218004-secure-ip-multicast-deployments

内容

はじめに

このドキュメントでは、IPマルチキャストネットワークインフラストラクチャを保護するためのベストプラクティスに関する一般的なガイダンスについて説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- IP マルチキャスト

使用するコンポーネント

このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

このドキュメントでは、基本的な概念と用語について説明し、次のトピックについて説明します。

- 特定のプラットフォームおよびネットワーク全体を保護するメカニズム。
- 任意のソースマルチキャスト(ASM)モデルとSource Specific Multicast(SSM)モデル

- マルチキャスト仮想プライベートネットワーク(MVPN)セキュリティ。
- Group Encrypted Transport(GET)Virtual Private Network(VPN)アーキテクチャは、マルチキャストデータプレーンまたはコントロールプレーントラフィックの機密性と整合性を提供します。

用語

IPマルチキャストには、次の2つの従来のサービスモデルがあります。

1.任意の送信元マルチキャスト(ASM)

2. Source Specific Multicast(SSM)

ASMでは、受信者はInternet Group Membership Protocol(IGMP)またはMulticast Listener Discovery(MLD)メンバーシップレポートを介してグループGに参加し、グループを示します。このレポートは、任意の送信元からグループGに送信されるトラフィックを要求するため、「any source」という名前が付けられます。 これに対して、SSMでは、受信側は送信元Sによって定義された特定のチャネルに参加し、送信元Sはグループ G に送信します。これらの各サービスモデルについて、以下で詳しく説明します。

任意の送信元マルチキャスト

ASMモデルの特徴は、「稠密モードのフラッドアンドプルーニング」と「希薄モードの明示的結合」という2つのプロトコルクラスです。

i)デンスモードのフラッドアンドプルーニングプロトコル(DVMRP/MOSPF/PIM-DM)

稠密モードプロトコルでは、ネットワーク内のすべてのルータがすべてのツリー、その送信元と受信側を認識します。Distance Vector Multicast Routing Protocol(DVMRP)やProtocol Independent Multicast(PIM)デンスモードなどのプロトコルは、特定のツリーに対するトラフィックが不要なトポロジ部分に「プルーニング状態」を作成することで、ネットワーク全体に「アクティブソース」情報をフラッディングし、ツリーを構築します。フラッドアンドプルーニングプロトコルとも呼ばれます。Multicast Open Shortest Path First(MOSPF)では、受信側に関する情報がネットワーク全体にフラッディングされ、ツリーの構築がサポートされます。

ネットワークの一部に組み込まれたすべてのツリーによって、ネットワーク内（または設定されている場合は管理スコープ内）のすべてのルータでリソースの使用率が常に（コンバージェンスの影響とともに）発生する可能性があるため、高密度モードプロトコルは望ましくありません。これらのプロトコルについては、この記事の後半では詳しく説明しません。

ii)スパースモード明示的参加プロトコル(PIM-SM/PIM-BiDir)

スパースモードの明示的参加プロトコルでは、受信側がグループの明示的なIGMP/MLDメンバーシップレポート（または「参加」）を送信しない限り、デバイスはネットワーク内にグループ固有の状態を作成しません。このASMのバリエーションは拡張性が高いことで知られており、マルチキャストパラダイムに重点が置かれています。

これがPIM-Sparseモードの基礎であり、これまではほとんどのマルチキャスト展開で使用されていました。これは、双方向PIM(PIM-BiDir)の基盤でもあります。双方向PIMは、MANY（送信元）からMANY（受信者）のアプリケーションに対して展開されることが増えています。

これらのプロトコルは、「スパース」レシーバ群を持つIPマルチキャスト配信ツリーを効率的にサポートし、送信元とレシーバ間のパスにあるルータ上と、ランデブーポイント(RP)であるPIM-SM/BiDir上でのみコントロールプレーンステートを作成するため、スパースモードと呼ばれます。ネットワークの他の部分で状態が発生することはありません。ルータ内のステートは、ダウンストリームルータまたはレシーバから参加を受信した場合にのみ明示的に構築されます。そのため、「明示的な参加プロトコル」という名前が付けられます。

PIM-SMとPIM-BiDirの両方で「SHARED TREES」が採用されており、任意の送信元からのトラフィックを受信側に転送できます。共有ツリー上のマルチキャスト状態は(*,G)状態と呼ばれ、*はANY SOURCEのワイルドカードです。さらに、PIM-SMは、特定の送信元からのトラフィックに関連する状態の作成をサポートします。これらはSOURCE TREESと呼ばれ、関連付けられた状態は(S,G)状態と呼ばれます。

Source-Specificマルチキャスト

SSMは、受信側（または一部のプロキシ）が(S,G)を「join」して、送信元Sからグループ Gに送信されたトラフィックを受信することを示すときに使用されるモデルです。これは、IGMPv3/MLDv2の「INCLUDE」モードメンバーシップレポートで可能です。このモデルは、Source-Specific Multicast(SSM)モデルと呼ばれます。SSMでは、ルータ間での明示的加入プロトコルの使用が義務付けられています。この標準プロトコルはPIM-SSMで、(S,G)ツリーの作成に使用されるPIM-SMのサブセットです。SSMには共有ツリー(*,G)状態はありません。

