighbor\_control

要阻止不需要的邻居，请使用 `ip pim neighbor-filter` 命令，如图7所示。此命令过滤所有不允许的邻居PIM数据包，包括Hello、加入/修剪数据包和BSR数据包。网段上的主机可能会伪装成源IP地址的PIM邻居。需要第2层安全机制（即IP源保护）来防止源地址在网段上伪装尝试，或在接入交换机中使用VLAN ACL来防止来自主机的PIM数据包。关键字“log-input”可在ACL中用于记录与ACE匹配的数据包。



PIM加入/修剪数据包被发送到PIM邻居，以添加或从特定(S, G)或(\*,G)路径中删除该邻居。PIM组播数据包是发送了生存时间(TTL)=1的链路本地组播数据包。所有这些数据包都组播到众所周知的全PIM路由器地址：224.0.0.13 的多播地址发送一次邻居消息。这意味着所有此类攻击必须与受攻击的路由器位于同一子网上。攻击可能包括伪造的Hello、加入/修剪和断言数据包。

**注意：**将PIM组播数据包中的TTL值人为增加或调整为大于1的值不会产生问题。所有PIM路由器地址始终在路由器上接收并本地处理。它绝不会由正常和合法路由器直接转发。

为了保护RP免受潜在的PIM-SM注册消息泛洪的影响，DR需要限制这些消息的速率。使用`ip pim register-rate-limit`命令：

```
ip pim register-rate-limit <count>
```

图8:PIM-SM寄存器隧道控制

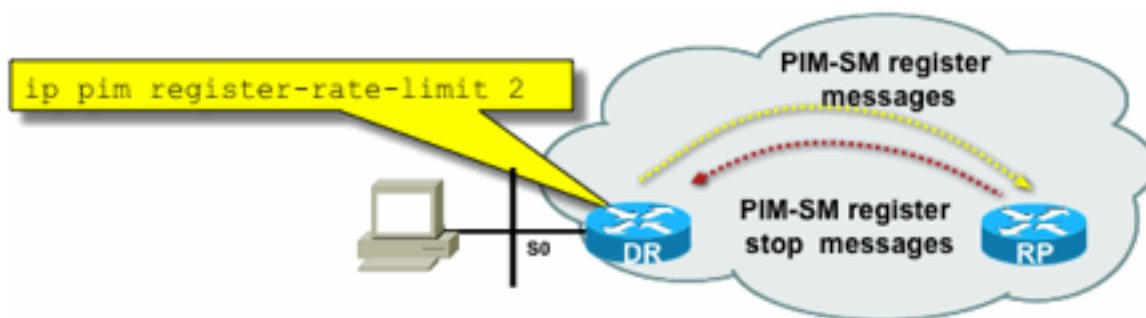


Fig8\_PIMSM\_Reg

Tunnel

PIM单播数据包可用于攻击RP。因此，基础设施ACL可以保护RP免受此类攻击。请记住，组播发送方和接收方永远不需要发送PIM数据包，因此PIM协议（IP协议103）通常可以在用户边缘过滤。

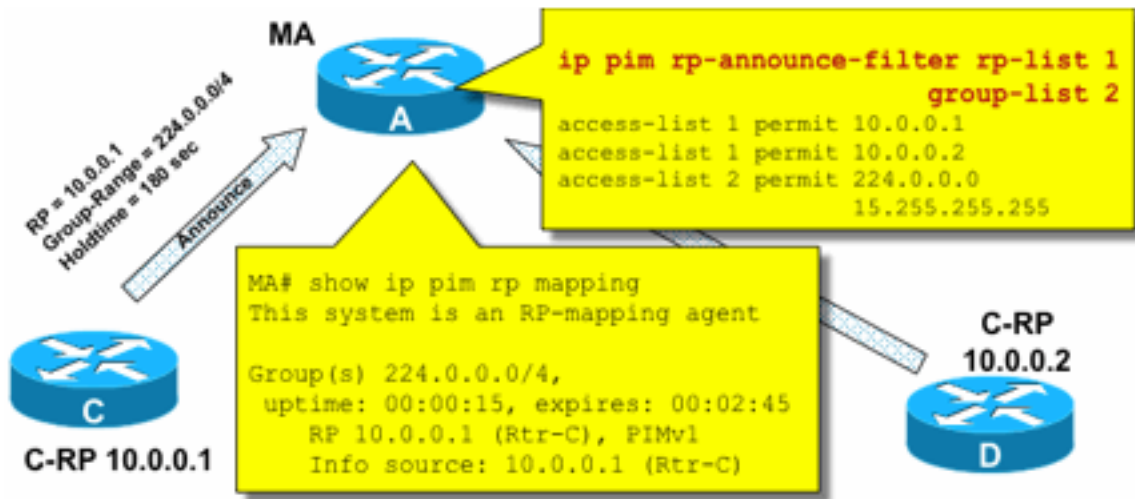
### 自动RP控制 — RP通告过滤器

`ip pim rp-announce filter`命令是附加的安全措施，可以尽可能使用自动RP进行配置：

```
ip pim rp-announce-filter
```

这可以在映射代理上配置，以控制哪些路由器被接受为哪个组范围/组模式的候选RP。

图9:自动RP - RP通告过滤器



图

9\_AutoRP\_RP\_Announce

## 自动RP控制 — 限制自动RP消息

使用multicast boundary命令将自动RP数据包、RP通告(224.0.1.39)或RP发现(224.0.1.40)限制到特定PIM域：

```
ip multicast boundary
```

