安全IP多點傳送部署

目錄

簡介

本文檔介紹有關保護IP組播網路基礎設施的最佳實踐的一般指南。

必要條件

需求

思科建議您瞭解以下主題：

- IP 多點傳送

採用元件

本文件所述內容不限於特定軟體和硬體版本。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

本文檔介紹一些基本概念和術語，並討論下列主題：

- 保護特定平台和整個網路的機制。
- 任何來源多點傳送(ASM)和來源特定多點傳送(SSM)型號。
- 多點傳送虛擬私人網路(MVPN)安全。
- 群組加密傳輸(GET)虛擬私人網路(VPN)架構，可為多點傳送資料平面或控制平面流量提供機密性和完整性。

技術

在IP組播中有兩種典型的服務模型：

1.任何來源多點傳送(ASM)

2.來源特定多點傳送(SSM)

在ASM中，接收方通過網際網路組成員協定(IGMP)或組播偵聽程式發現(MLD)成員身份報告加入組G以指示該組。此報告請求任何源傳送到組G的流量，因此名稱為「任何源」。 相反，在SSM中，接收方加入由源S定義的特定通道，該特定通道將傳送到組G。以下詳細描述每種服務模型。

任何來源多點傳送

ASM模型的特點是兩類協定："dense mode flood-and-prune"和"sparse mode explicit join":

i)密集模式泛洪和修剪協定(DVMRP/MOSPF/PIM-DM)

在密集模式協定中，網路中的所有路由器都知道所有樹、它們的源和接收器。距離向量組播路由協定(DVMRP)和協定無關組播(PIM)密集模式等協定在整個網路中泛洪「活動源」資訊，通過在拓撲中不需要特定樹流量的部分建立「修剪狀態」來構建樹。它們也稱為泛洪和修剪協定。在組播開放最短路徑優先(MOSPF)中，有關接收者的資訊在整個網路中泛洪以支援樹構建。

不需要使用密集模式協定，因為網路某些部分中構建的每個樹都可能始終導致網路中所有路由器（或管理範圍內，如果已配置）的資源利用率（具有收斂影響）。 這些協定在本文的其餘部分沒有進一步討論。

ii)稀疏模式顯式連線協定(PIM-SM/PIM-BiDir)

使用稀疏模式顯式連線協定時，裝置不會在網路中建立組特定狀態，除非接收方已傳送組的顯式IGMP/MLD成員報告（或「連線」）。眾所周知，ASM的這種變體可以很好地擴展，並且是組播模式的焦點。

這是PIM稀疏模式的基礎，大多陣列播部署已使用到這一點。這也是雙向PIM(PIM-BiDir)的基礎，PIM-BiDir越來越多地部署為多個（源）到多個（接收器）應用程式。

這些協定稱為稀疏模式，因為它們有效地支援具有「稀疏」接收器群體的IP組播傳送樹，並只在源與接收器之間的路徑中的路由器上以及在PIM-SM/BiDir中建立交匯點(RP)控制平面狀態。 他們絕不會在網路的其它部分建立狀態。只有在路由器收到來自下游路由器或接收者的加入時，才會顯式建立路由器中的狀態，因此命名為「顯式加入協定」。

PIM-SM和PIM-BiDir都使用「SHARED TREES」，允許將來自任何源的流量轉發到接收器。共用樹上的組播狀態稱為(*,G)狀態，其中*是ANY SOURCE的萬用字元。此外，PIM-SM支援建立與來自特定源的流量相關的狀態。這些狀態稱為源樹，相關聯的狀態稱為(S，G)狀態。

來源特定多點傳送

SSM是接收器（或某些代理）傳送(S，G)「加入」以指示其希望接收由源S傳送到組G的流量的模型。可以使用IGMPv3/MLDv2「INCLUDE」模式成員身份報告。此模式稱為來源特定多點傳送(SSM)模式。SSM要求路由器之間使用顯式連線協定。其標準協定是PIM-SSM，它只是用於建立(S，G)樹的PIM-SM的子集。SSM中沒有共用樹(*,G)狀態。

因此，組播接收器可以「加入」ASM組G，或「加入」（或更準確地說「訂閱」）SSM(S，G)通道。為了避免重複術語「ASM組或SSM通道」，使用了術語（組播）流，這意味著流可以是ASM組或SSM通道。

相關多點傳送通訊協定/封包型別

要保護組播網路，必須瞭解常見的資料包型別以及如何防範它們。需要關注的協定主要有三種：

1. IGMP/MLD
2. PIM
3. MSDP

下一節將分別討論這兩種協定以及每種協定可能產生的問題。

IGMP/MLD封包

IGMP/MLD是組播接收器使用的協定，用於向路由器發出訊號，表示他們希望接收特定組播組的內容。Internet組成員協定(IGMP)是IPv4中使用的協定，而組播偵聽程式發現(MLD)是IPv6中使用的協定。

IGMP有兩個版本，IGMPv2和IGMPv3。還有兩個版本MLD是兩個版本，MLDv1和MLDv2。

IGMPv2和MLDv1在功能上是等效的，IGMPv3和MLDv2在功能上是等效的。

這些協定在以下連結中指定：

IGMPv2:RFC 2236

MLDv1:RFC 3590

IGMPv3和MLDv2:RFC 4604

IGMPv2和IGMPv3不僅是一種協定，而且也是IPv4 IP協定（具體來說，是協定號2）。 它不僅按照這些RFC中的說明用於報告組播組成員身份，還被其他IPv4組播協定（如DVMRP、PIM版本1、mtrace和mrinfo）使用。當您嘗試過濾IGMP(例如透過Cisco IOS® ACL)時，請務必記住這一點。在IPv6中，MLD不是IPv6協定；相反，ICMPv6用於承載MLD資料包。PIM版本2是IPv4和IPv6中的相同協定型別（協定號103）。

PIM控制資料包

本節將討論多點傳送和單播PIM控制資料包。討論了在PIM-SM網路中選擇集結點和控制組到RP分配的自動快速成形和引導路由器(BSR)。

多點傳送PIM控制封包

組播PIM控制資料包包括：

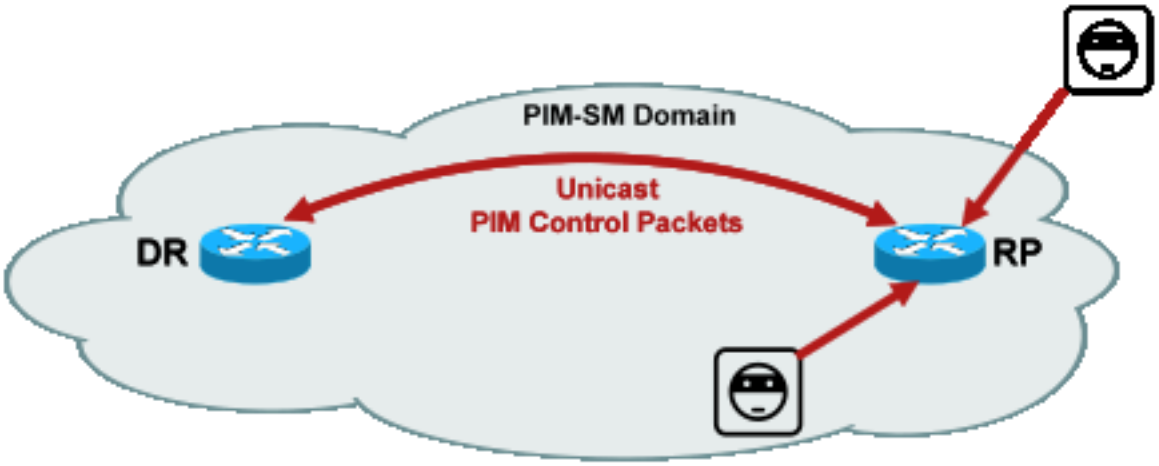
- **PIM Hello** - PIM Hello資料包是本地鏈路IP組播資料包，傳送到連線到同一網路的路由器以建立PIM鄰居。
- **PIM加入/修剪** - PIM加入/修剪是本地鏈路範圍IP組播資料包，傳送到建立/刪除組播狀態，並且僅傳送到PIM鄰居。它們是LAN中的多點傳送，旨在促進斷言、報告抑制和其他PIM通訊協定詳細資訊，但總是針對特定鄰居。
- **PIM DF-elect** - PIM Designated Forwarder是雙向PIM路由器，負責代表連線的接收方或下游PIM鄰居向RP傳送(*,G)連線。如果PIM路由器檢測到另一台路由器在相同組G的相同網段上傳送(*,G)加入，則選擇確定具有到RP的最佳路徑的路由器。
- **PIM斷言** - PIM斷言是當連線到網段的PIM路由器開始接收來自特定介面的特定資料包(S，G)的相同資料包時，傳送的本地鏈路IP組播資料包，該網段主動轉發來自特定介面的特定資料包(S，G)，而接收來自同一介面中轉發的特定資料包(S，G)。此事件表示有另一個路由器認為自己是此路由器(S，G)的單轉發器(SF)。 斷言機構為該(S，G)選擇唯一SF。 選擇PIM SF路由器為特定(S，G)流轉發資料包。PIM允許不同的路由器代表不同的(S，G)執行SF的角色，理想情況下，每個(S，G)只有一個SF。 請勿將SF與指定路由器混淆。PIM指定路由器負責將加入/修剪或源暫存器傳送到PIM-SM網路中的RP。
- **PIM Bootstrap** - PIM Bootstrap消息在PIMv2網路中傳送，以便於為特定組G動態選擇交匯點。

單播PIM控制資料包

單播PIM控制資料包定向到RP或從RP傳出，包括：

- **源註冊數**據包 — 傳送PIM源註冊資料包以向交匯點註冊新的組播源。一旦源開始傳送組播資料包，連線到源網路的指定路由器就會向RP傳送單播註冊流，以指示存在活動源，用於由RP負責的組播組。
  源暫存器資料包作為原始組播流的單播封裝傳送。
  PIM暫存器消息是進程級交換的，並且只在RP傳送暫存器停止消息之前傳送。這些封包的效能影響與來源(每(S，G)流量的速率成比例。
- **註冊停止**資料包 — PIM註冊停止資料包從集結點傳送到傳送註冊消息的PIM DR。當RP開始從源本地接收組播資料包時，會立即傳送註冊停止消息。
- **BSR候選 — 集結點通告資料包** - PIM BSR C-RP — 通告資料包被傳送到BSR，以便在選擇BSR後通告候選RP。

圖1:PIM單播資料包



1_PIM_unicast

利用這些資料包的攻擊可能來自任何地方，因為這些資料包是單播資料包。

自動RP資料包

自動RP是思科開發的協定，其用途與PIMv2 BSR相同。Auto-RP是在BSR之前開發的，只支援IPv4。 BSR支援IPv4和IPv6。 Auto-RP中的對映代理與BSR中的引導路由器功能相同。在BSR中，來自C-RP的消息單播到引導路由器。在自動RP中，消息通過組播傳送到對映代理，從而允許在邊界進行更簡單的過濾，如下文所述。自動RP在此連結中進行了詳細介紹：https://www.cisco.com/c/en/us/td/docs/ios/solutions_docs/ip_multicast/White_papers/rps.html

在Cisco IOS中，AutoRP/BSR資料包始終被轉發，並且當前未被禁用。這會在自動RP的情況下帶來特定的安全隱患。

圖2:自動RP資料包

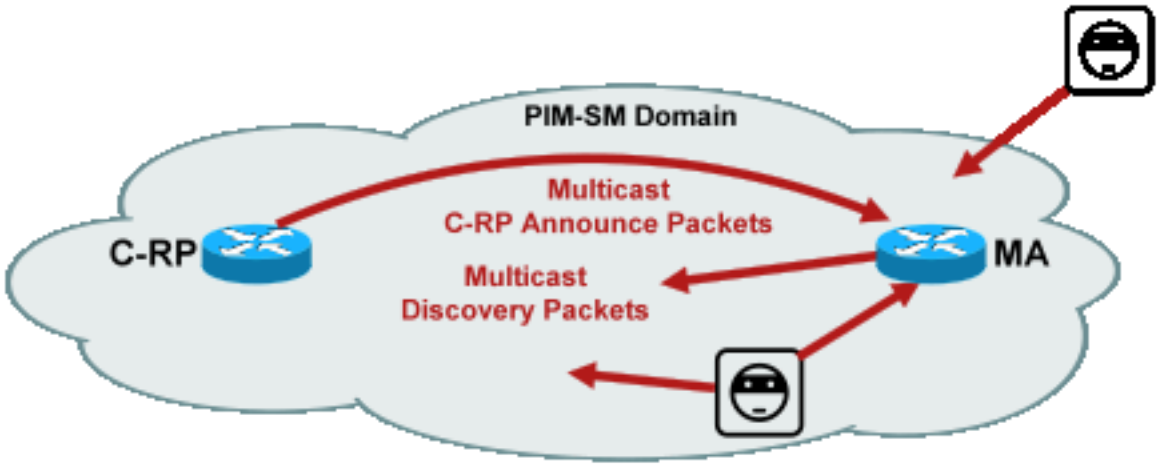


Fig2_A

utoRP_packets

附註：雖然自動RP被用作PIM-SM RP通告和發現的機制，但它不使用PIM資料包（IP協定

103）；相反，它使用使用者資料包協定(UDP)埠496資料包，帶有組播地址。

自動RP使用兩種資料包型別：

- C-RP-Announce資料包：這些資料包組播到所有對映代理，並使用網際網路編號指派機構(IANA)保留的「公認」地址(224.0.1.39)。 它們由C-RP傳送以通告RP能夠充當RP的RP地址和組範圍。
- C-RP發現資料包：這些資料包組播到所有PIM路由器，並使用IANA保留的「公認地址」(224.0.1.40)。 它們由自動RP對映代理傳送，以通告選擇為特定組範圍的RP的特定C-RP。