したがって、マルチキャスト受信側はASMグループGに「参加」、またはSSM(S,G)チャネルに「参加」（あるいはより正確に「サブスクライブ」）できます。「ASMグループまたはSSMチャネル」という用語の繰り返しを避けるために、（マルチキャスト）フローという用語が使用されます。これは、フローがASMグループまたはSSMチャネルであることを意味します。

関連するマルチキャストプロトコル/パケットタイプ

マルチキャストネットワークを保護するには、一般的に発生するパケットの種類と、それらから保護する方法を理解することが重要です。主に3つのプロトコルに注意する必要があります。

1. IGMP/MLD

(2)PIM

(3)MSDP

次のセクションでは、これらの各プロトコルと、各プロトコルで発生する可能性のある問題について説明します。

IGMP/MLDパケット

IGMP/MLDは、マルチキャスト受信側が、特定のマルチキャストグループのコンテンツを受信するようにルータに信号を送信するために使用するプロトコルです。Internet Group Membership Protocol(IGMP)はIPv4で使用されるプロトコルで、Multicast Listener Discovery(MLD)はIPv6で使用されるプロトコルです。

一般的に展開されているIGMPには、IGMPv2とIGMPv3の2つのバージョンがあります。また、一般的に導入されているMLDには、MLDv1とMLDv2の2つのバージョンがあります。

IGMPv2とMLDv1は機能的に同等であり、IGMPv3とMLDv2は機能的に同等です。

これらのプロトコルは、次のリンクで指定されます。

IGMPv2:RFC 2236

MLDv1:RFC 3590

IGMPv3およびMLDv2:RFC 4604

IGMPv2とIGMPv3はプロトコルであるだけでなく、IPv4 IPプロトコル（具体的にはプロトコル番号2）でもあります。これらのRFCで説明されているように、マルチキャストグループメンバーシップを報告するためだけでなく、DVMRP、PIMバージョン1、mtrace、mrinfoなどの他のIPv4マルチキャストプロトコルでも使用されます。これは、(Cisco IOS® ACLなどを使用して)IGMPをフィルタリングしようとする際に覚えておくことが重要です。IPv6では、MLDはIPv6プロトコルではなく、ICMPv6を使用してMLDパケットを伝送します。PIMバージョン2は、IPv4とIPv6（プロトコル番号103）で同じプロトコルタイプです。

PIM制御パケット

このセクションでは、マルチキャストおよびユニキャストPIM制御パケットについて説明します。PIM-SMネットワークでランデブーポイント(RP)を選出し、グループ間の割り当てを制御する方法である、Auto-RPとブートストラップルータ(BSR)について説明します。

マルチキャストPIM制御パケット

マルチキャストPIM制御パケットには次のものがあります。

- PIM Hello:PIM Helloパケットは、PIMネイバーを確立するために同じネットワークに接続されたルータに送信される、リンクローカルスコープのIPマルチキャストパケットです。
- PIM Join/Prune:PIM Join/Pruneは、マルチキャスト状態を作成または削除するために送信されるリンクローカルスコープのIPマルチキャストパケットであり、PIMネイバーにのみ送信されます。これらは、アサート、レポート抑制、およびその他のPIMプロトコルの詳細を容易にするためにLAN内でマルチキャストですが、常に特定のネイバーに送信されます。
- PIM DF-elect:PIM指定フォワーダは、接続されたレシーバまたはダウンストリームPIMネイバーに代わってRPに送信される(*,G)JOINを処理する双方向PIMルータです。PIMルータが