图10:组播边界命令

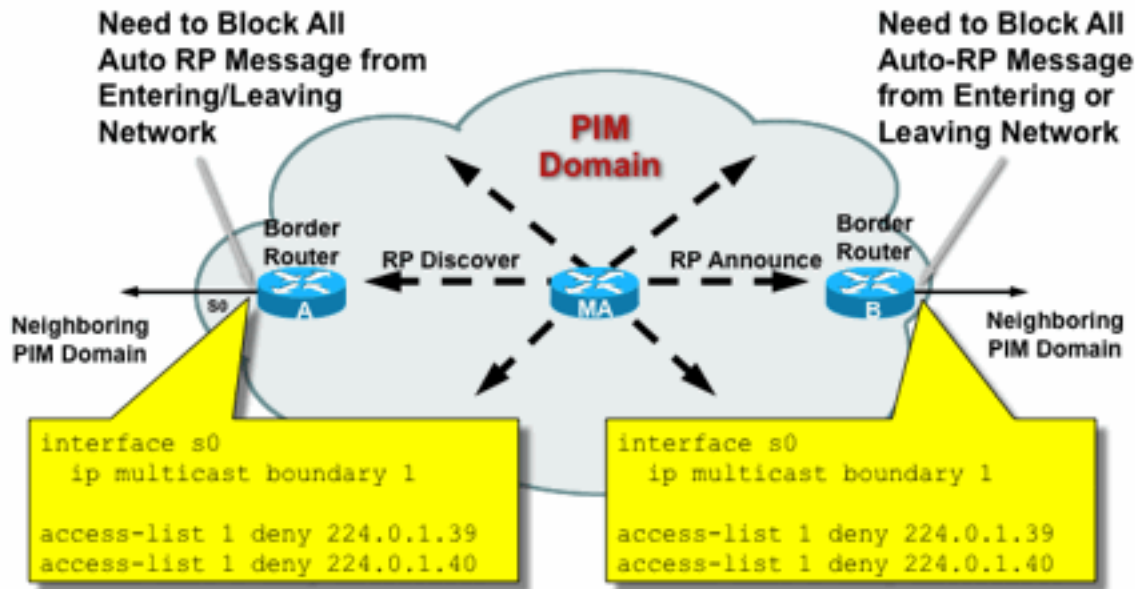


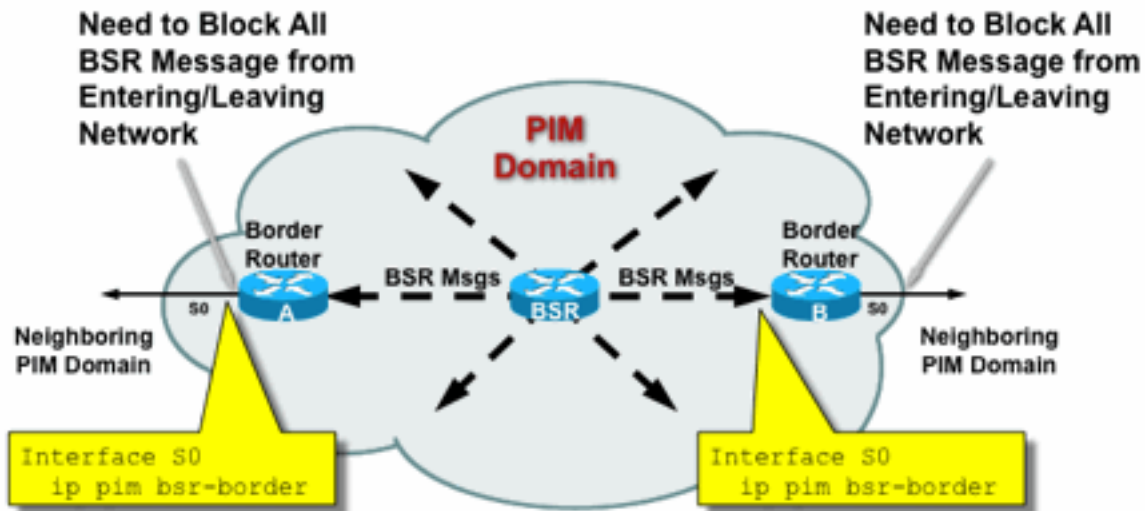
Fig10\_Mcast\_Boun

dary

### BSR控制 — 限制BSR消息

请使用 `ip pim bsr-border` 命令过滤PIM域边界的BSR消息。无需ACL，因为BSR消息会逐跳转发到本地链路组播。

图11:BSR边界



图

11\_BSR\_Router

### RP/PIM-SM相关过滤器

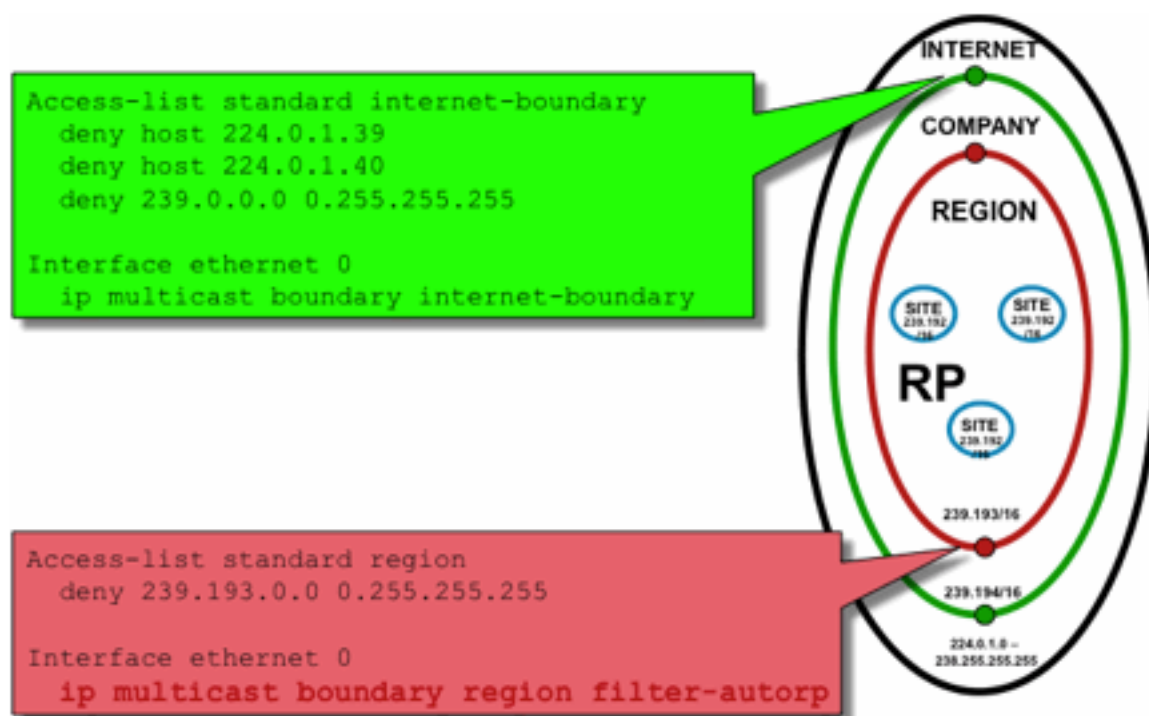
在最后一节中，将讨论针对PIM-SP和RP控制平面数据包以及自动RP、BSR和MSDP消息的过滤器。

。

## 自动RP过滤器

图12显示了结合地址范围的自动RP过滤器的示例。显示了两种不同的绑定区域的方法。从自动RP的角度来看，两个ACL是等效的。

图12:自动RP过滤器/范围



图

12\_AutoRP\_Filtering\_Scope

自动RP的接口边界过滤器的理念是确保自动RP通告仅到达它们支持的区域。定义了区域、公司和互联网范围，并且每种情况下在每个范围中都存在RP和自动RP通告。管理员只希望区域路由器知道区域RP，区域和公司路由器知道公司RP，并且希望所有互联网RP都全局可用。范围可以进一步扩展。

如图所示，过滤自动RP数据包有两种基本不同的方式：互联网边界明确调用自动rp控制组（224.0.1.39和224.0.1.40），这导致对所有自动RP数据包进行过滤。此方法可在管理域的边缘使用，在该域中没有通过自动RP数据包。区域边界使用filter-auto-rp关键字来检查自动RP数据包中的rp-to-group-range通告。当ACL明确拒绝通告时，会在转发数据包之前将其从自动RP数据包中删除。在示例中，这允许在整个区域内知道企业范围的RP，而在从区域到企业其余部分的边界处过滤整个区域范围的RP。

## 域间过滤器和MSDP

在本示例中，ISP1充当PIM-SM传输提供商。它们仅支持与邻居的MSDP对等，并且它们仅接受(S,G)，但不接受(\*,G)边界路由器上的流量。

在域间（通常在自治系统之间）要采取两种基本安全措施：

1. 通过**multicast boundary**命令保护数据平面。这可确保组播流量仅被定义的组（以及可能的源）接受。
2. 保护域间控制平面流量(MSDP)。这包括一系列单独的安全措施：MSDP内容控制、状态限制和邻居身份验证。

图13提供了在ISP1的边界路由器上配置接口过滤器的示例。

要在域边界保护数据平面，请通过**multicast boundary**命令针对主机0.0.0.0和管理范围地址通过过滤器阻止(\*,G)加入：

图13:域间(\*,G)过滤器

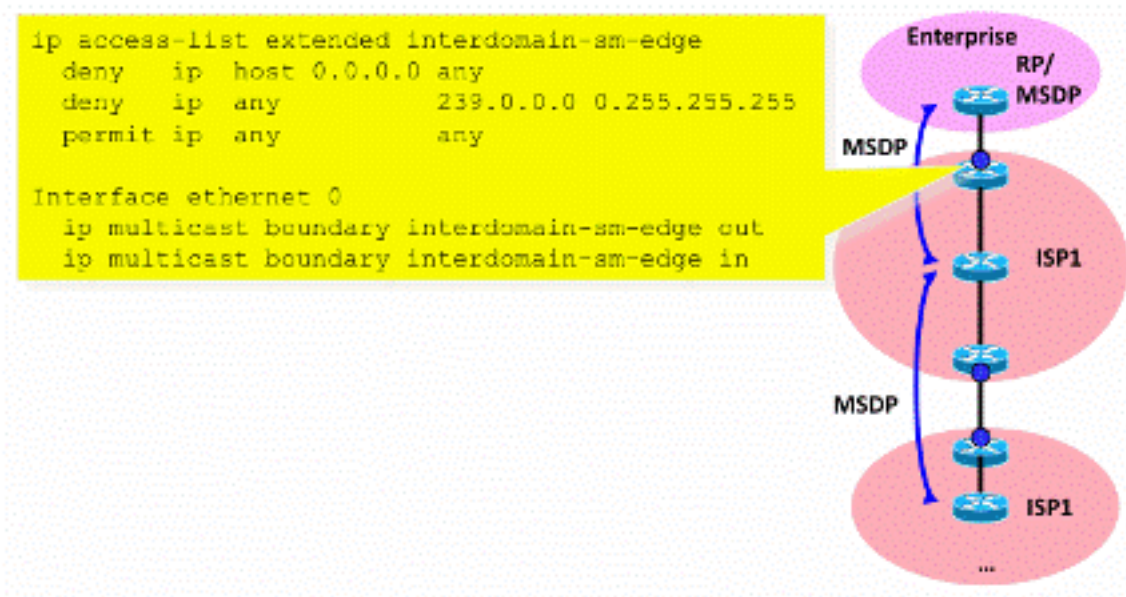


图13\_域间过滤器

要保护控制平面，请通过三个基本安全措施强化MSDP:

### 1)MSDP SA过滤器

通过MSDP SA过滤器过滤MSDP消息的内容是“最佳惯例”。此过滤器的主要思想是避免组播状态传播到不是互联网范围的应用和组，并且不需要转发到源域之外。理想情况下，从安全角度来看，过滤器仅允许已知组（以及潜在的发件人），并拒绝任何未知发件人和/或组。

通常无法明确列出所有允许的发件人和/或组。建议对每个组使用单个RP的PIM-SM域使用默认配置过滤器（无MSDP网状组）：

```

!--- Filter MSDP SA-messages.
!--- Replicate the following two rules for every external MSDP peer.
!
ip msdp sa-filter in <peer_address> list 111
ip msdp sa-filter out <peer_address> list 111
!
  