這些資料包型別中的每一種都旨在通過網路泛洪。

在Cisco IOS中，224.0.1.39和224.0.1.40都以PIM密集模式轉發，以避免當組用於分發RP資訊時，組的RP沒有事先知道的問題。這是僅推薦使用PIM密集模式。

在Cisco IOS XR中，自動RP訊息是反向路徑轉送(RPF) — 從鄰居到鄰居的逐跳泛洪。因此，無需建立PIM DM路由狀態來支援Cisco IOS XR中的自動RP。事實上，Cisco IOS XR完全不支援PIM-DM。

多點傳送服務探索通訊協定(MSDP)封包

MSDP是一種IPv4協定，它允許一個域中的源通過其各自的交匯點通告給另一個域中的接收器。RFC 3618中指定了MSDP。

為了在PIM域之間共用有關活動源的資訊，使用MSDP。如果一個域中的源變得活躍，則MSDP確保所有對等域及時瞭解這個新源，這允許其他域中的接收器快速聯絡這個新源，如果它恰好被傳送到接收器感興趣的組。ASM/PIM-SM組播通訊需要使用MSDP，它通過各個域中集結點之間配置的單播傳輸控制協定(TCP)連線運行。

組播環境中的威脅

信任區域和信任邊界

本文檔的此部分按網路中的功能實體組織。所討論的威脅模型圍繞這些實體形成。例如，本文檔說明了如何保護組播網路中的路由器（從組播的角度來看），而與路由器的部署位置無關。同樣，在如何部署網路範圍的安全措施，或在指定路由器、交匯點等上部署措施時，也會考慮以下事項

此處描述的威脅也遵循此邏輯，並根據網路中的邏輯功能進行組織。

威脅概述

在抽象級別上，任何組播部署都可能受到安全各方面的威脅。安全的關鍵方面是保密性、完整性和可用性。

- **保密性威脅**:在大多數應用中，多點傳播流量不會加密，因此任何人都可以在路徑中的任何線路或網元上偵聽或捕獲。在GET VPN一節中討論了加密組播流量以防止此類攻擊的方法。
- **對流量完整性的威脅**:如果沒有應用級安全或基於網路的安全性（如GET VPN），組播流量在傳輸過程中很容易被修改。這對於使用組播（例如OSPF、PIM和許多其他協定）的控制平面流量尤其重要。
- **網路完整性面臨的威**脅：如果沒有本文中描述的安全機制，未經授權的傳送者、接收者或受危害的網路元素可以訪問組播網路、未經授權傳送和接收流量（竊取服務）或過載網路資源。
- **可用性威脅**:有許多可能發生的拒絕服務攻擊會導致合法使用者無法使用資源。

接下來的部分將討論網路中每個邏輯功能的威脅。

對路由器的基本威脅

路由器面臨許多基本威脅，這些威脅與路由器是否支援組播以及攻擊是否涉及組播流量或協定無關。

拒絕服務(DoS)攻擊是網路中最重要的通用攻擊媒介。原則上，每個網路元素都可能遭受DoS攻擊，這可能使元素過載，進而導致合法使用者的服務丟失或降級。遵守適用於單播的基本網路安全建議至關重要。

值得注意的是，組播攻擊並非總是故意的，而往往是偶然的。例如，首次在2004年3月觀察到的Witty蠕蟲就是通過隨機攻擊IP地址傳播的一種蠕蟲病毒。由於地址空間完全隨機化，多播IP目標也受到蠕蟲的影響。在許多組織中，許多第一跳路由器崩潰，因為蠕蟲將資料包傳送到許多不同的組播目標地址。但是，路由器沒有使用關聯的狀態建立來承擔此類組播流量負載，並且實際上經歷了資源耗盡。這說明了即使企業未使用組播，也需要保護組播流量。

針對路由器的常見威脅包括：

- 任何型別的資料包泛洪；例如，針對硬體路徑(例如慢速(punt)路徑)和軟體路徑（例如管理或控制平面連線埠），包括安全殼層(SSH)、Telnet、邊界閘道通訊協定(BGP)、OSPF、網路時間通訊協定(NTP)等
- 入侵路由器，隨後利用路由器上的功能；弱Telnet或SSH密碼和弱簡易網路管理通訊協定(SNMP)社群字串是現代網路中的常見問題。
- 配置錯誤或內部攻擊等操作問題可能會危及整個網路及其流量的安全。

在路由器上啟用組播時，除了單播之外，還必須保護組播。使用IP組播不會改變基本的威脅模型；但是，它支援可能受到攻擊的額外協定(PIM、IGMP、MLD、MSDP)，這些協定需要特別保護。當這些通訊協定中使用單點傳播流量時，威脅模式與路由器執行的其他通訊協定相同。

必須注意的是，組播流量不能以與單播流量相同的方式使用以攻擊路由器，因為組播流量基本上是「接收器驅動的」，不能以遠端目標為目標。攻擊目標需要明確「加入」到組播流。在大多數情況下（自動RP是主要例外），路由器僅偵聽和接收「本地鏈路」組播流量。本地鏈路流量從不轉發。因此，對帶有組播資料包的路由器的攻擊只能來自直接連線的攻擊者。

來自源端的威脅

組播源（無論是PC還是影片伺服器）有時與網路不在相同的管理控制之下。因此，從網路運營商的角度來看，傳送方大多被視為不受信任。考慮到PC和伺服器的強大功能及其複雜的安全設定（通常並不完整），傳送方對任何網路（包括組播）都構成了嚴重威脅。這些威脅包括：

- **第2層攻擊**：第2層上有多種攻擊形式來執行各種型別的攻擊。這些適用於單播和組播。由於這些攻擊形式不是組播特有的，因此本文檔中不再詳細討論它們。有關詳細資訊，請參閱Cisco出版書籍《LAN Switch Security》，ISBN-10:1-58705-467-1．
- **組播流量攻擊：如前所述，由於第一跳路由器不會轉發組播流量**，因此很難對組播流量發起攻擊，除非組有偵聽器。但是，第一跳可以通過組播資料包以多種方式攻擊：
- 網路飽和攻擊：攻擊者可能會通過組播資料包泛洪資料段，從而過度利用可用頻寬，從而導致DoS情況。
- 組播狀態攻擊：第一跳路由器被組播資料包泛洪，這會造成太多的狀態，從而導致DoS攻擊情況。
- 傳送方可以通過傳送的PIM hello嘗試成為PIM DR。在這種情況下，任何流量都不會轉發到LAN或從LAN轉發。
- BiDir-PIM DF的PIM DF選舉資料包可能被偽裝。在這種情況下，任何流量都不會轉發到LAN或從LAN轉發。
- 傳送方可能偽裝AutoRP RP發現或BSR引導消息。這將有效通告虛假的RP，並關閉或中斷PIM-SM/BiDir服務。
- 傳送方可能發起單播攻擊（例如PIM源註冊/註冊停止消息），也可能傳送BSR通告資料包和通告虛假BSR。
- 傳送者可以傳送到任何有效的組播組，除非進行了過濾。如果源地址在邊緣被欺騙且未被阻止，則傳送方可以使用合法傳送方的源IP地址，並覆蓋部分網路中的內容。
- 針對控制平面協定的組播攻擊：許多與組播沒有關聯的協定（如OSPF和動態主機配置協定[DHCP]）使用組播資料包，它們可用於攻擊這些協定
- **偽裝：**傳送者可以假扮成另一個傳送者存在許多攻擊表單。欺騙源IP地址就是這種攻擊形式。
- **服務失竊：**除非對傳送方進行控制，否則可以從傳送方非法使用組播服務。

附註：主機通常不傳送或接收PIM資料包。執行此操作的主機可能嘗試發起攻擊。

來自接收方的威脅

接收方通常也是具有大量CPU功率和頻寬的平台，允許多種攻擊形式。這些威脅大多與傳送方威脅相同。第2層攻擊仍然是重要的攻擊媒介。在接收端也可能出現假接收者和服務失竊，但攻擊向量通常是IGMP（或如前所述的第2層攻擊）。

威脅交匯點和BSR

PIM-SM RP和PIM-BSR是組播網路中的關鍵點，因此是攻擊者的重要目標。如果第一跳路由器兩者都不是，則只有單播攻擊形式（包括PIM單播）才能直接針對這些元素。針對RP和BSR的威脅包括：

- 所有通用的攻擊形式，如「對路由器的基本威脅」一節所述。
- PIM單播攻擊（可能包含偽造的源IP地址）允許DoS攻擊，儘管PIM註冊或註冊停止消息由惡意裝置傳送。

多點傳送和單點傳送安全（比較）

狀態注意事項/過濾器

考慮圖3中的拓撲，其中顯示一個源、三個接收器(A、B、C)、一個交換機(S1)和兩個路由器（R1和R2）。 藍線表示單播流，紅線表示組播流。所有三個接收器都是組播流的成員。

圖3:路由器和交換機中的複製

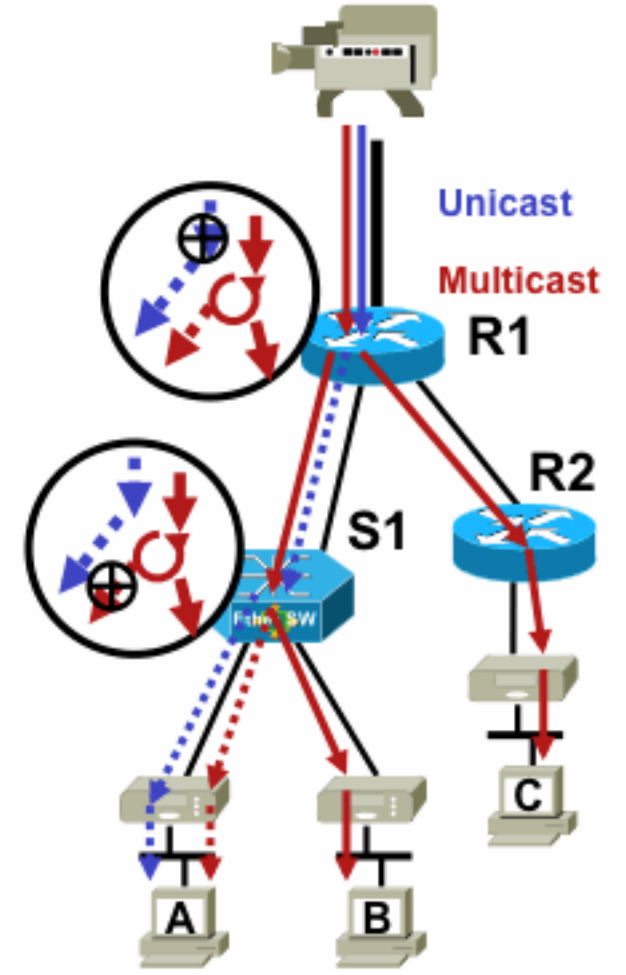


圖3_replication_RS

要禁止從特定源到特定接收方的流量，請執行以下操作：

- 對於單播流，在從傳送方到接收方的路徑上的任何位置安裝過濾器。
- 但是，對於組播流，管理員需要對安裝過濾器的位置進行更具體的說明：在接收端進行過濾，在最後複製點之後進行接收；在源端過濾在源之後的第一個複製點之前。

來自組播源的攻擊

本節適用於ASM和SSM服務模型，其中基於接收方顯式連線來轉發流量。

對於單播流，沒有隱式接收器保護。單點傳播來源可將流量傳送到目的地，即使此目的地沒有要求流量。因此，防火牆等防禦機制通常用於保護端點。另一方面，組播在協定中內建了一些隱性保護。理想情況下，流量僅到達已加入相關流量的接收器。

使用ASM，源可以通過將組播流量傳輸到活動RP支援的任何組，來啟動流量插入或DoS攻擊。理想情況下，此流量不會到達接收器，但至少可以到達路徑中的第一跳路由器，也可到達RP（允許有限攻擊）。但是，如果惡意來源知道目標接收者感興趣的組，並且如果沒有適當的過濾器，則可以將流量傳送到該組。只要接收者偵聽組，就會接收此流量。

使用SSM時，只有第一跳路由器上可能存在不受歡迎的源發起的攻擊，如果沒有接收方加入該(S，G)通道，流量會在該第一跳路由器上停止。這不會導致第一跳路由器受到任何狀態攻擊，因為它會丟棄接收器中不存在顯式加入狀態的所有SSM流量。在此模型中，僅讓惡意源知道目標對哪個組感興趣是不夠的，因為「連線」是源特定的。在這裡，需要偽裝的IP源地址以及潛在的路由攻擊才能成功。

狀態攻擊

即使網路中沒有接收器，PIM-SM也會在最靠近源的第一跳路由器上以及集結點上建立(S，G)和(*,G)狀態。因此，在源第一跳路由器和PIM-SM RP上可能存在對網路的狀態攻擊。