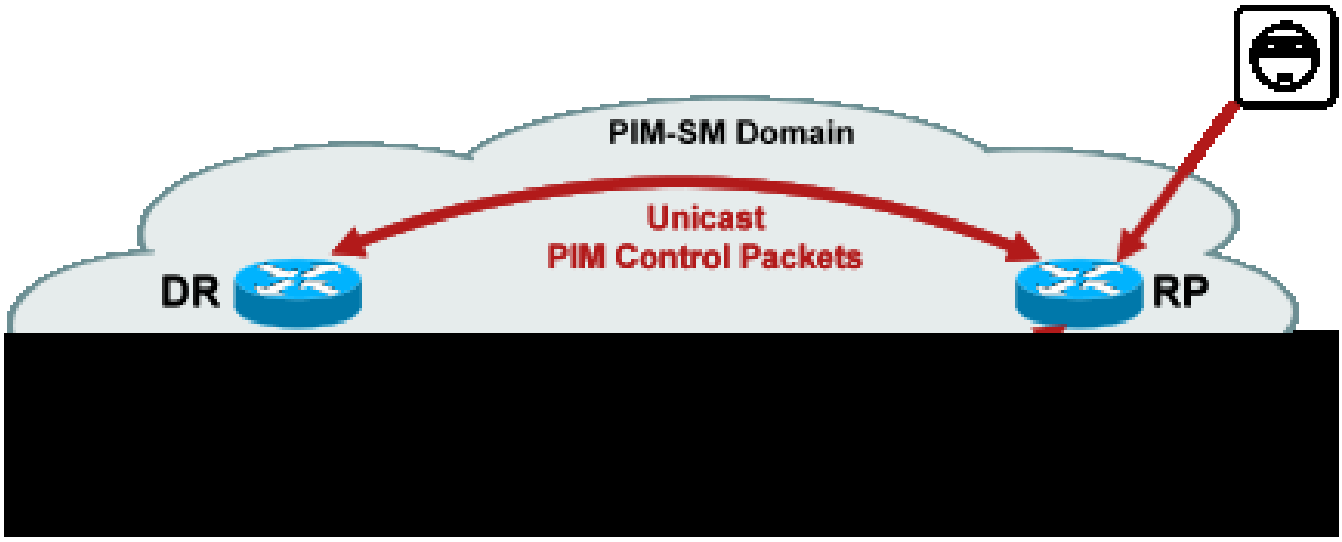
、同じグループGの同じセグメントで(*,G) JOINを送信する別のルータを検出した場合、RPへのベストパスを持つルータを判別するための選択があります。
- PIMアサート:PIMアサートは、特定のインターフェイスから特定(S,G)のパケットをアクティブに転送するネットワークセグメントに接続されたPIMルータが、転送される同じインターフェイスでその同じ(S,G)のパケットを受信し始めたときに送信されるリンクローカルIPマルチキャストパケットです。このイベントは、この(S,G)のシングルフォワーダ(SF)と見なされる別のルータが存在することを示します。アサートメカニズムは、その(S,G)に対して一意のSFを選択します。PIM SFルータは、特定の(S,G)ストリームのパケットを転送するように選択されます。PIMでは、異なるルータが異なる(S,G)の代わりにSFの役割を果たすことができます。理想的には、(S,G)ごとに1つのSFしかありません。SFと代表ルータを混同しないでください。PIM代表ルータ(DR)は、PIM-SMネットワークのRPに送信されるJOIN / PRUNESまたはSOURCE REGISTERSを担当するルータです。
- PIMブートストラップ:PIMブートストラップメッセージは、特定のグループGのランデブーポイント(RP)の動的な選択を容易にするためにPIMv2ネットワークで送信されます。

ユニキャストPIM制御パケット

ユニキャストPIM制御パケットは、RPに対して送受信され、次の内容が含まれます。

- Source Register Packet：ランデブーポイントに新しいマルチキャストソースを登録するためにPIMソースレジスタパケットが送信されます。送信元がマルチキャストパケットの送信を開始すると、送信元ネットワークに接続されている代表ルータ(DR)からRPにユニキャスト登録ストリームが送信され、RPが担当するマルチキャストグループに対してアクティブな送信元が存在することが示されます。
  ソースレジスタパケットは、元のマルチキャストストリームのユニキャストカプセル化として送信されます。
  PIM登録メッセージはプロセスレベルでスイッチングされ、RPがregister stopメッセージを送信するまで送信されません。これらのパケットのパフォーマンスへの影響は、送信元のレート((S,G)フローごと)に比例します。
- Register Stop Packet:PIM Register Stopパケットは、ランデブーポイント(RP)から、Registerメッセージを送信したPIM DRに送信されます。Register Stopメッセージは、RPが送信元からのマルチキャストパケットをネイティブに受信し始めるとすぐに送信されます。
- BSR Candidate-Rendezvous Point Advertisement Packet:PIM BSR C-RP-Advertisement Packetは、BSRが選出されると、BSRに送信されて候補RPをアドバタイズします。

図1:PIMユニキャストパケット



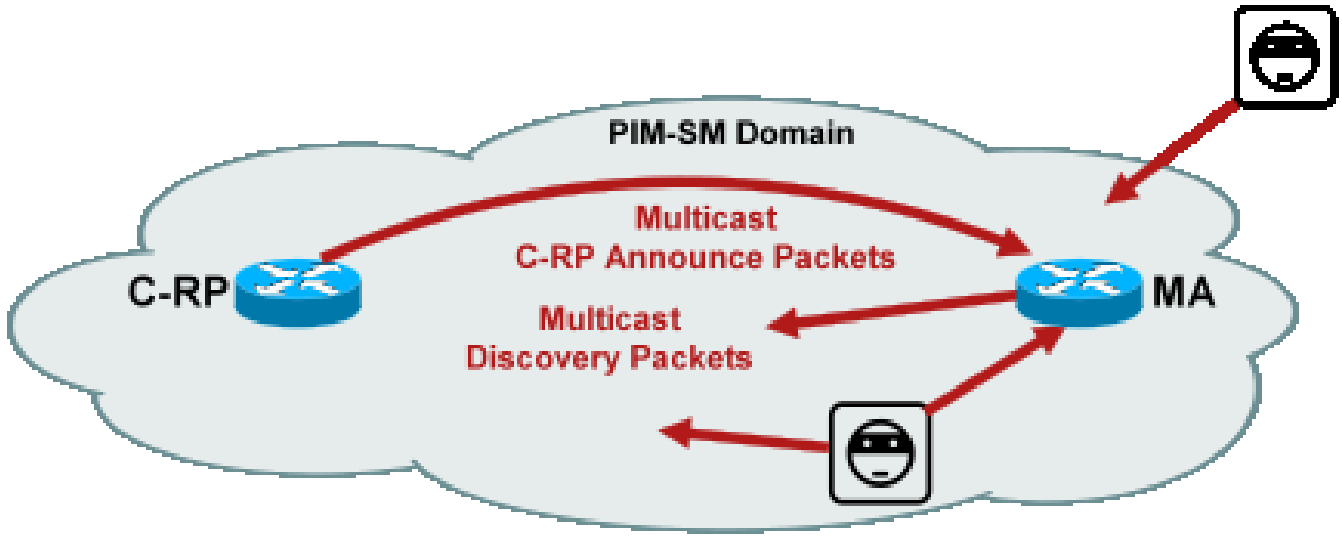
これらのパケットはユニキャストであるため、このようなパケットを悪用する攻撃はどこからでも発生する可能性があります。