```

```

!--- The redistribution rule is independent of peers.
!
ip msdp redistribute list 111
!
!--- ACL to control SA-messages originated, forwarded.
!
!--- Domain-local applications.
access-list 111 deny ip any host 224.0.2.2 !
access-list 111 deny ip any host 224.0.1.3 ! Rwhod
access-list 111 deny ip any host 224.0.1.24 ! Microsoft-ds
access-list 111 deny ip any host 224.0.1.22 ! SVRLOC
access-list 111 deny ip any host 224.0.1.2 ! SGI-Dogfight
access-list 111 deny ip any host 224.0.1.35 ! SVRLOC-DA
access-list 111 deny ip any host 224.0.1.60 ! hp-device-disc
!--- Auto-RP groups.
access-list 111 deny ip any host 224.0.1.39
access-list 111 deny ip any host 224.0.1.40
!--- Scoped groups.
access-list 111 deny ip any 239.0.0.0 0.255.255.255
!--- Loopback, private addresses (RFC 6761).
access-list 111 deny ip 10.0.0.0 0.255.255.255 any
access-list 111 deny ip 127.0.0.0 0.255.255.255 any
access-list 111 deny ip 172.16.0.0 0.15.255.255 any
access-list 111 deny ip 192.168.0.0 0.0.255.255 any
!--- Default SSM-range. Do not do MSDP in this range.
access-list 111 deny ip any 232.0.0.0 0.255.255.255
access-list 111 permit ip any any !

```

建议尽可能严格地过滤入站和出站方向。

有关MSDP SA过滤器建议的详细信息，请参阅：<https://www.cisco.com/c/en/us/support/docs/ip/ip-multicast/13717-49.html>

## 2)MSDP状态限制

当在多个自治系统(AS)之间启用MSDP时，建议限制由于从邻居接收的“源 — 活动”(SA)消息而在路由器中建立的状态量。您可以使用`ip msdp sa-limit`命令：

```
ip msdp sa-limit <peer> <limit>
```

图14:MSDP控制平面

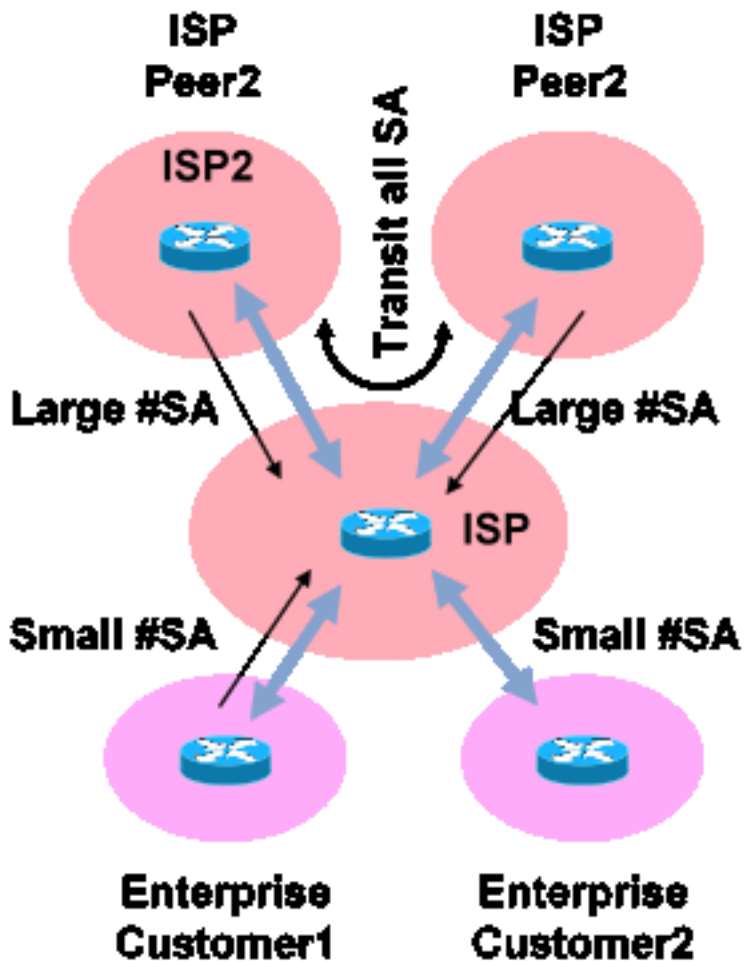


图14\_MSDP\_ControlPlane

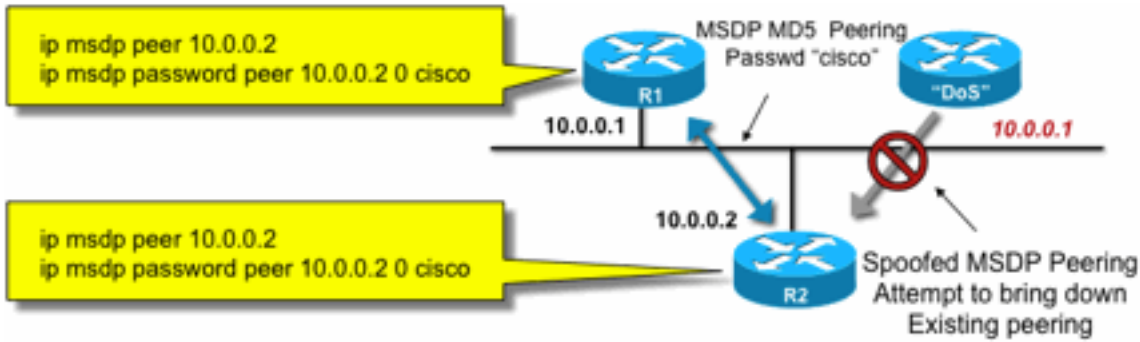
使用ip msdp sa-limit命令可以限制由于从MSDP对等体接收的SA消息而创建的SA状态的数量。一些简单的经验法则建议包括：

- 来自末节邻居的小限制
- 来自传输邻居的大限制(例如Internet中#SAs最大限制)
- 中转ISP — 配置您的平#SAs可支持的最大数量

### 3)MSDP MD5邻居身份验证

建议在MSDP对等设备上使用消息摘要算法(MD5)密码身份验证。这使用TCP MD5签名选项，等同于[RFC 6691](#)中所述的用于保护BGP的选项。

图15:MSDP MD5邻居身份验证



图

15\_MSDP\_MD5Auth

这三个MSDP安全建议追求不同的目标：

- 邻居身份验证（使用MD5）确保只有受信任的MSDP对等体才能发送消息。
- SA过滤器可确保即使受信任的MSDP对等也只能发送符合预先商定的源/组策略的SA通告。
- SA限制进一步确保即使有来自合法对等体的合法(S, G)通告，可用内存也无法耗尽。

## 发件人/源问题

通过适当的单播安全机制，可以缓解源自发送方的许多组播安全问题。下面是推荐的一些单播安全机制：

- **源地址欺骗保护**（接入层的单播逆向路径转发、uRPF或ACL和IP源保护）
- **基础设施ACL**(deny ip any(to)<core address space>)