如果惡意源開始向多個組傳送流量，則對於檢測到的每個組，如果相關組由RP配置允許，則處於網路狀態的路由器會在源和RP處建立狀態。

因此，PIM-SM會受到源和流量攻擊。如果來源在正確的字首內隨機變更其來源IP位址，或者換句話說，只有該位址的主機位被偽裝，則攻擊可能會加劇。

圖4:ASM RP攻擊

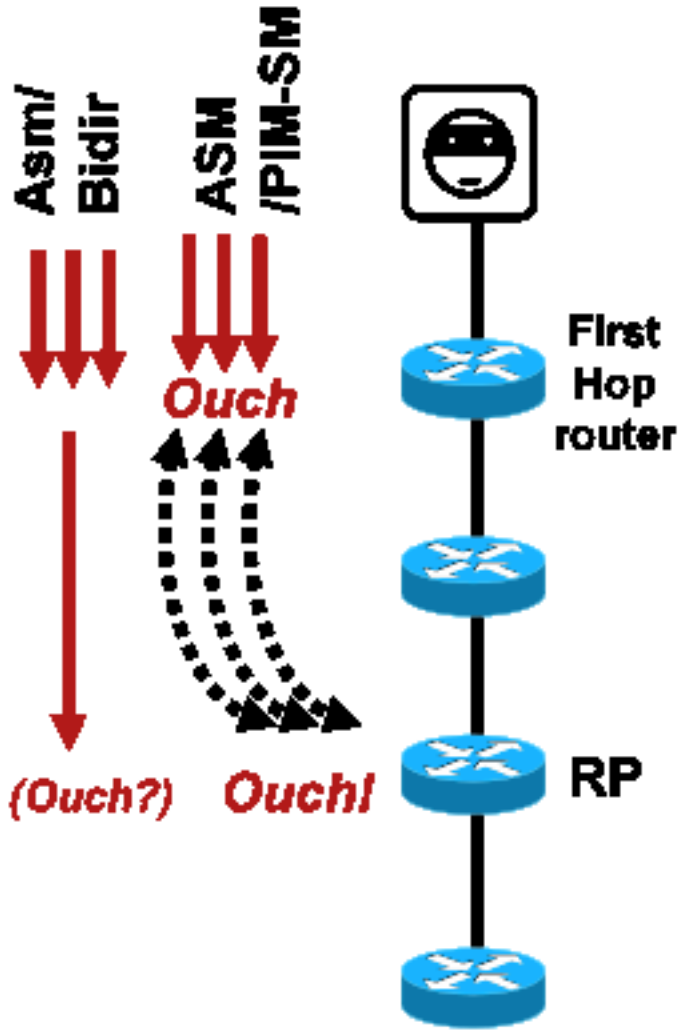


Fig4_ASM_RP_Attacks

與PIM-SSM一樣，來自源的PIM-BiDir狀態建立攻擊是不可能的。PIM-BiDir中的流量在由來自接收器的連線建立的狀態上轉發，同時狀態上轉發到RP的流量，這樣它就可以到達RP後面的接收器，因為連線只轉到RP。向RP轉發流量的狀態稱為(*,G/M)狀態，由RP配置（靜態、自動RP、BSR）建立。 它在源存在的情況下不會改變。因此，攻擊者可以向PIM-BiDir RP傳送組播流量，但與PIM-SM不同的是，PIM-BiDir RP不是「活動」實體，而只是為PIM-BiDir組轉發或丟棄流量。

> **附註**：某些Cisco IOS平台(*,G/M)狀態不受支援。在這種情況下，源可以通過將流量組播到多個PIM-BiDir組(導致(*,G)狀態建立)來攻擊路由器。例如，Catalyst 6500交換機支援(*、G/M)狀態)。

接收器發起的攻擊

攻擊可能源自組播接收器。任何傳送IGMP/MLD報告的接收器通常會在第一跳路由器上建立狀態。單播中沒有等價機制。

圖5:接收方基於顯式連線的流量轉發

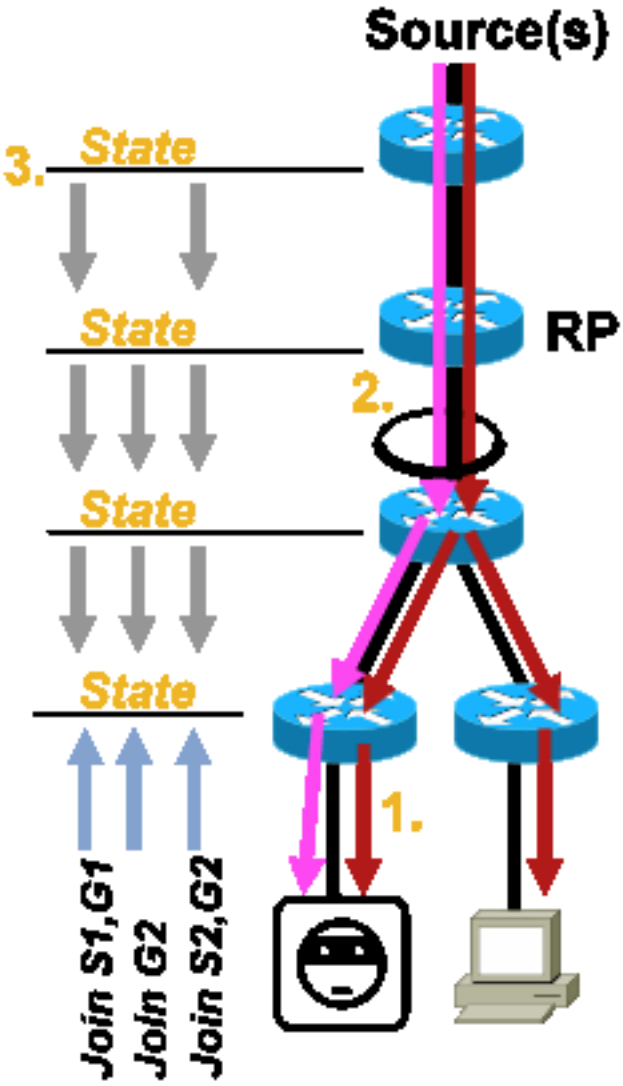


圖5_Receiver_Explicit_Join

接收器攻擊可分為三種：

1. 組播接收器可以嘗試加入其未授權的流，並嘗試接收其未授權接收的內容。
2. 組播接收器可能會通過關注許多組或通道來過載可用網路頻寬。這種攻擊變成了對其他潛在內容接收者的共用頻寬攻擊。
3. 組播接收器可能會嘗試對路由器或交換機發起攻擊。可以生成大量IGMP報告，從而產生大量的組播樹狀態和潛在的路由器過載。這反過來又會導致組播收斂時間延長，或導致路由器上的DoS增加。

緩解此類攻擊的各種方法將在下一節「組播網路中的安全性」中介紹。

組播網路中的安全性

網路元素安全性

安全不是單點功能，而是每個網路設計的一個固有部分。因此，必須在網路的每個點考慮安全性。每個網路元素都得到適當的保護至關重要。一種可能的攻擊場景是路由器被入侵者破壞，適用於任

何技術。一旦入侵者控制了路由器，攻擊者就可以運行許多不同的攻擊場景。因此，每個網路元素都必須相應地受到保護，以免受任何形式的基本攻擊以及特定組播攻擊。

控制階段管制(CoPP)

CoPP是路由器ACL(rACL)的演變，在大多數平台上可用。原則是一樣的：CoPP只管制發往路由器的流量。

服務策略使用與任何服務品質策略相同的語法，包括策略對映和類對映。因此，它會使用速率限制器將rACL（允許/拒絕）的功能擴展到向控制平面傳輸的特定流量。

> **附註**：某些平台（例如Catalyst 9000系列交換器）預設啟用CoPP，且保護不會取代。如需其他資訊，請參閱CoPP指南。

如果您決定在即時網路中調整、修改或建立rACL或CoPP，請務必小心。由於這兩個功能都能夠過濾到控制平面的所有流量，因此必須明確允許所有所需的控制平面和管理平面協定。所需的通訊協定清單非常龐大，因此很容易忽略不太明顯的通訊協定，例如終端存取控制器存取控制系統(TACACS)。 所有非預設rACL和CoPP配置在部署到生產網路之前，必須始終在實驗室環境中進行測試。此外，初始部署只需從「允許」策略開始。這將允許使用ACL命中計數器驗證任何意外命中。

在組播環境中，必須在rACL或CoPP中允許所需的組播協定（PIM、MSDP、IGMP等）才能使組播正常工作。請務必記住，在PIM-SM場景中，來自源的組播流中的第一個資料包被用作控制平面資料包，以幫助建立組播狀態，位於裝置的控制平面。因此，在rACL或CoPP中允許相關組播組非常重要。由於存在許多特定於平台的例外，因此在部署之前查閱相關文檔和測試任何計畫的配置非常重要。

本機封包傳輸服務(LPTS)

在Cisco IOS XR上，本地封包傳輸服務(LPTS)充當通向路由器控制平面的流量管制器，類似Cisco IOS上的CoPP。此外，接收流量（包括單播和組播流量）可以經過過濾和速率限制。

多點傳送特定安全

在啟用組播的網路中，每個網路元素都需要使用組播特定的安全功能進行保護。本節針對一般路由器保護對這些進行了概述。下一節將討論並非每台路由器都需要的功能（但僅針對網路中的特定位置），以及需要路由器之間互動的功能（如PIM身份驗證）。

Mroute限制

mroute limit命令限制路由器上的全域性組播路由量，有助於防止DoS攻擊。

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

圖6:Mroute限制

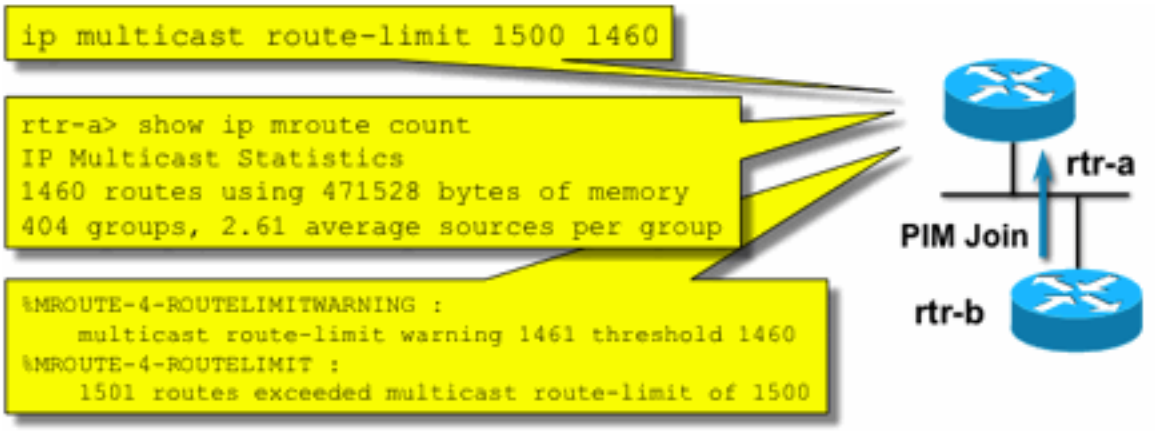


圖6_Mroute_Limits

Mroute限制允許為組播路由表中允許的路由數量設定閾值。如果啟用了組播路由限制，則不會建立超出配置限制的組播狀態。還有一個警告閾值。當路由數量超過警告閾值時，將觸發系統日誌警告消息。在mroute limit處，會觸發狀態的任何其他資料包都會被丟棄。

每個MVRF還可以使用**ip multicast route-limit**命令。

禁用SAP偵聽：no ip sap listen

sap listen命令使路由器收到會話通告協定/會話描述協定(SAP/SDP)消息。SAP/SDP是一種從組播主幹(MBONE)開始使用的傳統協定。 這些消息指示未來或當前可用的有關組播內容的目錄資訊。這可能是針對路由器CPU和記憶體資源的DoS源，因此需要禁用此功能。

控制對mrinfo資訊的訪問 — "ip multicast mrinfo-filter"命令

mrinfo命令（在Cisco IOS上以及在某些Microsoft Windows和Linux版本上提供）使用各種消息查詢組播路由器以獲取資訊。**ip multicast mrinfo-filter**全域性配置命令可用於將對此資訊的訪問限制到源的子集，或者完全禁用該資訊。

此示例拒絕源自192.168.1.1的查詢，而允許來自任何其他源的查詢：

```
ip multicast mrinfo-filter 51

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

此示例拒絕 *mrinfo* 來自任何來源的請求：