Auto-RPパケット

Auto-RPは、PIMv2 BSRと同じ目的で動作するシスコが開発したプロトコルです。Auto-RPはBSRより前に開発されており、IPv4のみをサポートします。BSRはIPv4とIPv6をサポートします。Auto-RPのMapping Agentは、BSRのブートストラップルータと同じ機能を果たします。BSRでは、C-RPからのメッセージはブートストラップルータへのユニキャストです。Auto-RPでは、メッセージはマルチキャストを介してMapping Agentに送信されます。これにより、後述するように、境界でのフィルタ処理が容易になります。Auto-RPの詳細については、http://www.cisco.com/c/en/us/td/docs/ios/solutions_docs/ip_multicast/White_papers/rps.htmlを参照してください。

Cisco IOSでは、AutoRP/BSRパケットは常に転送され、現在は無効にされていません。これは、Auto-RPの場合、特定のセキュリティ上の問題を引き起こす可能性があります。

図2:Auto-RPパケット



注:Auto-RPはPIM-SM RPアナウンスおよびディスカバリのメカニズムとして使用されていますが、PIMパケット（IPプロトコル103）を使用せず、代わりにマルチキャストアドレスでユーザデータグラムプロトコル(UDP)ポート496パケットを使用します。

Auto-RPでは、次の2つのパケットタイプが使用されます。

- C-RP-Announceパケット：これらのパケットはすべてのマッピングエージェントに対してマルチキャストであり、Internet Assigned Numbers Authority(IANA)によって予約された「既知の」アドレス(224.0.1.39)を使用します。これらはC-RPから送信され、RPがRPとして動作できるRPアドレスとグループ範囲をアナウンスします。
- C-RPディスカバリパケット：これらのパケットはすべてのPIMルータに対してマルチキャストであり、IANAによって予約された「既知の」アドレス(224.0.1.40)を使用します。これらはAuto-RPマッピングエージェントによって送信され、特定のグループ範囲のRPとして選択された特定のC-RPをアナウンスします。

これらのパケットタイプは、それぞれネットワークを通じてフラッディングされることを目的としています。

Cisco IOSでは、グループがRP情報の配布に使用される際に、そのグループに関するRPの事前認識がないという問題を回避するために、224.0.1.39と224.0.1.40の両方がPIMデンスモードで転送されます。これは、PIMデンスモードの唯一の推奨される使用方法です。

Cisco IOS XRでは、Auto-RPメッセージはReverse Path Forwarding（RPF；リバースパス転送）によってネイバーからネイバーへホップ単位でフラッディングされます。したがって、Cisco IOS XRでAuto-RPをサポートするためにPIM DM mroute状態を作成する必要はありません。実際、Cisco IOS XRはPIM-DMをまったくサポートしていません。

Multicast Service Discovery Protocol(MSDP)パケット

MSDPは、あるドメイン内の送信元をそれぞれのランデブーポイントを介して別のドメイン内の受信者にアナウンスできるようにするIPv4プロトコルです。MSDPはRFC 3618で指定されています。

PIMドメイン間でアクティブな送信元に関する情報を共有するには、MSDPが使用されます。あるドメインで送信元がアクティブになった場合、MSDPによってすべてのピアドメインがこの新しい送信元についてタイムリーに学習するため、他のドメインの受信者は、受信者が関心を持つグループに送信した場合でも、この新しい送信元とすばやく連絡を取ることができます。MSDPはASM/PIM-SMマルチキャスト通信に必要で、各ドメインのランデブーポイント間に設定されたユニキャストTransport Control Protocol(TCP)接続上で動作します。

マルチキャスト環境における脅威

信頼ゾーンと信頼境界

このセクションは、ネットワーク内の機能エンティティ別に構成されています。ここで説明する脅威モデルは、これらのエンティティを中心に形成されています。たとえば、このドキュメントでは、ルータの配置場所に関係なく、マルチキャストネットワーク内のルータを（マルチキャストの観点から）保護する方法について説明します。同様に、ネットワーク全体のセキュリティ対策、または代表ルータやランデブーポイントでの対策の導入方法についても考慮する必要があります

ここで説明する脅威もこのロジックに従い、ネットワーク内の論理機能別に整理されます。

脅威の概要

抽象的なレベルでは、あらゆるマルチキャスト展開が、セキュリティのさまざまな側面に関する多数の脅威の影響を受ける可能性があります。セキュリティの重要な側面は、機密性、整合性、および可用性です。