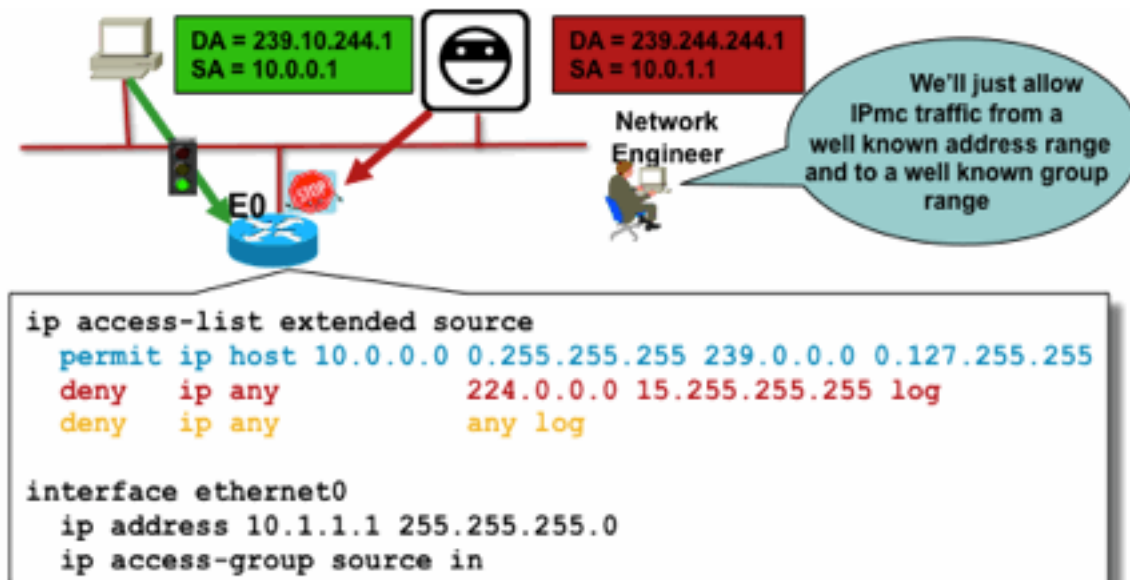
此类措施可用于阻止对核心的定向攻击。例如，这还可以解决使用PIM单播数据包到RP的攻击等问题，RP位于网络的“内部”，因此受基础设施ACL保护。

## 基于数据包过滤器的访问控制 — 控制源

在图16所示的示例中，过滤器是在第一跳组播路由器（指定路由器）的LAN接口(E0)上配置的。过滤器由称为“源”的扩展访问控制列表定义。此ACL应用于连接到源LAN的指定路由器的面向源的接口。事实上，由于组播流量的性质，可能需要在所有面向局域网的接口上配置一个类似的过滤器，源设备可能会变为活动状态。由于不可能在所有情况下都准确知道源活动发生的位置，因此建议对进入网络的所有入口点应用此类过滤器。

图16:控制源





图

## 16\_Controlling\_Sources

此过滤器的目的是防止从特定源地址或源地址范围到特定组或组地址范围的流量。此过滤器在PIM创建任何路由之前起作用，有助于限制状态。

这是标准数据平面ACL。这在高端平台上的ASIC上实施，不会产生性能损失。对于直接连接的源，建议使用数据平面ACL，并且优先于控制平面ACL，因为它们最大限度地减少了不需要的流量对控制平面的影响。限制数据包可以发送到的目标（IP组播组地址）也非常有效。由于这是一个路由器命令，因此它无法克服伪造的源IP地址（请参阅本部分前面部分）。因此，建议为可以连接到特定局域网/虚拟局域网(LAN/VLAN)的所有设备提供额外的第2层(L2)机制或一致的策略。

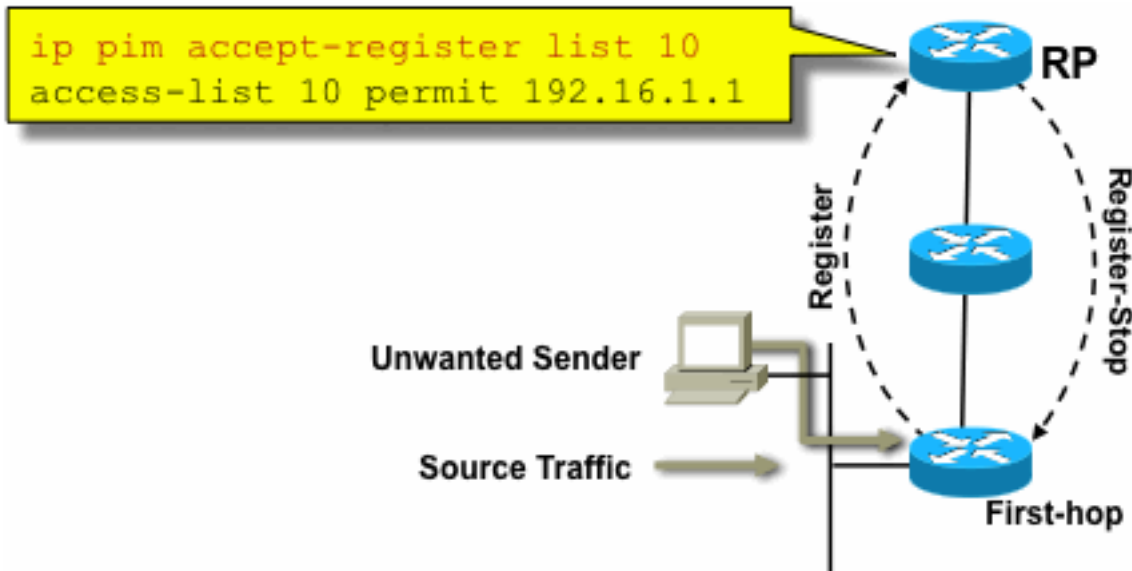
**注意：**ACL中的“log”关键字非常有助于了解针对特定ACL条目的命中情况；但是，这会消耗CPU资源，需要小心处理。此外，在基于硬件的平台上，ACL日志消息由CPU生成，因此必须考虑CPU的影响。

## PIM-SM源控制

从安全角度来看，ASM/PIM-SM架构的实际优势之一是，交汇点为网络中的所有源为任意组范围提供单一的控制点。这可以通过称为accept-register过滤器的设备来实现。此过滤器的命令如下：

```
ip pim accept-register / ipv6 pim accept-register
```

图17:PIM-SM源控制



图

17\_PIMSM\_Control

在PIM-SM网络中，可以使用此命令控制不需要的流量源。当源流量到达第一跳路由器时，第一跳路由器(DR)会创建(S, G)状态，并向RP发送PIM源寄存器消息。如果源未列在accept-register过滤器列表（在RP上配置）中，则RP拒绝注册，并向DR发回立即注册停止消息。

在显示的示例中，简单的ACL已应用到RP，RP仅过滤源地址。也可以在RP上使用扩展ACL过滤源和组。

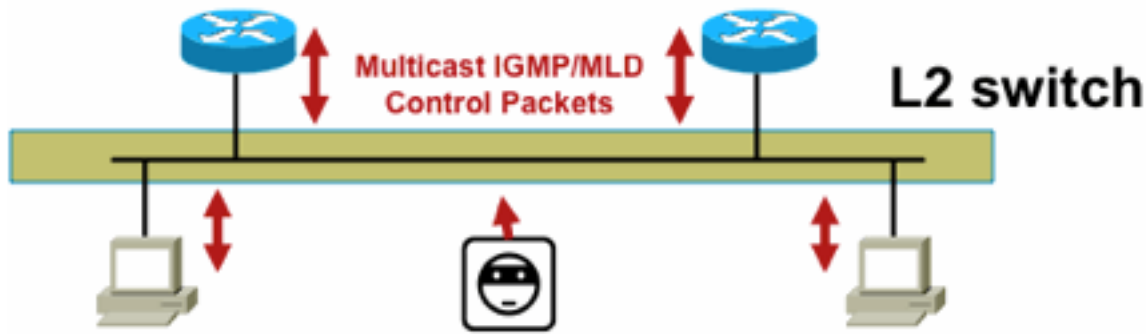
源过滤器有一些缺点，因为在RP上使用pim accept-register命令，仍会在源的第一跳路由器上创建PIM-SM(S, G)状态。这可能导致源本地接收器处的数据流以及源与RP之间的数据流。此外，pim accept-register命令在RP的控制平面上运行。这可用于使用虚假注册消息使RP过载，并可能导致DoS情况。

建议在RP上应用pim accept-register命令，以及其他方法，例如在所有的DR上、所有进入网络的入口点上应用简单的数据平面ACL。虽然DR上的入口ACL在配置完善且运行良好的网络中足够用，但建议在RP上配置pim accept-register命令，作为边缘路由器配置错误时的辅助安全机制。具有相同目标的分层安全机制称为“深度防御”，是安全领域的常见设计原则。

## 接收器问题 — 控制IGMP/MLD

大多数接收器问题属于IGMP/MLD接收器协议交互领域。

图18:控制IGMP



图

18\_Controlling\_IGMP

过滤IGMP或MLD数据包时，请记住以下几点：

- IPv4:IGMP是IPv4协议类型 ( IPv4协议2 )
- IPv6:MLD在ICMPv6协议类型数据包中传输

启用IP组播后，IGMP进程默认启用。IGMP数据包还承载这些协议，因此只要启用组播，就会启用所有这些协议：

- PIMv1 - PIMv1是PIM的第一个版本，在Cisco IOS中始终启用，用于迁移目的。当前部署都使用PIMv2。
- Mrinfo - Mrinfo是Cisco IOS继承的Unix命令，用于显示组播邻居。Cisco建议使用SNMP而不是mrinfo命令。
- DVMRP - DVMRP是一种传统密集模式距离矢量协议，扩展特性非常有限。Cisco IOS对DVMRP的支持已停用或已弃用。
- Mtrace - Mtrace是单播“traceroute”的等价组播协议，是一个非常有用的工具

有关详细信息，[请参阅IANA的互联网组管理协议\(IGMP\)类型编号](#)

```
Router> mtrace 172.16.0.0 172.16.0.10 239.254.254.254
```

Type escape sequence to abort.