```
ip multicast mrinfo-filter 52

access-list 52 deny any
```

附註：與任何ACL一樣，*deny*表示過濾封包，而permit表示允許封包。

如果將**mrinfo**命令用於診斷目的，則強烈建議使用適當的ACL配置**ip multicast mrinfo-filter**命令，以便僅允許從源地址的子集進行查詢。*mrinfo*命令提供的資訊也可通過SNMP檢索。強烈建議使用完整的mrinfo請求塊（從裝置的查詢中阻止任何源）。

網路安全

本節討論了保護PIM組播和單播控制資料包以及自動RP和BSR的各種方法。

禁用組播組

ip multicast group-range/ipv6 multicast group range命令可用於為ACL拒絕的組禁用所有操作：

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

如果資料包顯示為被ACL拒絕的任何組，則它們會在所有控制協定（包括PIM、IGMP、MLD、MSDP）中丟棄，並在資料平面上丟棄。因此，從未為這些組範圍建立IGMP/MLD快取條目、PIM、組播路由資訊庫/組播轉發資訊庫(MRIB/MFIB)狀態，並且所有資料包都會立即被丟棄。

這些命令在裝置的全域性配置中輸入。

建議您在網路中的所有路由器上部署此命令，以便控制源自網路外部的所有組播流量。請注意，這些命令會影響資料平面和控制平面。如果可用，此命令提供的覆蓋範圍比標準ACL更廣泛，因此是首選命令。

PIM安全

PIM鄰居控制

PIM路由器必須收到PIM Hello才能建立PIM鄰居關係。PIM鄰居關係也是指定路由器(DR)選舉、DR故障轉移以及傳送/接收PIM加入/修剪/斷言消息的基礎。

圖7:PIM鄰居控制

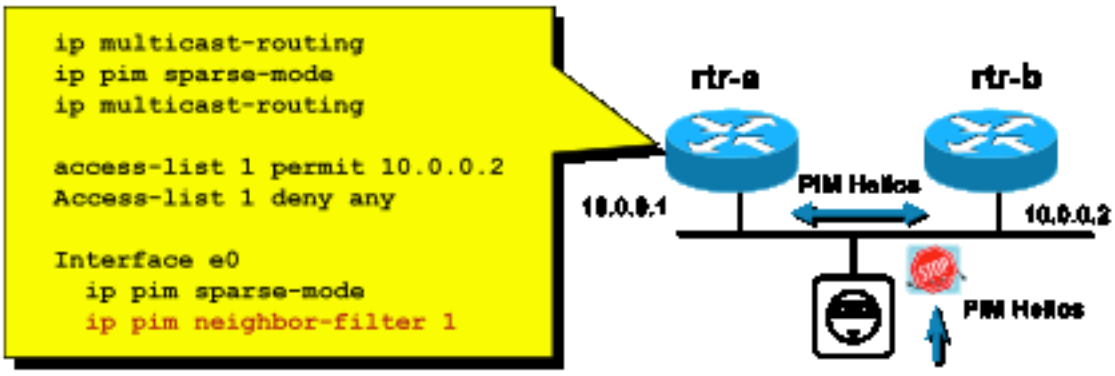


Fig7_PIM_neighbor_control

要阻止不需要的鄰居，請使用 **ip pim neighbor-filter** 命令如圖7所示。此命令過濾所有不允許的鄰居PIM資料包，包括Hello、加入/修剪資料包和BSR資料包。網段上的主機可能會偽裝源IP地址，偽裝成PIM鄰居。需要第2層安全機制（即IP源保護）來防止源地址在網段上進行欺騙嘗試，或在接入交換機中使用VLAN ACL來阻止來自主機的PIM資料包。關鍵字「log-input」可用於在ACL中記錄與ACE匹配的資料包。

PIM加入/修整資料包被傳送到PIM鄰居，以新增該鄰居或從特定(S，G)或(*,G)路徑中刪除該鄰居。PIM組播資料包是以生存時間(TTL)=1傳送的鏈路本地組播資料包。所有這些資料包都組播到眾所周知的全PIM路由器地址：224.0.0.13 .這表示所有此類攻擊必須源自與受攻擊的路由器相同的子網。攻擊可能包括偽造的Hello、加入/修剪和斷言資料包。

> **附註**：將PIM組播資料包中的TTL值人為增加或調整到高於1不會產生問題。All-PIM-Routers地址始終在路由器本地接收和處理。正常和合法路由器從不直接轉發它。

為了保護RP免受潛在的PIM-SM註冊消息泛洪的影響，DR需要對這些消息進行速率限制。使用**ip pim register-rate-limit**命令：

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

圖8:PIM-SM暫存器通道控制

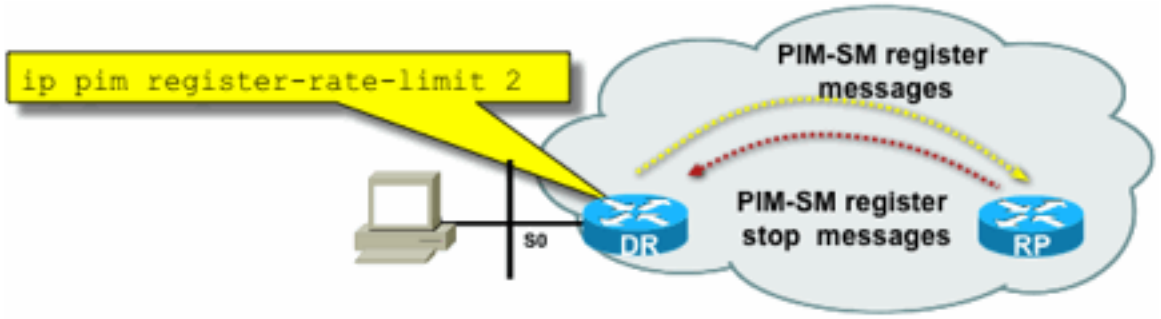


Fig8_PIMSM_Reg Tunnel

PIM單播資料包可用於攻擊RP。因此，RP可以通過基礎設施ACL來抵禦此類攻擊。請記住，組播傳送方和接收方永遠不需要傳送PIM資料包，因此PIM協定（IP協定103）通常可以在使用者邊緣進行過濾。

自動RP控制 — RP通告過濾器

ip pim rp-announce filter 命令是附加的安全措施，可以儘可能使用自動RP進行配置：

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

這可以在對映代理上配置，以控制哪些路由器被接受為哪個組範圍/組模式的候選RP。

圖9:自動RP - RP通告過濾器

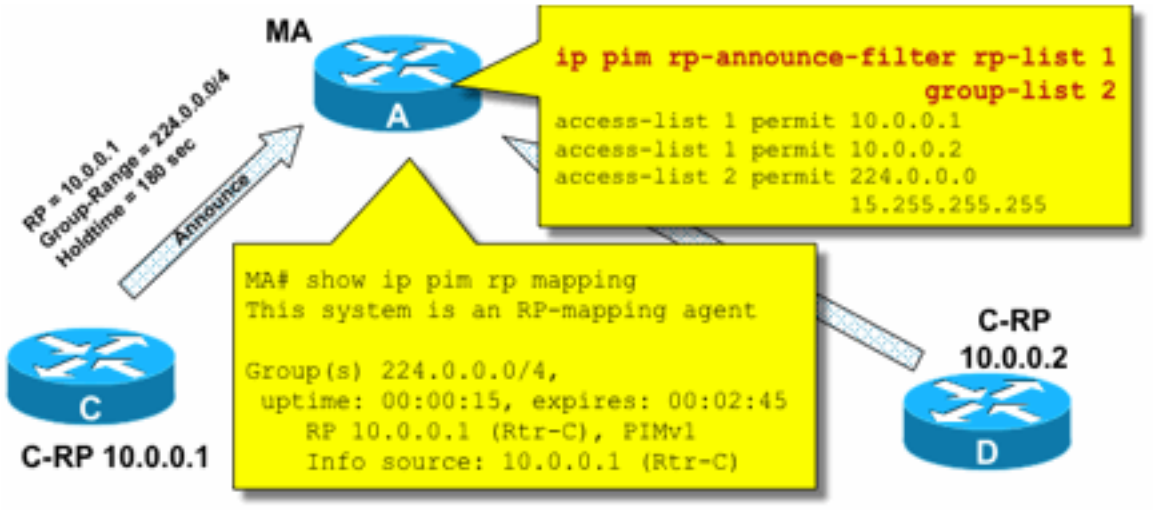


Fig9_AutoRP_RP_Announce

自動RP控制 — 限制自動RP消息

使用multicast boundary命令將AutoRP資料包、RP通告(224.0.1.39)或RP發現(224.0.1.40)限制到特定PIM域：

```
ip multicast boundary
```

圖10:多點傳送邊界命令

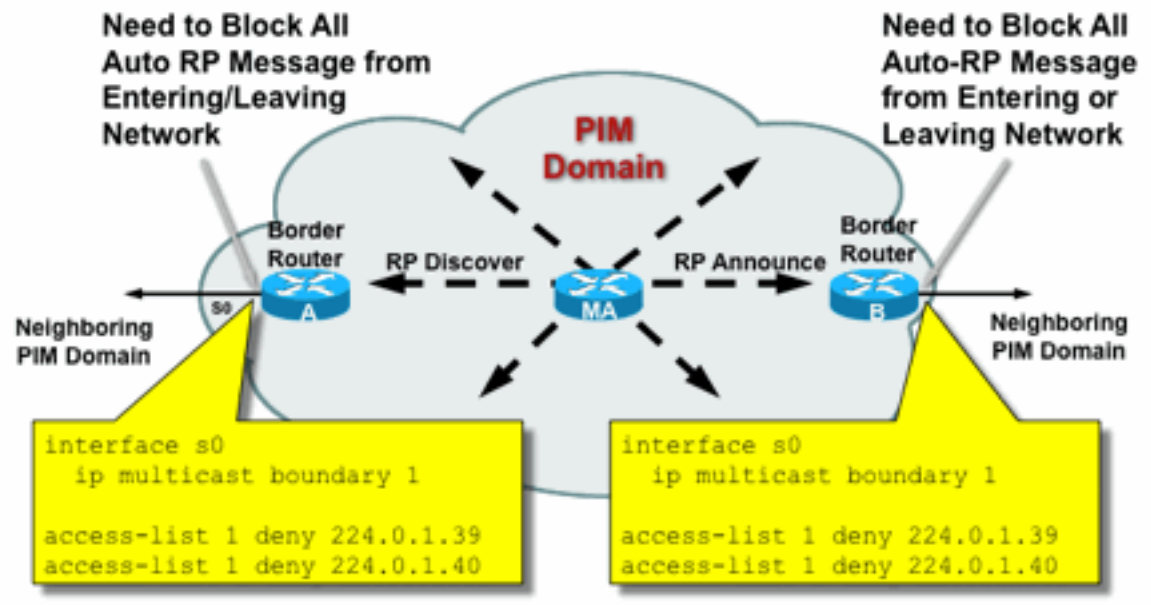


Fig10_Mcast_Boundary

BSR控制 — 限制BSR消息

使用 **ip pim bsr-border** 命令過濾PIM域邊界的BSR消息。無需ACL，因為BSR消息是通過鏈路本地組播逐跳轉發的。

圖11:BSR邊框

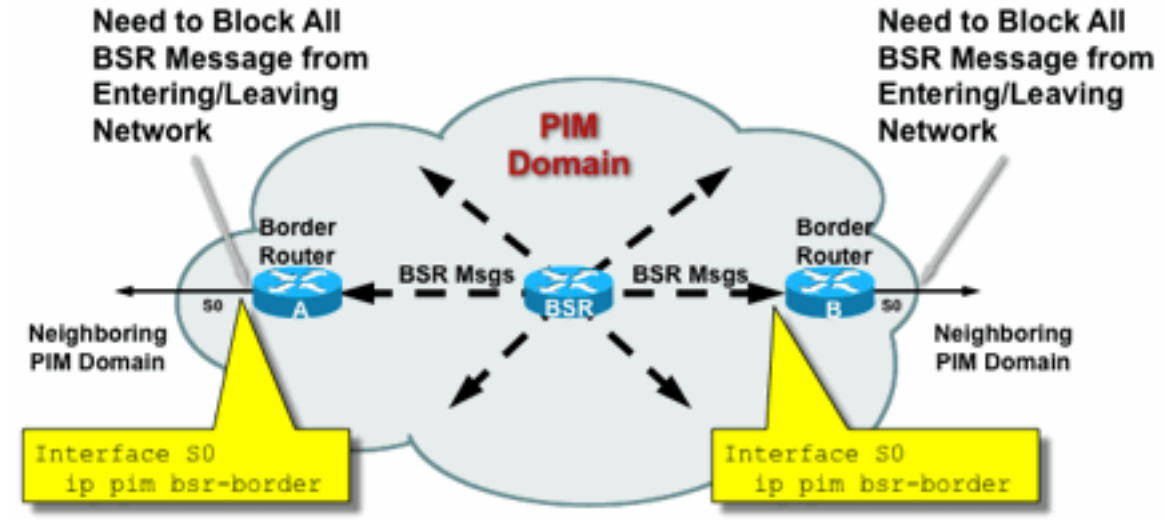


Fig11_BSR_Router

RP/PIM-SM相關過濾器

在最後一部分中，將討論針對PIM-SP和RP控制平面資料包以及自動RP、BSR和MSDP消息的過濾器。

自動RP過濾器

圖12顯示了與地址範圍結合使用的自動RP過濾器的示例。顯示了兩種不同的繫結區域的方法。從自動RP的角度來看，兩個ACL是等效的。

圖12:自動RP過濾器/範圍

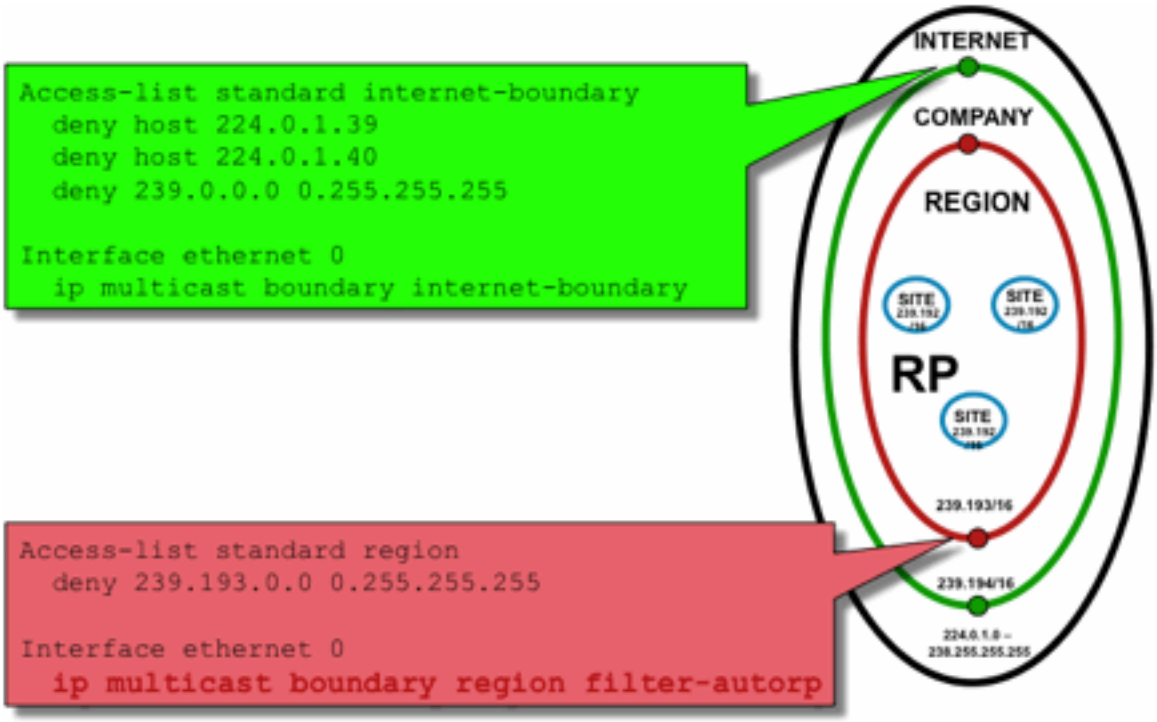


Fig12_AutoRP_Filtering_Scoping

自動RP的介面邊界過濾器的思想是確保自動RP通告僅到達它們支援的區域。定義區域、公司和網際網路範圍，並在每個範圍內有RP和自動RP通告。管理員僅希望區域路由器知道區域RP，區域和公司路由器知道公司RP，並希望所有網際網路RP全域性可用。範圍可以進一步擴展。

如圖所示，過濾自動RP封包有兩種基本不同的方式：Internet邊界顯式呼叫自動rp控制組（224.0.1.39和224.0.1.40），這導致對所有自動RP資料包進行過濾。此方法可以在管理域的邊緣使用，在該邊緣沒有通過自動RP資料包。區域邊界使用filter-auto-rp關鍵字來檢查自動RP資料包中的rp到組範圍通告。當ACL明確拒絕通知時，會在轉發資料包之前將其從自動RP資料包中刪除。在示例中，這允許在區域內知道企業範圍的RP，而在從區域到企業其餘部分的邊界處過濾區域範圍的RP。

網域間過濾器和MSDP

在本示例中，ISP1充當PIM-SM傳輸提供商。它們僅支援與鄰居的MSDP對等，並且它們只接受(S，G)，但邊界路由器上不接受(*,G)流量。

在域間（通常在自治系統之間）要採取兩種基本的安全措施：

1. 通過**multicast boundary**命令保護資料平面。這可確保組播流量僅被定義的組（以及可能的源）接受。
2. 保護網域間控制平面流量(MSDP)。 這包括若干單獨的安全措施：MSDP內容控制、狀態限制和鄰居身份驗證。

圖13提供了在ISP1的邊界路由器上配置介面過濾器的示例。

要保護域邊界的資料平面通過過濾器禁止(*,G)加入「主機0.0.0.0」，並通過**multicast boundary**命令管理範圍地址：

圖13:域間(*,G)過濾器

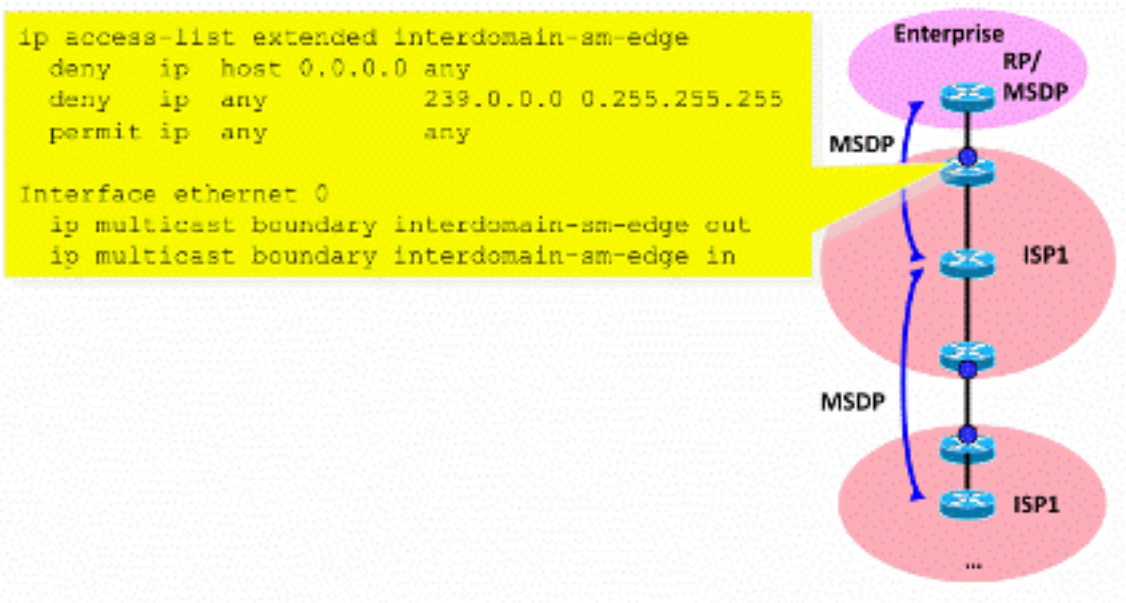


Fig13_Interdomain_Filter

要保護控制平面，可通過三種基本安全措施強化MSDP:

1)MSDP SA過濾器

通過MSDP SA過濾器過濾MSDP消息的內容是一種「最佳慣例」。此過濾器的主要思想是避免組播狀態的傳播，適用於不是泛網際網路應用程式並且不需要在源域之外轉發的應用程式和組。理想情況下，從安全形度來看，過濾器僅允許已知組（以及可能的發件人）並拒絕任何未知發件人和/或組。

通常無法明確列出所有允許的發件人和/或組。建議對每個組使用單個RP的PIM-SM域使用預設配置過濾器（無MSDP網狀組）：