- 機密性に対する脅威：ほとんどのアプリケーションでは、マルチキャストトラフィックは暗号化されないため、パス内の任意の回線またはネットワーク要素でリッスンまたはキャプチャを行う任意のユーザに対してオープンです。「GET VPN」の項では、このような攻撃を防ぐためにマルチキャストトラフィックを暗号化する方法について説明しています。
- トラフィックの整合性に対する脅威：アプリケーションレベルのセキュリティまたはGET VPNなどのネットワークベースのセキュリティを使用しないと、マルチキャストトラフィックは送信中に変更される可能性があります。これは、OSPF、PIM、およびその他の多くのプロトコルなど、マルチキャストを使用するコントロールプレーントラフィックにとって特に重要です。
- ネットワークの完全性に対する脅威：このドキュメントで説明されているセキュリティメカニズムがないと、許可されていない送信者、受信者、または侵害されたネットワーク要素がマルチキャストネットワークにアクセスしたり、許可されていないトラフィックの送受信（サービスの盗難）やネットワークリソースの過負荷が発生する可能性があります。
- アベイラビリティに対する脅威：正当なユーザがリソースを使用できないようにするために、サービス拒否攻撃が数多く発生する可能性があります。

次のセクションでは、ネットワーク内の各論理機能の脅威について説明します。

ルータに対する基本的な脅威

ルータに対する基本的な脅威は数多く存在しますが、それらはルータがマルチキャストをサポートするかどうか、および攻撃がマルチキャストトラフィックやプロトコルに関係するかどうかに

は関係ありません。

サービス拒否(DoS)攻撃は、ネットワーク内で最も重要な一般的な攻撃ベクトルです。原則として、すべてのネットワーク要素がDoS攻撃の対象となり、正当なユーザに対するサービスが失われたり低下したりする可能性があるため、要素が過負荷になる可能性があります。ユニキャストに適用される基本的なネットワークセキュリティの推奨事項に従うことは最も重要です。

マルチキャスト攻撃は必ずしも意図的なものではなく、多くの場合は偶発的なものであることは注目に値します。たとえば、2004年3月に初めて観察されたWittyワームは、IPアドレスへのランダムな攻撃によって広がったワームの一例です。アドレス空間の完全なランダム化の結果、マルチキャストIP宛先もこのワームの影響を受けました。多くの組織では、ワームが多数のマルチキャスト宛先アドレスにパケットを送信したため、多数のファーストホップルータがクラッシュしました。しかし、ルータは、関連するステートの作成によってこのようなマルチキャストトラフィックの負荷の範囲を特定できず、リソースの枯渇を効果的に経験しました。これは、企業でマルチキャストが使用されていない場合でも、マルチキャストトラフィックを保護する必要性を示しています。

ルータに対する一般的な脅威は次のとおりです。

- 低速（パント）パスなどのハードウェアパスや、セキュアシェル(SSH)、Telnet、ボーダーゲートウェイプロトコル(BGP)、OSPF、ネットワークタイムプロトコル(NTP)などを含む管理またはコントロールプレーンポートなどのソフトウェアパスに対する、あらゆるタイプのパケットフラッディング
- ルータへの侵入とその後のルータ機能の悪用。TelnetまたはSSHパスワードの脆弱性、およびSimple Network Management Protocol（SNMP；簡易ネットワーク管理プロトコル）コミュニティストリングの脆弱性は、現代のネットワークでは一般的な問題です。
- 設定ミスやインサイダー攻撃などの運用上の問題は、ネットワーク全体とそのトラフィックのセキュリティを脅かす可能性があります。

ルータでマルチキャストを有効にする場合は、ユニキャストに加えてマルチキャストを保護する必要があります。IPマルチキャストを使用しても、基本的な脅威モデルは変わりませんが、攻撃の対象となる可能性がある追加プロトコル(PIM、IGMP、MLD、MSDP)を有効にします。このプロトコルは特に保護する必要があります。これらのプロトコルでユニキャストトラフィックが使用されている場合、脅威モデルはルータによって実行される他のプロトコルと同じです。

マルチキャストトラフィックは基本的に「レシーバ駆動型」であり、リモート宛先を対象とできないため、マルチキャストトラフィックをユニキャストトラフィックと同様に使用してルータを攻撃することはできません。攻撃ターゲットは、マルチキャストストリームに明示的に「参加」する必要があります。ほとんどの場合（Auto-RPが主な例外）、ルータは「リンクローカル」マルチキャストトラフィックのみをリッスンして受信します。リンクローカルトラフィックは転送されません。したがって、マルチキャストパケットを含むルータへの攻撃は、直接接続された攻

撃者からのみ発生します。

発信元側からの脅威

マルチキャストソース (PCまたはビデオサーバのいずれも、ネットワークと同じ管理制御下にない場合があります) したがって、送信側は、ネットワークオペレータの観点からは、ほとんどの場合、信頼できないものとして扱われます。PCとサーバの強力な機能と、それらが持つ複雑なセキュリティ設定は不完全であることが多いため、送信側はマルチキャストを含むすべてのネットワークに対して重大な脅威を与えます。これらの脅威には次のものがあります。