Mtrace from 172.16.0.0 to 172.16.0.10 via group 239.254.254.254

From source (?) to destination (?)

Querying full reverse path...

```
0 172.16.0.10
-1 172.16.0.8 PIM thresh^ 0 0 ms
-2 172.16.0.6 PIM thresh^ 0 2 ms
-3 172.16.0.5 PIM thresh^ 0 894 ms
-4 172.16.0.3 PIM thresh^ 0 893 ms
-5 172.16.0.2 PIM thresh^ 0 894 ms
-6 172.16.0.1 PIM thresh^ 0 893 ms
```

单播IGMP数据包 ( 用于IGMP/UDLR ) 可以过滤，因为它们最可能是攻击数据包，而不是有效的IGMP协议数据包。Cisco IOS支持单播IGMP数据包，以支持单向链路和其他异常情况。

伪造的IGMP/MLD查询数据包可导致IGMP版本低于预期。

特别是，理想情况下，主机从不发送IGMP查询，因为用较低的IGMP版本发送的查询可能导致收到此查询的所有主机恢复到较低版本。在IGMPv3/SSM主机存在的情况下，这可以“攻击”SSM流。对于IGMPv2，这会导致更长的离开延迟。

如果存在具有单个IGMP查询器的非冗余LAN，路由器需要丢弃收到的IGMP查询。

如果存在冗余/通用被动LAN，则需要能够进行IGMP监听的交换机。在这种情况下，有2个特定功能可以帮助：

- 路由器防护
- IGMP最低版本命令

### 路由器防护

如果交换机在该端口上收到组播路由器控制数据包（IGMP通用查询、PIM Hello或CGMP Hello），则任何交换机端口都可以成为组播路由器端口。当交换机端口成为组播路由器端口时，所有组播流量都会发送到该端口。这可以通过“路由器防护”加以阻止。路由器防护功能不需要启用IGMP监听。

路由器防护功能允许将指定的端口指定为组播主机端口。即使收到组播路由器控制数据包，该端口也不能成为路由器端口。

如果在启用路由器防护的端口上收到以下数据包类型，则丢弃这些数据包：

- IGMP查询消息
- IPv4 PIMv2消息
- IGMP PIM消息(PIMv1)
- IGMP DVMRP消息
- 路由器端口组管理协议(RGMP)消息
- 思科组管理协议(CGMP)消息

当丢弃这些数据包时，会更新统计信息，指示由于路由器防护而丢弃数据包。

### IGMP最低版本

可以配置允许的IGMP主机的最低版本。例如，您可以禁止所有IGMPv1主机或所有IGMPv1和IGMPv2主机。此过滤器仅适用于成员身份报告。

如果主机连接到一个通用的“被动”LAN（例如，不支持IGMP监听的交换机，或者没有针对它进行配置），则路由器除了忽略随后触发的“旧版本”成员身份报告而无法执行此类错误查询之外，也不能自行执行其他操作。

由于IGMP查询必须对所有主机可见，因此不能使用具有预共享密钥(例如静态密钥IPSec)的基于哈希的消息身份验证(HMAC)机制来验证来自“有效路由器”的IGMP查询。如果两个或多个路由器连接到一个通用LAN网段，则需要选举IGMP查询器。在这种情况下，唯一可以使用的过滤器是ip access-group filter，它基于发送查询的其他IGMP路由器的源IP地址。

必须允许“正常”组播IGMP数据包。

此过滤器可用于接收器端口，以仅允许“正常”IGMP数据包，并过滤已知的“不良”数据包：

```
ip access-list extended igmp-control
<snip>
deny igmp any any pim ! No PIMv1
deny igmp any any dvmrp ! No DVMRP packets
deny igmp any any host-query ! Do not use this command with redundant routers.
! In that case this packet type is required !
permit igmp any host 224.0.0.22 ! IGMPv3 membership reports
permit igmp any any 14 ! Mtrace responses
permit igmp any any 15 ! Mtrace queries
```

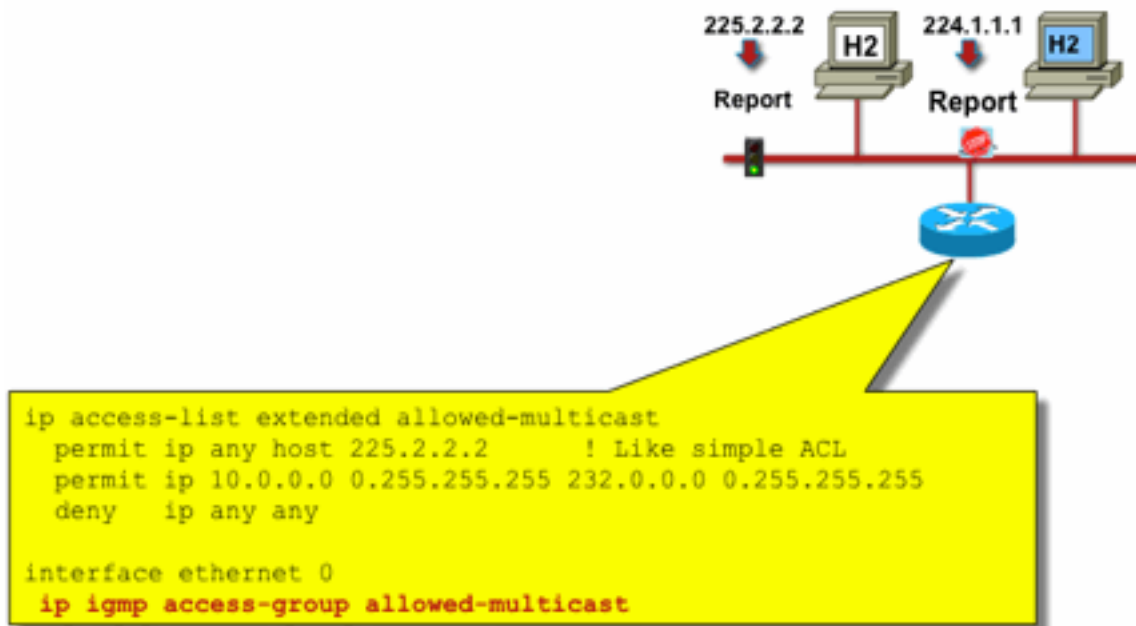
```

permit igmp any 224.0.0.0 10.255.255.255 host-query ! IGMPv1/v2/v3 queries
permit igmp any 224.0.0.0 10.255.255.255 host-report ! IGMPv1/v2 reports
permit igmp any 224.0.0.0 10.255.255.255 7 ! IGMPv2 leave messages
deny igmp any any ! Implicitly deny unicast IGMP here!
<snip> permit ip any any ! Permit other packets interface ethernet 0 ip access-group igmp-
control in

```

**注意：**此类IGMP过滤器可用于接收ACL或CoPP。在这两种应用中，都需要将其与过滤器结合使用，以用于处理其他流量，例如路由和管理平面协议。

**图19:主机接收器端访问控制**



图

19\_Host\_Receiver\_Access

要过滤发往接收方的流量，请勿过滤数据平面流量，而是过滤控制平面协议IGMP。由于IGMP是接收组播流量的必要前提，因此不需要数据平面过滤器。

特别是，您可以限制接收方可以加入的组播流（连接到配置该命令的接口）。在这种情况下，请使用 `ip igmp access-group / ipv6 mld access-group` 命令：

`ip igmp access-group / ipv6 mld access-group`

对于ASM组，此命令仅根据目标地址进行过滤。然后忽略ACL中的源IP地址。对于使用IGMPv3/MLDv2的SSM组，它会过滤源和目标IP。

此示例过滤所有IGMP扬声器的给定组：

```

access-list 1 deny 226.1.0.0 0.0.255.255
access-list 1 permit any log
! interface ethernet 1/3 ip igmp access-group 1

```

此示例过滤给定组的特定IGMP扬声器（因此为特定组播接收器）：

```

ip access-list extended test5

```

```
deny igmp host 10.4.4.4 host 232.2.30.30
permit igmp any any
!
interface Ethernet0/3
 ip igmp access-group test5
```

**注意：**请记住，对于ASM组，将忽略源。

## 准入控制

访问控制为特定流量提供二进制、是或否答案，与网络状态无关。相对而言，准入控制限制了发送方/接收方可以使用的资源数量，假设它们通过了访问控制机制。在组播环境中，可以使用各种设备帮助进行准入控制。