```
!--- 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 !
```

建議儘可能嚴格地過濾入站和出站兩個方向的流量。

有關MSDP SA篩選器建議的詳細資訊，請使用：https://www.cisco.com/c/en/us/support/docs/ip/ip-multicast/13717-49.html

2)MSDP狀態限制

當在多個自治系統(AS)之間啟用MSDP時，建議限制由於從鄰居接收的「源 — 活動」(SA)消息而在路由器中建立的狀態量。您可以使用**ip msdp sa-limit**命令：

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

圖14:MSDP控制平面

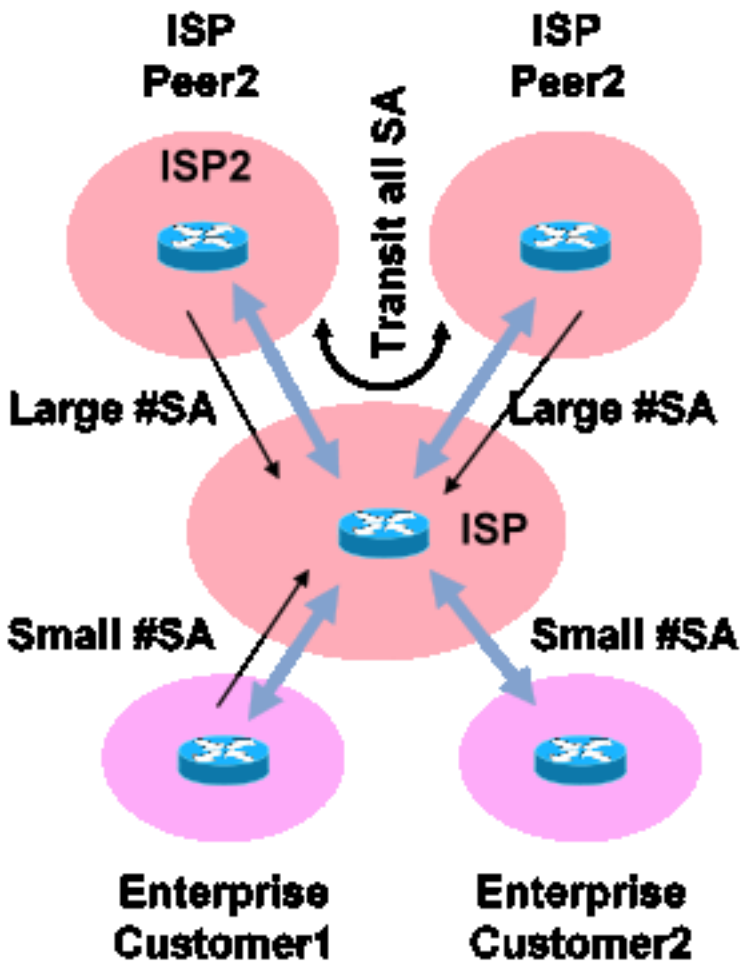


Fig14_MSDP_ControlPlane

使用**ip msdp sa-limit**命令，您可以限制由於從MSDP對等體接收的SA消息而建立的SA狀態數。一些簡單的經驗法則建議包括：

- 來自末節鄰居的小限制
- 來自傳輸鄰居的大限制(例如Internet#SAs的最大限制)
- 傳輸ISP — 配置您的平#SAs可支援的最大數量

3)MSDP MD5鄰居身份驗證

建議對MSDP對等點使用消息摘要演算法(MD5)密碼驗證。這使用TCP MD5簽名選項，相當於RFC 6691中所述用於保護BGP的使用。

圖15:MSDP MD5鄰居身份驗證

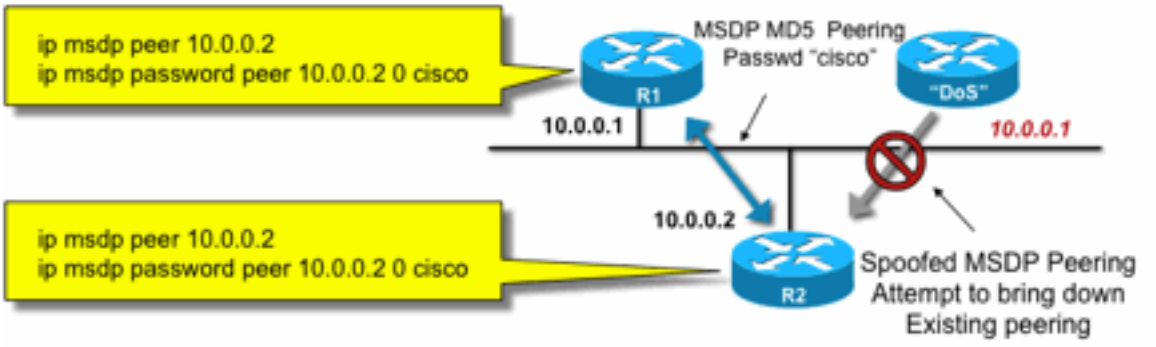


Fig15_MSDP_MD5Auth

以下三項MSDP安全建議追求不同的目標：

- 鄰居身份驗證（使用MD5）可確保只有受信任的MSDP對等體才能傳送消息。
- SA過濾器可確保即使受信任的MSDP對等體也只能傳送符合預先同意的源/組策略的SA通告。
- SA限制進一步確保即使有來自合法對等體的合法(S，G)通告，可用的記憶體也不會被耗盡。

發件人/源問題

通過適當的單播安全機制，可以緩解源自傳送方的許多組播安全問題。下面是建議採用的一些單播安全機制：

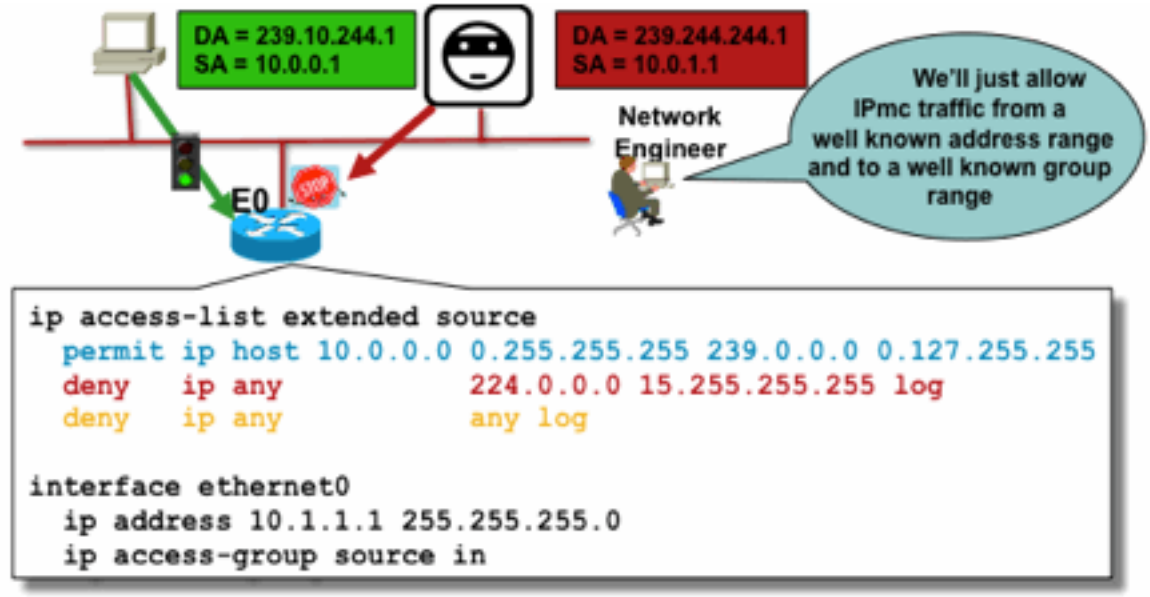
- **源地址欺騙保護**（接入層的單播反向路徑轉發、uRPF或ACL和IP源防護）
- **基礎架構**ACL(deny ip any(to)<core address space>)

此類措施可用於阻止對核心的定向攻擊。例如，這還可以解決類似使用PIM單播資料包到RP的攻擊的問題，RP位於網路的「內部」，因此受基礎設施ACL保護。

基於資料包過濾器的訪問控制 — 控制源

在圖16所示的示例中，過濾器是在第一跳組播路由器（指定路由器）的LAN介面(E0)上配置的。 過濾器由稱為「源」的擴展訪問控制清單定義。此ACL應用於連線到源LAN的指定路由器的面向源介面。事實上，由於組播流量的性質，可能需要在所有面向LAN的介面上配置類似的過濾器，源裝置可能會變為活動狀態。由於不可能在所有情況下都準確地知道源活動發生的位置，因此建議對網路中的所有入口點應用此類過濾器。

圖16:控制源



圖

16_Controlling_Sources

此過濾器的用途是防止從特定源地址或源地址範圍到特定組或組地址範圍的流量。此過濾器在PIM建立任何路由之前起作用，並幫助限制狀態。

這是標準資料平面ACL。這在高端平台上的ASIC上實施，不會導致效能下降。對於直接連線的源，建議使用資料平面ACL並優先使用它們，因為它們會最大程度地減少不需要的流量對控制平面的影響。將資料包傳送到目的地（IP組播組地址）的限制也非常有效。因為這是一個路由器命令，所以它無法克服偽裝的源IP地址（請參閱本節前面的部分）。 因此，建議為能夠連線到特定區域網/虛擬區域網(LAN/VLAN)的所有裝置提供額外的第2層(L2)機制或一致的策略。

> **附註**：ACL中的「log」關鍵字非常有助於瞭解針對特定ACL專案的命中；但是，這會消耗CPU資源，需要小心處理。此外，在基於硬體的平台上，ACL日誌消息由CPU生成，因此必須考慮CPU的影響。

PIM-SM源控制

從安全形度來看，ASM/PIM-SM體系結構的實際優勢之一是，交匯點為網路中的所有源在任何組範圍內提供單點控制。這可以和稱為接受暫存器過濾器的裝置一起使用。此過濾器的命令如下：

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

圖17:PIM-SM源控制

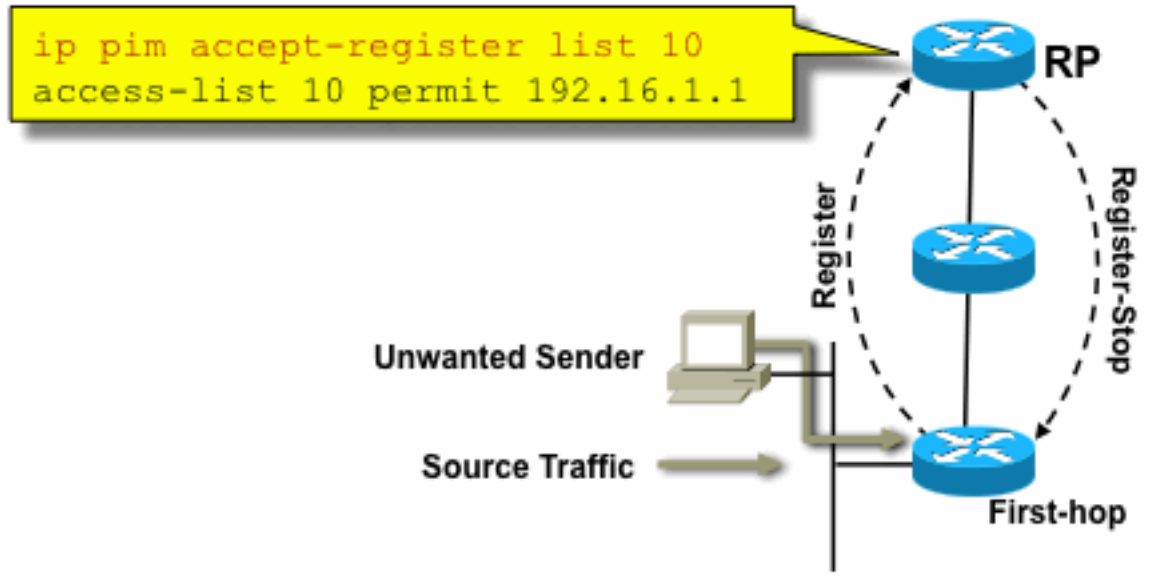


Fig17_PIMSM_Control

在PIM-SM網路中，可以使用此命令控制不需要的流量源。當源流量到達第一跳路由器時，第一跳路由器(DR)建立(S，G)狀態並向RP傳送PIM源暫存器消息。如果來源未列在accept-register過濾器清單（在RP上配置）中，則RP拒絕註冊，並將立即註冊停止消息傳送回DR。

在所示的示例中，簡單的ACL已應用到RP，RP僅過濾源地址。也可以在RP上使用擴展ACL來過濾源和組。

源過濾器有一些缺點，因為在RP上使用**pim accept-register**命令時，仍會在源的第一跳路由器上建立PIM-SM(S，G)狀態。這可能會導致在源本地接收器處產生流量，並且流量位於源和RP之間。此外，**pim accept-register** 命令在RP的控制平面上工作。這可用於使用虛假的註冊消息使RP過載，並可能導致DoS情況。

建議在RP上應用pim accept-register命令，以及其他方法，例如在所有的DR上、所有進入網路入口點上應用簡單的資料平面ACL。雖然在DR上的輸入ACL在配置完好並運行的網路中已經足夠，但建議在RP上配置**pim accept-register**命令，作為邊緣路由器上配置錯誤的次要安全機制。具有相同目標的分層安全機制稱為「深度防禦」，是安全領域的常見設計原則。

接收器問題 — 控制IGMP/MLD

大多數接收器問題屬於IGMP/MLD接收器協定互動領域。

圖18:控制IGMP

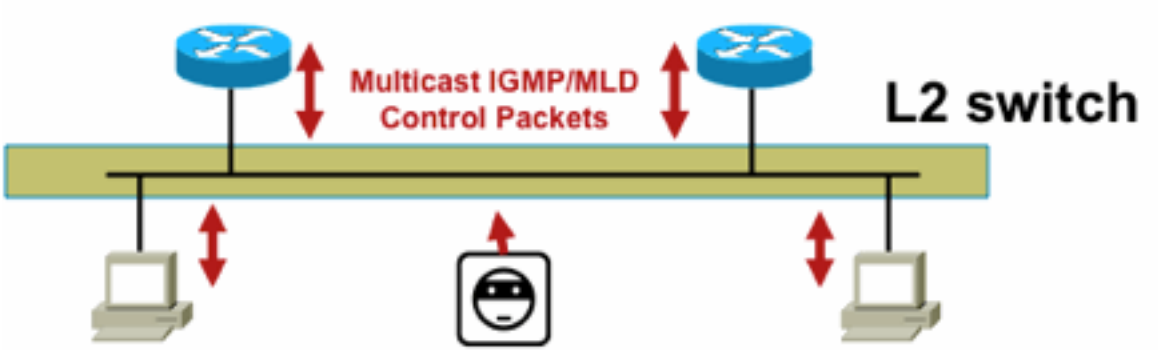


Fig18_Controlling_IGMP

過濾IGMP或MLD封包時，請記住以下幾點：

- IPv4:IGMP是IPv4通訊協定型別（IPv4通訊協定2）
- IPv6:MLD以ICMPv6協定型別資料包的形式傳輸

啟用IP組播後，IGMP進程預設啟用。IGMP資料包還攜帶這些協定，因此只要啟用了組播，就會啟用所有這些協定：

- PIMv1 - PIMv1是PIM的第一個版本，在Cisco IOS中始終啟用，用於遷移目的。當前部署全部使用PIMv2。
- Mrinfo - Mrinfo是Cisco IOS繼承的Unix命令，用於顯示組播鄰居。思科建議使用SNMP而不是mrinfo命令。
- DVMRP - DVMRP是一種傳統密集模式距離向量協定，其擴展特性非常有限。Cisco IOS對DVMRP的支援已停用或已棄用。
- Mtrace - Mtrace是單播「traceroute」的等價組播協定，是一個非常有用的工具

有關詳細資訊，請參見IANA的Internet組管理協定(IGMP)型別編號