- レイヤ2攻撃：レイヤ2にはさまざまな種類の攻撃を実行するための多様な攻撃形式があります。これらはマルチキャストだけでなくユニキャストにも適用されます。これらの攻撃形式はマルチキャストに固有のものではないため、このドキュメントでは詳細に説明しません。詳細については、Cisco Press発行の書籍『LAN Switch Security』(ISBN-10:1-58705-467-1)を参照してください。
- マルチキャストトラフィックによる攻撃：前述のように、ファーストホップルータはグループのリスナーが存在しない限りマルチキャストトラフィックを転送しないため、マルチキャストトラフィックによる攻撃は困難です。ただし、マルチキャストパケットを使用すると、ファーストホップをさまざまな方法で攻撃できます。
  - ネットワーク飽和攻撃：攻撃者は、利用可能な帯域幅を使用してマルチキャストパケットでセグメントをフラッディングし、DoS状態につながる可能性があります。
  - マルチキャスト状態攻撃：ファーストホップルータはマルチキャストパケットでフラッディングされるため、状態が過剰になり、結果としてDoS攻撃状態が発生する可能性があります。
  - 送信側は、送信されたPIM helloを通じてPIM DRになろうとします。このような場合、LANとの間でトラフィックが転送されることはありません。
  - BiDir-PIM DFのPIM DF選択パケットはスプーフィングされる可能性があります。このような場合、LANとの間でトラフィックが転送されることはありません。
  - 送信者は、AutoRP RPディスカバリまたはBSRブートストラップメッセージをスプーフィングする可能性があります。これは実際には偽のRPをアナウンスし、PIM-SM/BiDirサービスをダウンまたは中断させます。
  - 送信者は、PIMソースレジスタ/レジスタ停止メッセージなどのユニキャスト攻撃を送信したり、BSRアナウンスパケットを送信して偽のBSRをアナウンスしたりできます。
  - 送信者は、フィルタリングされていない限り、任意の有効なマルチキャストグループに送信できます。送信元アドレスがスプーフィングされてもエッジで阻止されない場合、送信者は正当な送信者の送信元IPアドレスを使用し、ネットワークの一部のコンテンツを上書きできます。
  - コントロールプレーンプロトコルに対するマルチキャスト攻撃：OSPFやDynamic Host Configuration Protocol(DHCP)など、マルチキャストに関連付けられていない多数のプロトコルは、マルチキャストパケットを使用して、これらのプロトコルを攻撃するために使用できます
- マスカレード：送信者が別の送信者のふりをできる攻撃形式は数多くあります。スプーフィングされた送信元IPアドレスは、このような攻撃形式の1つです。

- サービスの盗難：送信者が制御されない限り、送信側からマルチキャストサービスを不正に使用する可能性があります。

注：通常、ホストはPIMパケットを送受信しません。これを行うホストは、攻撃を試みる可能性があります。

受信側からの脅威

また、レシーバは通常、CPUパワーと帯域幅が大きいプラットフォームであり、さまざまな攻撃形態に対応できます。これらは送信側の脅威とほとんど同じです。レイヤ2攻撃は、依然として重要な攻撃ベクトルです。偽のレシーバやサービスの盗用もレシーバ側で発生する可能性がありますが、攻撃ベクトルは通常IGMP（または前述のようにレイヤ2攻撃）です。

ランデブーポイントとBSRに対する脅威

PIM-SM RPおよびPIM-BSRはマルチキャストネットワークの重要なポイントであるため、攻撃者にとって重要なターゲットです。どちらのルータもファーストホップルータではない場合は、PIMユニキャストを含むユニキャスト攻撃形式のみをこれらの要素に対して直接標的にすることができます。RPとBSRに対する脅威には次のものがあります。