### 全局和每个接口的IGMP限制

在最靠近感兴趣的组播接收器的路由器上，可以限制全局和每个接口加入的IGMP组数量。您可以使用`ip igmp limit/ipv6 mld limit`命令：

```
ip igmp limit <n> [ except <ext-acl> ]
ipv6 mld limit <n> [ except <ext-acl> ]
```

建议始终按接口全局配置此限制。在每种情况下，限制是指IGMP缓存中的条目计数。

接下来的两个示例展示如何使用此命令帮助限制住宅宽带网络边缘的组数量。

#### 示例1 — 将接收组限制为仅包含SDR通告和一个接收信道

会话目录(SDR)用作某些组播接收器的信道指南。有关详细信息，请参阅[RFC 2327](#)。

一个常见要求是限制接收器接收SD组加一个信道。可以使用以下示例配置：

```
ip access-list extended channel-guides
 permit ip any host 239.255.255.254 ! SDR announcements
 deny ip any any
```

```
ip igmp limit 1 except channel-guides
```

```
interface ethernet 0
 ip igmp limit 2 except channel-guides
```

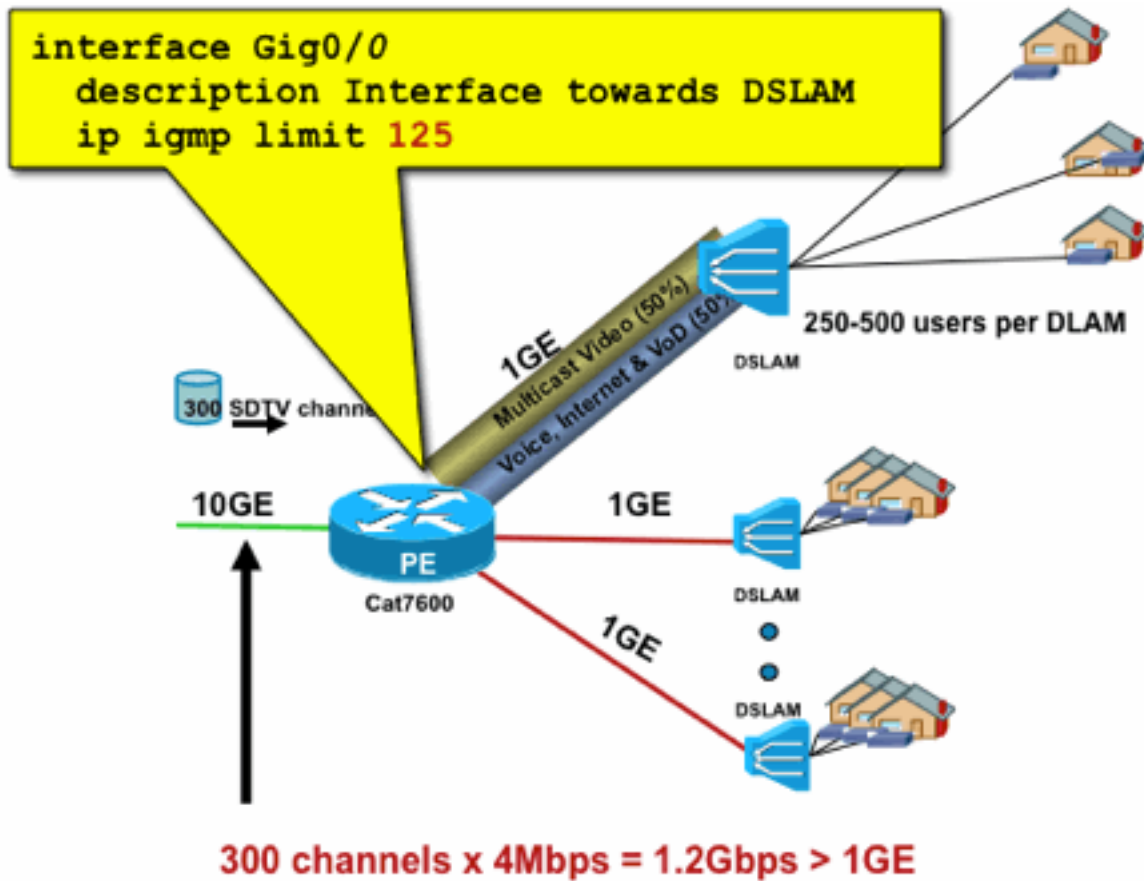
本示例中的访问列表仅指定通道指南；全局`ip igmp limit`命令将每个IGMP源限制为单个(1)通道，但不包括始终可以接收的通道指南。`interface`命令会覆盖全局命令，并且除了通道指南外，还允许在此接口上接收两(2)个通道。

#### 示例2 — 汇聚DSLAM链路上的准入控制

此命令还可用于提供某种形式的带宽准入控制。例如，如果需要分配300个SDTV频道（每个频道4Mbps），并且有1Gbps链路连接到数字用户线路接入复用器(DSLAM)，则您可以做出策略决策，将电视带宽限制为500 Mbps，其余频道留给Internet和其他用途。在这种情况下，您可以将IGMP状态限制为 $500 \text{ Mbps} / 4 \text{ Mbps} = 125$  IGMP状态。

此配置可用于本例：

图20:使用每个接口的IGMP限制；Agg-DSLAM链路上的准入控制



图

20\_PerInterface\_IGMP

## 每个接口的mroute限制

启用每个接口的mroute状态限制是一种更通用的准入控制形式。它不仅在传出接口上限制IGMP和PIM状态，还提供了一种对传入接口进行状态限制的方法。

使用ip multicast limit命令：

```
ip multicast limit [ rpf | out | connected ] <ext-acl> <max>
```

可在输入和输出接口上单独限制状态。直接连接的源状态也可以使用“已连接”关键字进行限制。示例说明了此命令的用法：

### 示例1 - Agg-DSLAM链路上的出口准入控制

在本示例中，有300个SD电视频道。假设每个SD信道需要4 Mbps，总速率不超过500 Mbps。最后，还假设需要支持基本、扩展和高级捆绑包。带宽分配示例：

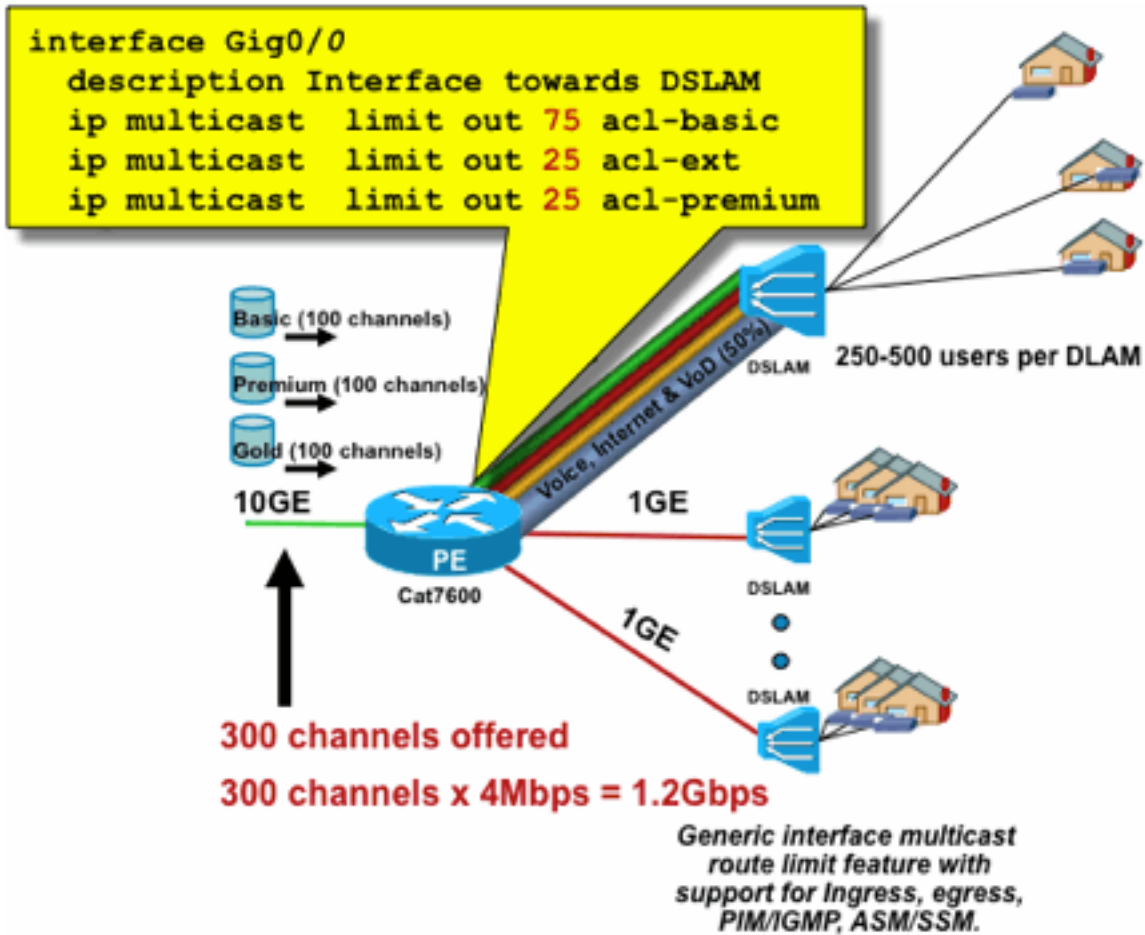
- 60% / 300 Mbps基本
- 20% / 100 Mbps扩展
- 20% / 100 Mbps高级版