```
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
```

單點傳播IGMP封包（針對IGMP/UDLR）可以過濾，因為這些封包很可能是攻擊封包且不是有效的IGMP通訊協定封包。Cisco IOS支援單點傳播IGMP封包，以支援單向連結和其他例外情況。

偽造的IGMP/MLD查詢資料包可導致IGMP版本低於預期。

特別地，理想情況下主機從不傳送IGMP查詢，因為以較低的IGMP版本傳送的查詢可能導致收到此查詢的所有主機恢復為較低版本。在IGMPv3/SSM主機存在的情況下，這可以「攻擊」SSM流。對於IGMPv2，這可能會導致更長的離開延遲。

如果存在具有單個IGMP查詢器的非冗餘LAN，路由器需要丟棄收到的IGMP查詢。

如果存在冗餘/通用被動LAN，則需要能夠進行IGMP監聽的交換機。在此案例中，有2個特定功能可以為您提供幫助：

- 路由器防護
- IGMP最低版本命令

路由器防護

如果交換器在該連線埠上收到多點傳送路由器控制封包（IGMP一般查詢、PIM Hello或CGMP Hello），則任何交換器連線埠均可成為多點傳送路由器連線埠。當交換器連線埠成為多點傳送路由器連線埠時，所有多點傳送流量都會傳送到該連線埠。可以使用「路由器防護」防止這種情況。路由器防護功能不需要啟用IGMP監聽。

路由器防護功能允許將指定的埠指定為組播主機埠。即使收到組播路由器控制資料包，該埠也無法成為路由器埠。

如果在已啟用Router Guard的連線埠上收到以下封包型別，則系統會捨棄這些封包型別：

- IGMP查詢消息
- IPv4 PIMv2訊息
- IGMP PIM消息(PIMv1)
- IGMP DVMRP消息
- 路由器埠組管理協定(RGMP)消息
- Cisco Group Management Protocol(CGMP)消息

當丟棄這些資料包時，更新統計資訊，指示由於路由器防護而丟棄資料包。

IGMP最低版本

可以配置允許的IGMP主機的最低版本。例如，您可以禁止所有IGMPv1主機或所有IGMPv1和IGMPv2主機。此篩選器僅適用於成員資格報告。

如果主機連線到一個通用的「被動」LAN（例如，不支援IGMP監聽的交換機，或者沒有針對它進行配置），則路由器除了忽略隨後觸發的「舊版本」成員身份報告而不回退自身之外，對此類錯誤查詢也無能為力。

由於IGMP查詢必須對所有主機可見，因此不能使用具有預共用金鑰(例如靜態金鑰IPSec)的基於雜湊的消息身份驗證(HMAC)機制來驗證來自「有效路由器」的IGMP查詢。如果兩個或多個路由器連線到一個公共LAN網段，則需要選擇IGMP查詢器。在這種情況下，唯一可用的過濾器是ip access-group filter，它基於傳送查詢的另一IGMP路由器的源IP地址。

必須允許「正常」組播IGMP資料包。

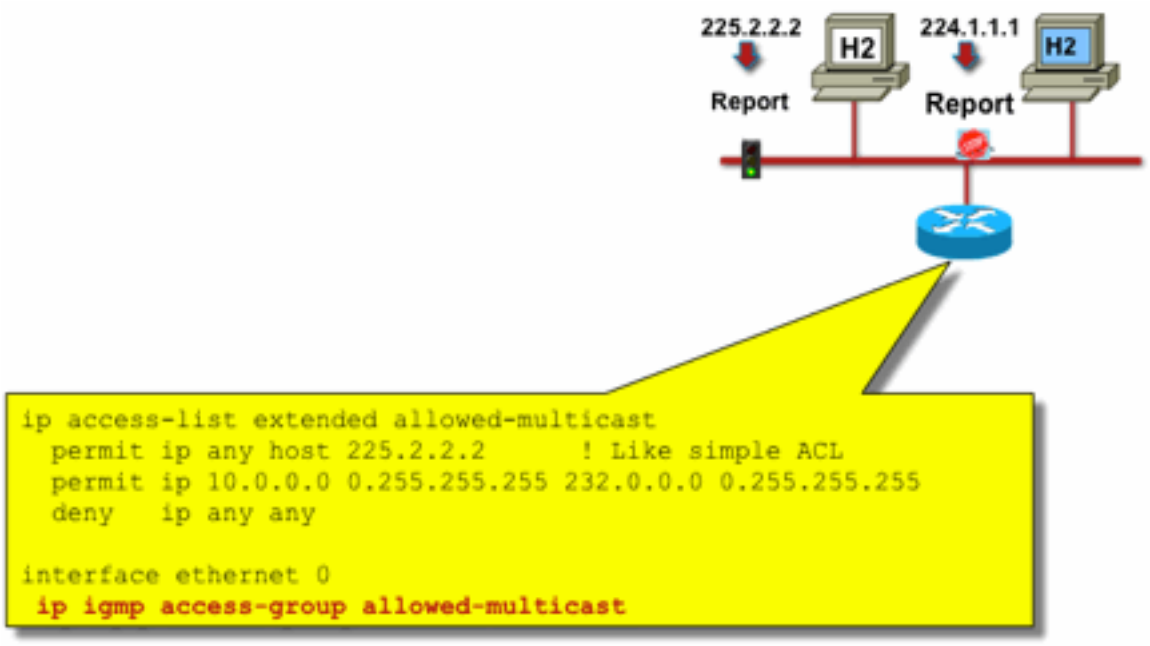
此過濾器可用於接收器埠，以僅允許「正常」IGMP資料包，並過濾已知的「不良」資料包：