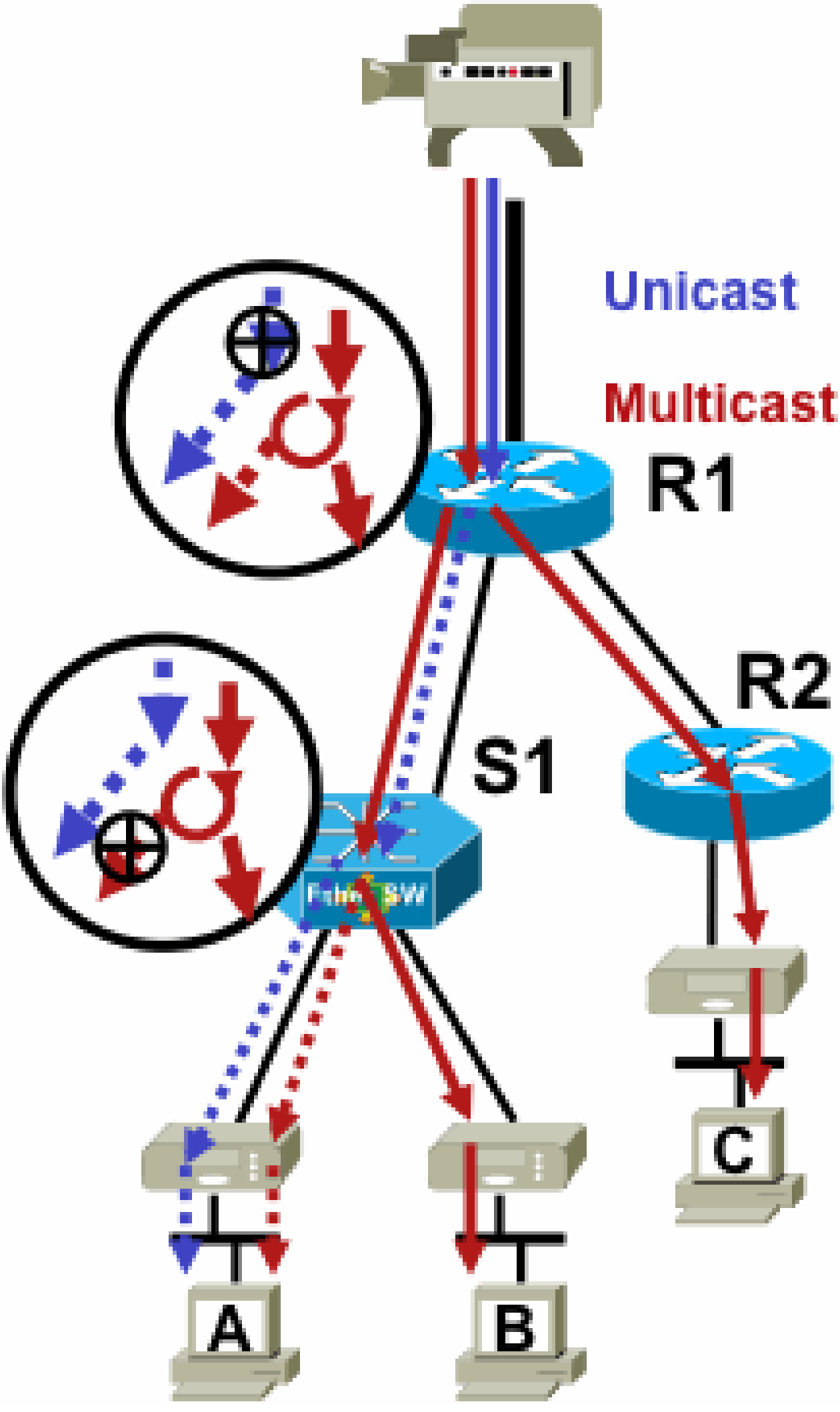
- 「ルータに対する基本的な脅威」の項で説明されている、すべての一般的な攻撃形式。
- スプーフィングされた送信元IPアドレスを使用する可能性のあるPIMユニキャスト攻撃では、悪意のあるデバイスから送信されるPIM登録メッセージまたは登録停止メッセージを介してDoS攻撃が可能になります。

マルチキャストおよびユニキャストセキュリティ（比較）

状態に関する考慮事項/フィルタ

図3のトポロジを考えてみます。このトポロジでは、1つの送信元(A、B、C)と3つの受信側(A、B、C)、1つのスイッチ(S1)、および2つのルータ（R1とR2）が示されています。青い線はユニキャストストリームを表し、赤い線はマルチキャストストリームを表します。3つのレシーバはすべてマルチキャストフローのメンバーです。

図3：ルータとスイッチでの複製


Unicast
Multicast
R1
R2
S1
A
B
C

1. マルチキャスト受信者は、許可されていないフローへの参加を試みたり、許可されていないコンテンツの受信を試みたりすることができます。
2. マルチキャスト受信側は、多くのグループやチャネルに関心を持つことで、使用可能なネットワーク帯域幅を過負荷にする可能性があります。この種の攻撃は、コンテンツの他の潜在的な受信者に対する共有帯域幅攻撃になります。
3. マルチキャスト受信側は、ルータまたはスイッチに対する攻撃を試みることができます。大量のIGMPレポートを生成できるため、大量のマルチキャストツリーステートが生成され、ルータのキャパシティが過負荷になる可能性があります。その結果、マルチキャストコンバージェンス時間が長くなったり、ルータでDoSが発生したりする可能性があります。

次のセクション「マルチキャストネットワーク内のセキュリティ」では、このような攻撃を軽減するさまざまな方法について説明します。

マルチキャストネットワーク内のセキュリティ

ネットワークエレメントセキュリティ

セキュリティは重要な機能ではなく、すべてのネットワーク設計に不可欠な要素です。そのため、ネットワーク内のすべてのポイントでセキュリティを考慮する必要があります。すべてのネットワーク要素を適切に保護することが最も重要です。あらゆるテクノロジーに適用できる攻撃シナリオの1つに、侵入者によって破壊されたルータがあります。侵入者がルータを制御すると、攻撃者はさまざまな攻撃シナリオを実行できます。したがって、各ネットワーク要素は、あらゆる形式の基本攻撃や特定のマルチキャスト攻撃に対して適切に保護する必要があります。

コントロール プレーン ポリシング（CoPP）

CoPPはルータACL(rACL)の進化であり、ほとんどのプラットフォームで使用できます。原則は同じです。ルータ宛てのトラフィックだけがCoPPによってポリシングされます。

サービスポリシーは、ポリシーマップとクラスマップを使用して、あらゆるQuality of Service(QoS)ポリシーと同じ構文を使用します。そのため、コントロールプレーンに向かう特定のトラフィックに対するレートリミッタを備えたrACL（許可/拒否）の機能を拡張します。