然后每个信道使用4 Mbps，将DSLAM上行链路限制为：

- 基本75个状态
- 扩展25个状态
- 高级版25状态

配置从PEAgg面向DSLAM的出站接口限制：

图21:使用每个接口的mroute限制；Agg-DSLAM链路路上的准入控制



图

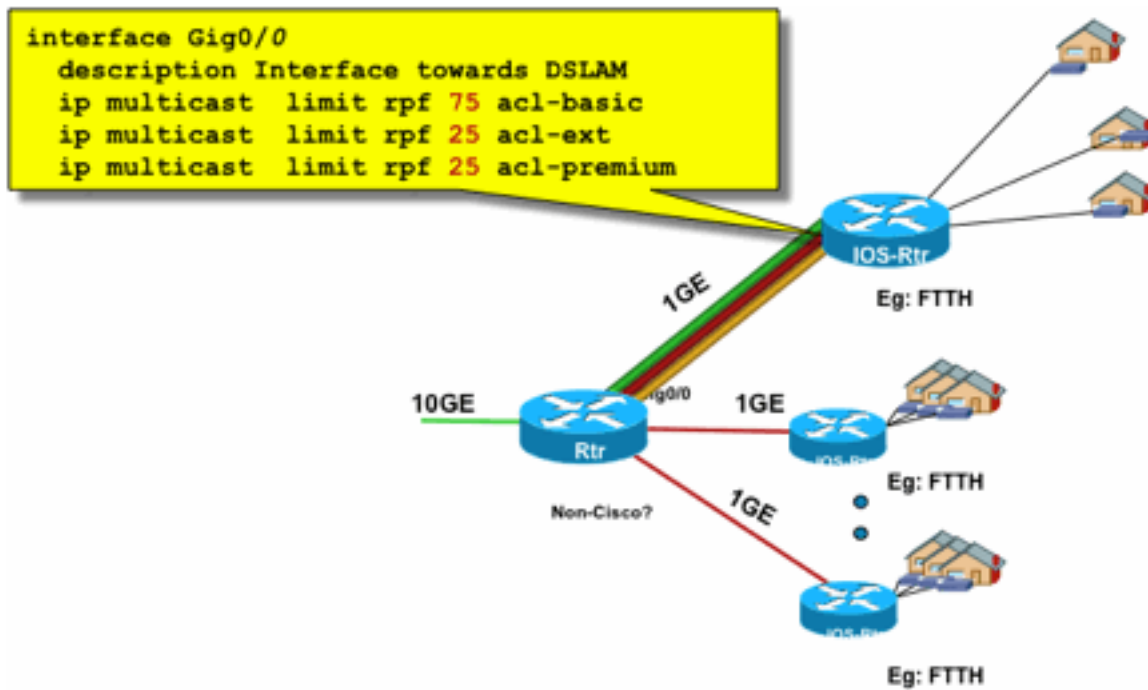
21\_PerInterface\_Mroute

### 示例2 - Agg-DSLAM链路路上的入口准入控制

可以在下游设备的RPF接口上使用RPF限制，而不是上游设备的出站接口上的“out”限制。这实际上与上一个示例的结果相同，如果下游设备不是Cisco IOS设备，则可能非常有用。

图22:使用每个接口的mroute限制；输入准入控制





22\_PerInterface\_Mroute\_inputControl

图

### 示例3 — 基于带宽的限制

您可以在多个内容提供商之间进一步划分访问带宽，并为每个内容提供商提供到DSLAM的上行链路带宽的公平份额。在这种情况下，请使用**ip multicast limit cost**命令：

```
ip multicast limit cost <ext-acl> <multiplier>
```

使用此命令，可以将“开销”（使用“multiplier”中指定的值）归属于与ip组播限制中的扩展ACL匹配的任何状态。

此命令是一个全局命令，可以同时配置多个开销。

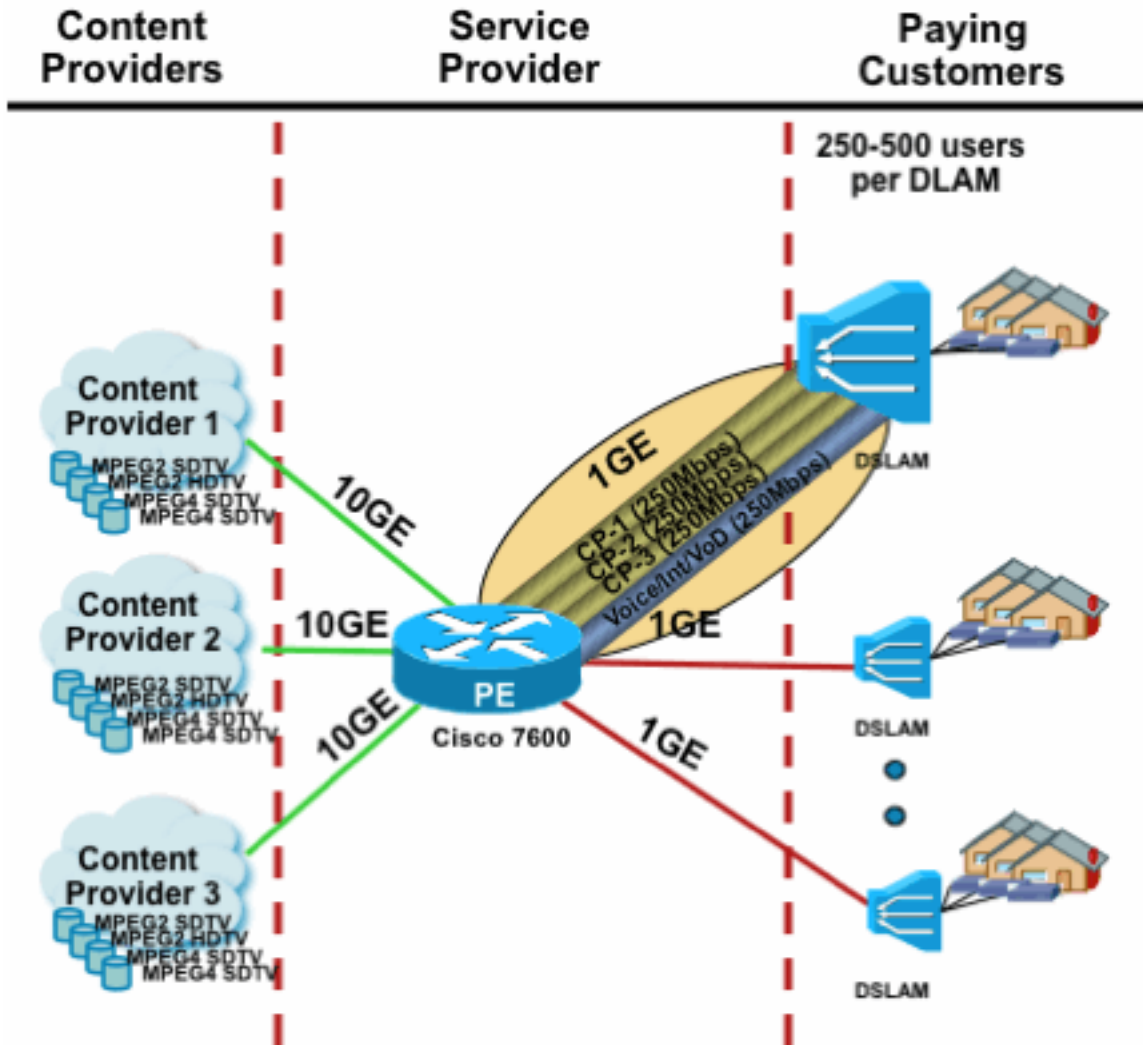
在本例中，必须支持三个不同的内容提供商公平地访问每个内容提供商进入网络。此外，在本示例中，需要支持各种类型的运动图像专家组(MPEG)流：