```
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
```

附註：此型別的IGMP過濾器可用於接收ACL或CoPP。在這兩種應用中，都需要將其與過濾器結合使用，以用於處理其他流量，例如路由和管理平面協定。

圖19:主機接收器端存取控制



圖

19_Host_Receiver_Access

要過濾發往接收方的流量，不要過濾資料平面流量，而是過濾控制平面協定IGMP。由於IGMP是接收組播流量的必要前提，因此不需要資料平面過濾器。

特別是，您可以限制接收者可以加入的組播流（連線到配置該命令的介面）。 在這種情況下，請使用**ip igmp access-group/ipv6 mld access-group**命令：

ip igmp access-group / ipv6 mld access-group

對於ASM組，此命令僅根據目標地址進行過濾。然後會略過ACL中的來源IP位址。對於使用IGMPv3/MLDv2的SSM組，它會根據源IP和目標IP進行過濾。

此示例過濾所有IGMP揚聲器的給定組：

```
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
```

此示例針對給定組過濾特定的IGMP揚聲器（因此，特定的組播接收器）：

```
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
```

附註：請記住，對於ASM組，將忽略源。

准入控制

訪問控制可以為特定流量提供二進位制、是或否答案，與網路狀態無關。相對而言，准入控制限制了傳送方/接收方可以使用的資源數量，假定它們通過了訪問控制機制。在組播環境中，各種裝置可用於幫助進行准入控制。

全域性和每個介面的IGMP限制

在最靠近感興趣的組播接收器的路由器上，有可能限制全域性和每個介面加入的IGMP組數。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> ]
```

建議始終為每個介面以及全域性配置此限制。在每種情況下，限制是指IGMP快取中的條目計數。

接下來的兩個示例展示如何使用此命令幫助限制住宅寬頻網路邊緣的組數。

示例1 — 將接收組限製為僅包含SDR通知和一個接收管道

會話目錄(SDR)充當某些組播接收器的通道指南。如需詳細資訊，請參閱RFC 2327。

常見的要求是限制接收器接收SD組加一個通道。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
```

本示例中的訪問清單僅指定通道指南；全域性**ip igmp limit**命令將每個IGMP源限製為單個(1)通道，但不包括始終可以接收的通道指南。interface命令會覆蓋全域性命令，並且除了通道指南外，還允許在此介面上接收兩(2)個通道。

範例2 — 彙總 — DSLAM連結上的許可控制

此命令還可用於提供某種形式的頻寬准入控制。例如，如果必須分配300個SDTV頻道（每個頻道為4Mbps），並且有1Gbps鏈路連線到Digital-Subscriber-Line-Access-Multiplexer(DSLAM)，則您可以作出策略決定，將電視頻寬限製為500 Mbps，而將剩餘部分留給Internet和其他用途。在這種情況下，您可以將IGMP狀態限製為500 Mbps/4 Mbps = 125 IGMP狀態。

在此情況下可以使用以下設定：

圖20:使用每個介面的IGMP限制；Agg-DSLAM鏈路上的准入控制

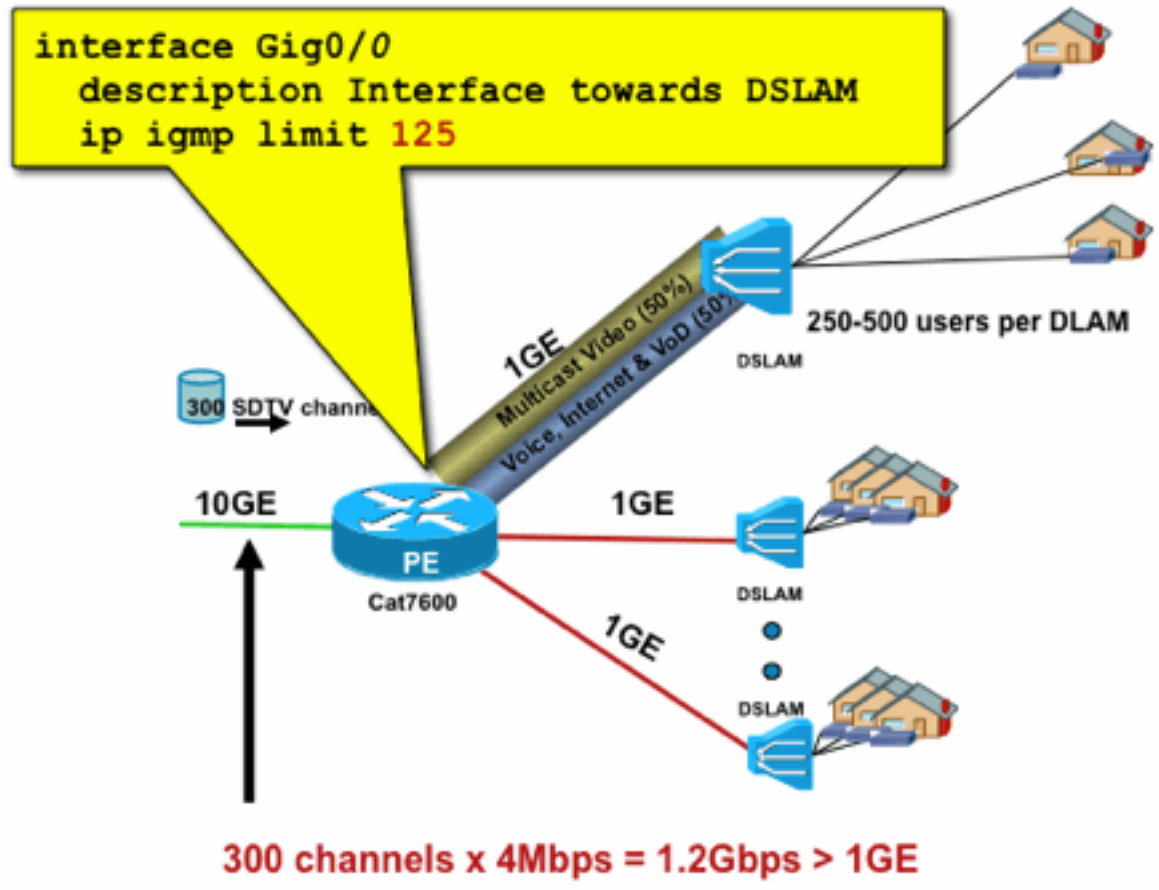


Fig20_PerInterface_IGMP

每個介面的mroute限制

啟用每個介面的mroute狀態限制是一種更通用的准入控制形式。它不僅在傳出介面上限制IGMP和PIM狀態，還提供了一種對傳入介面進行狀態限制的方法。

使用**ip multicast limit**命令：

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

可在輸入和輸出介面上單獨限制狀態。直接連線的源狀態也可以使用「已連線」關鍵字進行限制。以下範例說明此命令的使用方式：

示例1 - Agg-DSLAM鏈路上的出口准入控制

在此示例中，有300個SD電視頻道。假設每個SD通道需要4 Mbps，總速率不超過500 Mbps。最後，還假設需要支援基本、擴展和高級捆綁包。頻寬分配示例：

- 60% / 300 Mbps（基本）
- 20% / 100 Mbps擴展
- 20% / 100 Mbps高級版

然後每個通道使用4 Mbps，將DSLAM上行鏈路限製為：

- 基本75個州
- 擴展的25個狀態
- 溢價25狀態

配置從PEAgg面向DSLAM的出站介面的限制：

圖21:使用每個介面的mroute限制；Agg-DSLAM鏈路上的准入控制

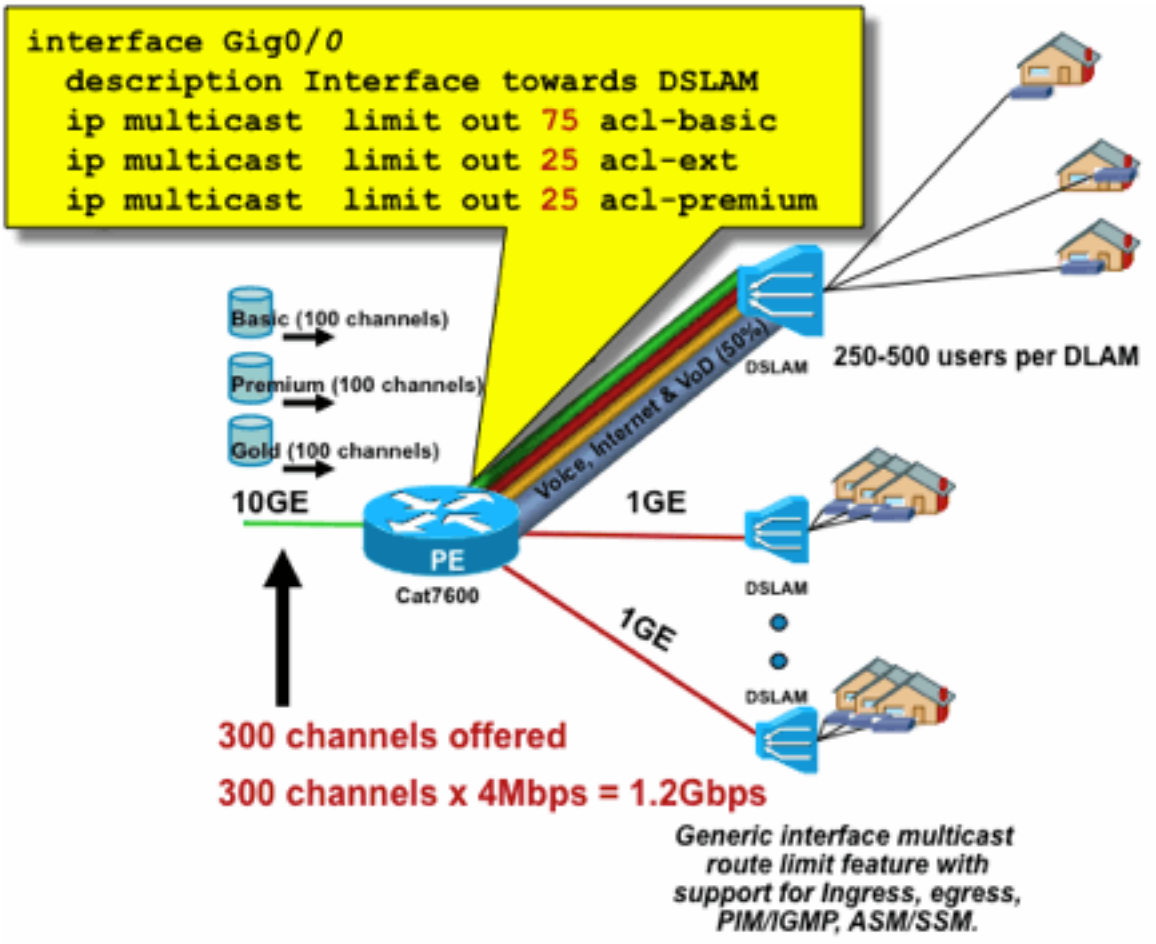


圖 *21_PerInterface_Mroute*

範例2 - Agg-DSLAM連結上的輸入許可控制

除了上游裝置的出站介面上的「外寄」限制之外，還可以對下游裝置的RPF介面使用RPF限制。這實際上與先前的範例具有相同的結果，如果下游裝置不是Cisco IOS裝置，則此結果可能會很有用。

圖22:使用每個介面的mroute限制；輸入許可控制

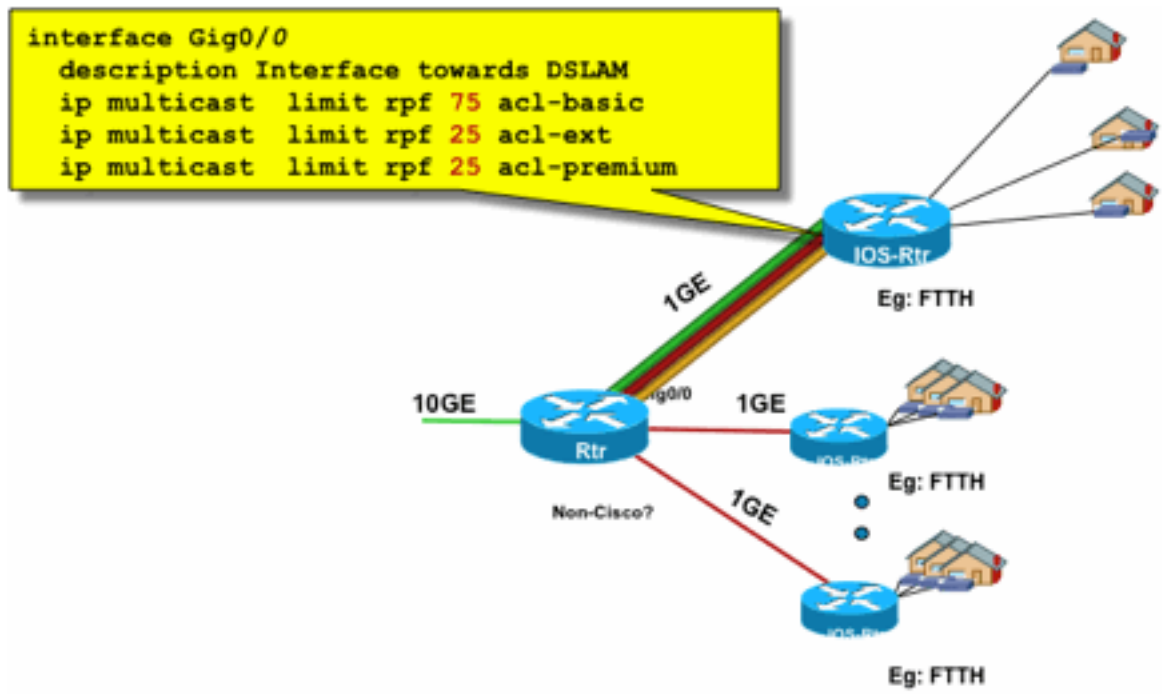


Fig22_PerInt

erface_Mroute_inputControl

示例3 — 基於頻寬的限制

您可以在多個內容提供商之間進一步劃分訪問頻寬，並為每個內容提供商提供到DSLAM的上行鏈路頻寬的公平份額。在這種情況下，請使用**ip multicast limit cost**命令：

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

使用此命令，可以將「開銷」（使用「乘數」中指定的值）歸為ip組播限制中任何與擴展ACL匹配的狀態。

此命令是全域性命令，可以配置多個同時開銷。

在此示例中，必須支援三個不同的內容提供商，他們每個人都可以公平地訪問網路。此外，在本示例中，要求支援各種型別的運動影象專家組(MPEG)流：

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

在這種情況下，您可以將頻寬成本分配給每種流型別，並在具有此配置的三個內容提供商之間共用750 Mbps的其餘部分：

```
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
```

圖23:每個介面的Mroute狀態限制的成本係數

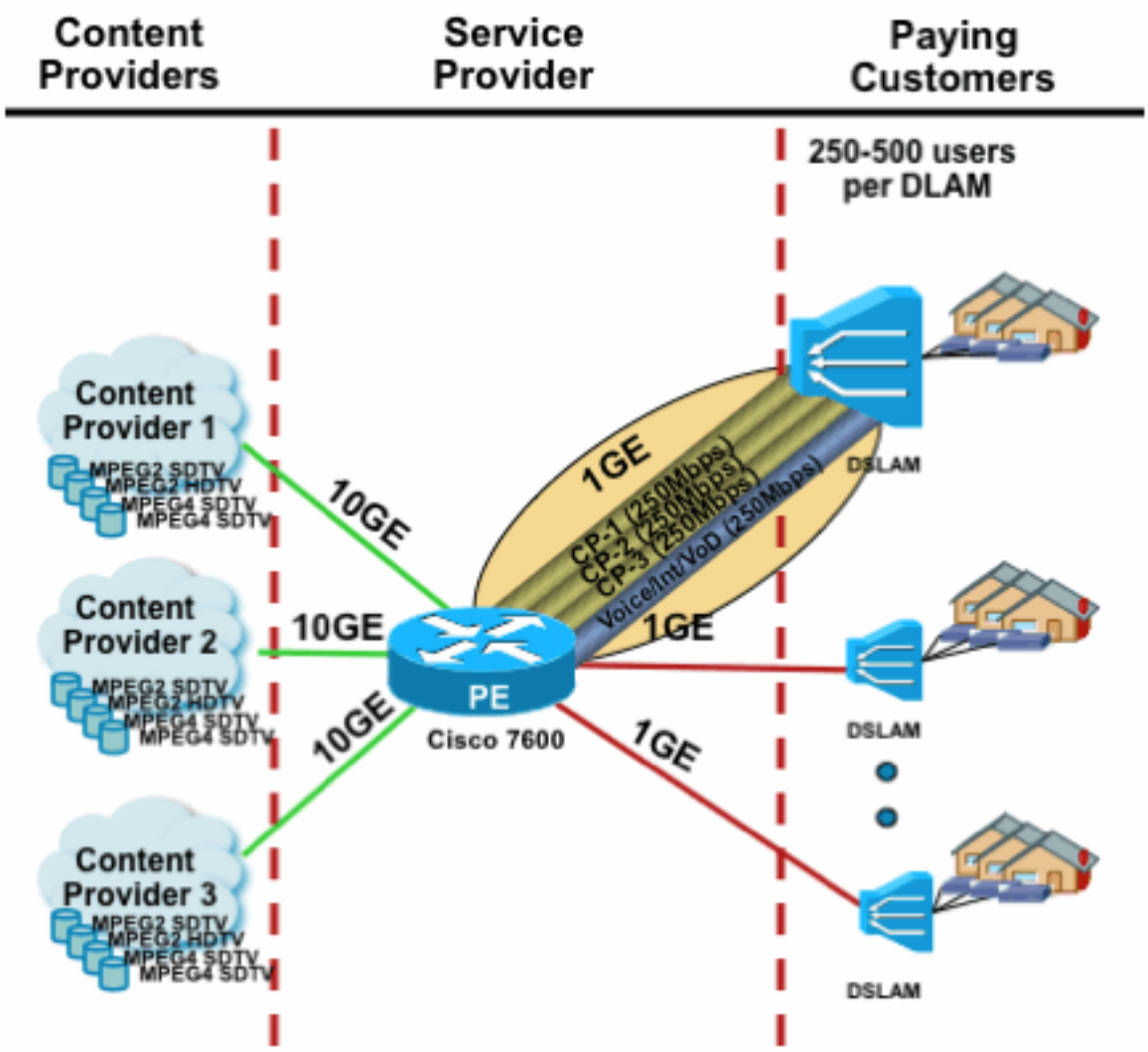


Fig23_Cost_P

erInterface

組播和IPSec

GET VPN簡介

與單播一樣，組播流量有時也需要加以保護以提供機密性或完整性保護。可能需要提供此類服務的兩個主要領域：

- 對組播流的加密（例如在將機密資料流到使用組播的大型接收器的銀行應用程式中）— 這就是資料平面安全。
- 例如，對使用組播、OSPF或PIM的控制平面協定的加密 — 這就是控制平面安全。

IPSec作為一種通訊協定[RFC 6040、7619、4302、4303、5282]，特別限制於單點傳播流量（由RFC）。 兩個單播對等體之間建立了「安全關聯」(SA)。若要將IPSec套用至多點傳播流量，其中一個選項是封裝在GRE通道中的多點傳播流量，然後將IPSec套用至GRE通道（單點傳播）。較新的方法使用在組的所有成員之間建立的單一安全關聯。解釋的組域(GDOI)[RFC 6407]定義了如何實現。

基於GDOI，思科開發了一種稱為組加密傳輸(GET)VPN的技術。此技術使用文檔「draft-ietf-msec-ipsec-extensions」中定義的「具有地址保留的隧道模式」。在GET VPN中，首先在組的所有成員

之間建立組安全關聯。隨後，使用ESP（封裝的安全負載）或AH（身份驗證報頭）保護流量，該模式使用具有地址保留的隧道模式。

總之，GET VPN封裝使用原始報頭地址資訊的組播資料包，然後使用ESP保護與組策略相關的內部資料包。

GET VPN的優勢在於組播流量完全不受安全封裝機制的影響。路由的IP報頭地址與原始IP報頭相同。無論是否使用GET VPN，組播流量都可以以相同的方式得到保護。

應用於GET VPN節點的策略在組金鑰伺服器上集中定義，並分發到所有組節點。因此，所有組節點都具有相同的策略，且將相同的安全設定應用於組流量。與標準IPSec類似，加密策略定義哪種型別的流量需要以何種方式受到保護。這允許GET VPN用於各種用途。

使用GET VPN加密組播資料平面流量

在組金鑰伺服器上設定網路範圍的加密策略，並將其分發到GET VPN終端。策略包含IPSec策略(IPSec模式 — 此處：帶有報頭保留的隧道模式)，以及要使用的安全演算法（例如AES）。 它還包含一個策略，描述哪些流量可以受到保護，如ACL所定義。

GET VPN可用於組播和單播流量。ACL可以定義保護單播流量的策略：

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

這會對來源IP為10/8且目的地IP為10/8的所有流量進行加密。GET VPN會忽略所有其他流量，例如從10/8到另一個地址的流量。

GET VPN在組播流量方面的應用技術相同。例如，此訪問控制條目(ACE)可用於保護從任何源到相應組播組的流量：

```
permit ip any 239.192.0.0 0.0.255.255
```

此策略匹配所有源(「any」)和以239.192開頭的所有組播組。流向其他組播組的流量不安全。

> **附註**：加密型ACL的構造必須引起足夠的重視。必須將管理流量，或源自GET VPN域之外但在內部終止的流量（即僅通過一個加密端點的流量）排除在GDOI策略之外。

常見的錯誤包括：

- permit ip any 224.0.0.0 0.255.255.255:這也會加密OSPF流量和其他控制平面流量，例如目的地為對等路由器。
- 管理流量不排除在加密策略之外，加密策略在網路中終止。其中包括GDOI流量本身。

使用GET VPN驗證控制平面流量

通常最佳做法是對控制平面流量（例如路由協定）進行身份驗證，以確保消息來自受信任的對等體。對於使用單播的控制平面協定（例如BGP），這相對簡單。但是，許多控制平面協定使用組播流量。例如OSPF、RIP和PIM。有關完整清單，請參閱IANA的IPv4組播地址空間註冊。

其中一些協定具有內建身份驗證，如路由資訊協定(RIP)或增強型內部組路由協定(EIGRP)，其他協定則依靠IPSec提供此身份驗證（例如OSPFv3、PIM）。 對於後一種情況，GET VPN提供了一種

可擴展的方法來保護這些協定。在大多數情況下，要求是協定消息身份驗證，或者換句話說，驗證消息是由受信任的對等體傳送的。但是，GET VPN也允許加密此類消息。

要保護此類控制平面流量（通常僅進行身份驗證），需要使用ACL描述流量並將其包括在GET VPN策略中。詳細資訊取決於要保護的通訊協定，其中需要留意ACL是否包括僅通過輸入GET VPN節點（已封裝）或也通過輸出節點的流量。

保護PIM協定有兩種基本方法：

- **permit ip any 224.0.0.13 0.0.0.0**:這是「所有PIM路由器」組播組。但是，這並不能保護單播PIM消息
- **permit pim any**:這可以保護PIM協定，與使用組播還是單播無關

  附註：這些命令作為示例提供，可幫助解釋一個概念。例如，必須排除某些用於引導PIM的PIM協定，如BSR或自動RP。這兩種方法都有一定的優點和不便，它們依賴於部署。有關詳細資訊，請參閱有關如何使用GET VPN保護PIM的特定文獻。

結論

組播是網路中越來越常見的一種服務。住宅/家庭寬頻網路中的IPTV服務的出現，以及在世界許多金融市場向電子交易應用的發展僅僅是要求組播成為絕對要求的兩個例子。組播具有各種不同的配置、操作和管理挑戰。其中一個關鍵挑戰是安全。

本文考察了多種可以保護組播的方法：

- 首先，檢視整個組播控制和資料平面，解釋與單播的差異如何帶來新的安全挑戰。
- 接下來，對多星網路中遇到的主要協定（特別是IGMP、PIM和MSDP）進行了一些詳細的檢查。每種情況下都提供了安全威脅的描述以及針對這些威脅推薦的最佳緩解方法。
- 此外，還舉例說明在某些特定應用中如何保護多點傳送，例如寬頻邊緣網路，與特定視訊流可能需要的頻寬量相比，其頻寬可能有限。
- 最後，GET VPN架構被描述為與IPSec整合的組播方式，用於傳送安全VPN。

考慮到組播安全，請記住它與單播的不同之處。組播傳輸基於動態狀態的建立，組播涉及動態資料包複製，組播響應PIM JOIN / PRUNE消息建立單向樹。整個環境的安全涉及瞭解和部署豐富的Cisco IOS命令框架。這些命令主要圍繞保護協定操作、狀態（組播）或針對諸如CoPP等資料包的策略器為中心。正確使用這些命令可以為IP組播提供強大的保護服務。

綜上所述，本文提出並描述了多種方法：

1. SSM的廣泛使用 — 這是最簡單的PIM模式，也允許使用(S，G)轉發。
2. 如果需要ASM服務，請確保可以提供強大的服務 — 使用靜態定義的RP比動態RP通告提供更安全的控制平面。自動RP和BSR更靈活
3. 如果啟用PIM-SM，請檢視存在特定漏洞的區域（例如RP的註冊隧道），並確保DR始終受到良好的保護。CoPP在這些領域非常有用。
4. 如果需要域間ASM服務，請考慮是否可以部署BiDir PIM。
5. 使用全域性mroute/igmp狀態限制 — 瞭解您的平台的功能，以及在正常情況下和最壞情況下所需的預期最大狀態量。在平台功能內配置限制，使網路能夠最大程度地運行。
6. 基本過濾器 — rACL/CoPP和基礎設施ACL，它們會阻止接入層的PIM

IP組播是一種令人興奮的可擴展方式，可用於提供各種應用服務。與單播一樣，它需要在各種不同

區域進行保護。本文提供了保護IP組播網路的基本構建塊。

相關資訊

- 企業IP組播地址分配指南
- 配置IPv4 IGMP過濾器
- 群組加密傳輸VPN

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。