- MPEG2 SDTV:4Mbps
- MPEG2 HDTV:18Mbps
- MPEG4 SDTV:1.6Mbps
- MPEG4 HDTV:6Mbps

在这种情况下，您可以为每个流类型分配带宽成本，并通过以下配置在三个内容提供商之间共享750Mbps的剩余部分：

```
ip multicast limit cost acl-MP2SD-channels 4000 ! from any provider ip multicast limit cost
acl-MP2HD-channels 18000 ! from any provider ip multicast limit cost acl-MP4SD-channels 1600 !
from any provider ip multicast limit cost acl-MP4HD-channels 6000 ! from any provider !
interface Gig0/0 description --- Interface towards DSLAM --- <snip> ! CAC ip multicast limit out
250000 acl-CP1-channels ip multicast limit out 250000 acl-CP2-channels ip multicast limit out
250000 acl-CP3-channels
```

图23:每个接口的Mroute状态限制的开销系数



图

23\_Cost\_PerInterface

## 组播和IPSec

### GET VPN简介

与单播一样，组播流量有时也需要加以保护，以提供机密性或完整性保护。可能需要提供此类服务的两个主要领域：

- 加密组播流（例如，在银行应用程序中，将机密数据发送到使用组播的大量接收器）— 这是数据平面安全。
- 例如，使用组播、OSPF或PIM的控制平面协议加密 — 这是控制平面安全。

IPSec作为一种协议[RFC 6040、[7619](#)、[4302](#)、[4303](#)、5282]特别限于单播流量（通过RFC）。两个单播对等体之间建立了“安全关联”(SA)。为了将IPSec应用于组播流量，一个选项是在GRE隧道内封装组播流量，然后将IPSec应用于GRE隧道（单播）。较新的方法使用在组的所有成员之间建立的单一安全关联。Group Domain of Interpretation(GDOI)[RFC [6407](#)]定义了如何实现。

基于GDOI，思科开发了一种称为组加密传输(GET)VPN的技术。此技术使用文档“draft-ietf-msec-ipsec-extensions”中定义的“带地址保留的隧道模式”。在GET VPN中，首先在组的所有成员之间建立组安全关联。随后，使用ESP（封装安全负载）或AH（身份验证报头）保护流量，后者使用具有

地址保留的隧道模式。

总之，GET VPN封装使用原始报头地址信息的组播数据包，然后使用ESP保护与组策略相关的内部数据包。

GET VPN的优点是组播流量完全不受安全封装机制的影响。路由的IP报头地址仍与原始IP报头相同。无论是否使用GET VPN，组播流量均可采用相同的方法加以保护。

应用于GET VPN节点的策略在组密钥服务器上集中定义，并分发到所有组节点。因此，所有组节点都具有相同的策略，且对组流量应用相同的安全设置。与标准IPSec类似，加密策略定义哪种类型的流量需要以何种方式受到保护。这允许GET VPN用于各种用途。

## 使用GET VPN加密组播数据平面流量

在组密钥服务器上设置网络范围的加密策略，并将其分发到GET VPN终端。策略包含IPSec策略 (IPSec模式 — 此处：带有报头保留的隧道模式)，以及要使用的安全算法 (例如AES)。它还包含一个策略，描述哪些流量可以受到保护，如ACL所定义。

GET VPN可用于组播和单播流量。ACL可以定义保护单播流量的策略：

```
permit ip 10.0.0.0 0.255.255.255 10.0.0.0 0.255.255.255
```

这将加密源IP为10/8而目标IP为10/8的所有流量。GET VPN将忽略所有其他流量，例如从10/8到另一个地址的流量。

GET VPN在组播流量方面的应用技术上也是相同的。例如，此访问控制条目(ACE)可用于保护从任何源到相应组播组的流量：

```
permit ip any 239.192.0.0 0.0.255.255
```

此策略匹配所有源(“any”)和以239.192开头的组播组。流向其他组播组的流量不安全。

**注意：**必须高度重视加密ACL的构建。必须将管理流量，或者源自GET VPN域之外但终止于内部的流量 (即仅通过一个加密端点的流量) 排除在GDOI策略之外。

常见的错误包括：

- permit ip any 224.0.0.0 0.255.255.255:这还会加密OSPF流量和其他控制平面流量，例如发往对等路由器的流量。
- 管理流量不会从加密策略中排除，加密策略在网络内终止。这包括GDOI流量本身。

## 使用GET VPN验证控制平面流量

通常最佳做法是对控制平面流量 (例如路由协议) 进行身份验证，以确保消息来自受信任的对等体。对于使用单播的控制平面协议 (例如BGP) 来说，这相对简单。但是，许多控制平面协议使用组播流量。例如OSPF、RIP和PIM。有关完整列表，请参阅[IANA的IPv4组播地址空间注册](#)。

其中一些协议具有内置身份验证，如路由信息协议(RIP)或增强型内部组路由协议(EIGRP)，其他协议则依靠IPSec提供此身份验证 (例如OSPFv3、PIM)。对于后一种情况，GET VPN提供了一种可扩展的方法来保护这些协议。在大多数情况下，要求是协议消息身份验证，或者换句话说，验证

消息是否由受信任的对等体发送。但是，GET VPN也允许加密此类消息。

要保护（通常仅进行身份验证）此类控制平面流量，需要使用ACL描述流量并将其包括在GET VPN策略中。详细信息取决于要保护的协议，其中需要注意的是ACL是否包括仅通过入口GET VPN节点（已封装）或也通过出口节点的流量。

保护PIM协议有两种基本方法：

- **permit ip any 224.0.0.13 0.0.0.0**:这是“所有PIM路由器”组播组。但是，这并不能保护单播PIM消息
- **permit pim any**:这可以确保PIM协议的安全，无论使用的是组播还是单播

**注意：**这些命令作为示例提供，以帮助解释概念。例如，必须排除用于引导PIM的某些PIM协议，例如BSR或自动RP。这两种方法都有一定的优点和不便之处，这取决于部署情况。有关详细信息，请参阅有关如何使用GET VPN保护PIM的特定文献。

## 结论

组播在网络中正逐渐成为一种常见服务。家庭/家庭宽带网络中的IPTV服务的出现，以及世界许多金融市场向电子交易应用的转移，仅仅是要求组播成为绝对要求的两个例子。组播具有各种不同的配置、操作和管理挑战。其中一个关键挑战是安全。

本文档研究了多种保护组播的方法：

- 首先，查看整体组播控制和数据平面，解释与单播的差异如何带来新的安全挑战。
- 接下来，对多址网络中遇到的主要协议（特别是IGMP、PIM和MSDP）进行了一些详细的研究。在每种情况下，都会提供安全威胁说明和针对这些威胁推荐的缓解最佳做法。
- 此外，关于如何在某些特定应用中保护组播的一些特定示例，例如宽带边缘网络，与特定视频流可能需要的带宽量相比，宽带边缘网络的带宽可能会受到限制。
- 最后，GET VPN架构被描述为与IPSec集成的组播方式，用于安全VPN的传输。

考虑到组播安全，请记住它与单播的不同之处。组播传输基于动态状态的创建，组播涉及动态数据包复制，组播会响应PIM JOIN / PRUNE消息构建单向树。整个环境的安全性包括了解和部署丰富的Cisco IOS命令框架。这些命令主要围绕保护协议操作、状态（组播）或针对CoPP之类的数据包放置的策略器为中心。正确使用这些命令可以为IP组播提供强大的保护服务。

综上所述，本文提出并描述了多种方法：

1. 广泛使用SSM — 这是最简单的PIM模式，也允许使用(S, G)转发。
2. 如果需要ASM服务，请确保可提供强大的服务 — 使用静态定义的RP比动态RP通告提供更安全的控制平面。自动RP和BSR更加灵活
3. 如果已启用PIM-SM，请观察特定漏洞区域，如到RP的注册隧道，并确保DR始终受到良好的保护。CoPP在这些领域非常有用。
4. 如果需要域间ASM服务，请考虑是否可以部署BiDir PIM。
5. 使用全局mroute/igmp状态限制 — 了解您的平台的功能以及在正常情况下以及在最坏情况下您所需的最大状态数量。在平台功能范围内配置限制，使您的网络能够最大限度地运行。
6. 基本过滤器 — rACL/CoPP和基础设施ACL，在接入层阻止PIM

IP组播是一种激动人心的可扩展方式，可提供各种应用服务。与单播一样，它需要在各种不同的区域受到保护。本文提供了可用于保护IP组播网络的基本构建块。

## 相关信息

- [企业IP组播地址分配指南](#)
- [配置IPv4 IGMP过滤器](#)
- [群组加密传输 VPN](#)

## 关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。