注:Catalyst 9000シリーズスイッチなどの特定のプラットフォームでは、CoPPがデフォルトで有効になっており、この保護は置き換えられません。 詳細については、『CoPPガイド』を参照してください。

稼働中のネットワークでrACLまたはCoPPを調整、変更、または作成する場合は、注意が必要です。どちらの機能もコントロールプレーンへのすべてのトラフィックをフィルタリングする機能を備えているため、必要なすべてのコントロールプレーンプロトコルと管理プレーンプロトコルを明示的に許可する必要があります。必要なプロトコルのリストは大きく、Terminal Access

Controller Access Control System(TACACS)など、あまり目立たないプロトコルは見逃しやすい場合があります。デフォルト以外のすべてのrACLおよびCoPPの設定は、実稼働ネットワークに導入する前に、必ずラボ環境でテストする必要があります。さらに、初期導入は「許可」ポリシーだけで開始する必要があります。これにより、ACLヒットカウンタを使用した予期しないヒットの検証が可能になります。

マルチキャスト環境では、マルチキャストが正常に機能するために、必要なマルチキャストプロトコル（PIM、MSDP、IGMPなど）がrACLまたはCoPPで許可されている必要があります。PIM-SMシナリオでは、送信元からマルチキャストストリームの最初のパケットがコントロールプレーンパケットとして使用され、デバイスのコントロールプレーンでマルチキャスト状態を作成するのに役立ちます。したがって、rACLまたはCoPPで関連するマルチキャストグループを許可することが重要です。プラットフォーム固有の例外が多数あるため、導入前に関連するドキュメントを参照し、計画されている設定をテストすることが重要です。

ローカルパケットトランスポートサービス(LPTS)

Cisco IOS XRでは、Local Packet Transport Service(LPTS)が、Cisco IOSのCoPPと同様に、ルータのコントロールプレーンへのトラフィックのポリサーとして機能します。さらに、ユニキャストおよびマルチキャストトラフィックを含む受信トラフィックをフィルタリングし、レートを制限できます。

マルチキャスト固有のセキュリティ

マルチキャスト対応ネットワークでは、各ネットワーク要素をマルチキャスト固有のセキュリティ機能で保護する必要があります。一般的なルータ保護については、このセクションで説明します。すべてのルータで必要とされていない機能ですが、ネットワーク内の特定の場所でのみ必要となる機能、およびルータ間の対話が必要な機能（PIM認証など）については、次の項で説明します。

Mrouteの制限

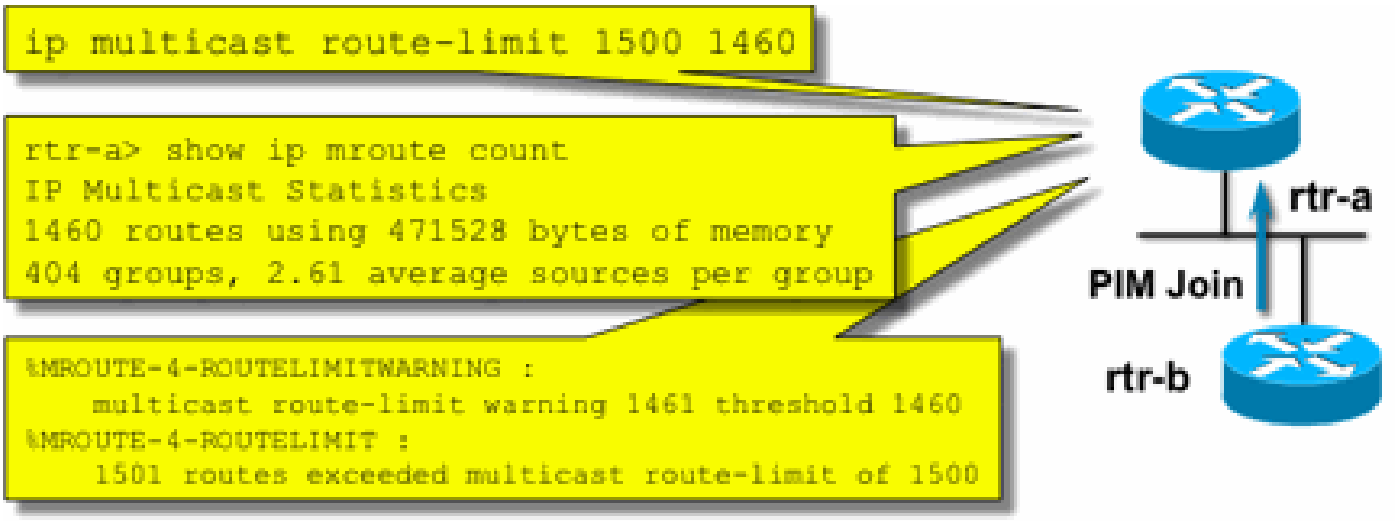
mroute limitコマンドは、ルータ上のマルチキャストルートの量をグローバルに制限し、DoS攻撃の防止に役立ちます。

<#root>

```
ip multicast route-limit
```

```
 <mroute-limit> <warning-threshold>
```

図6:Mrouteの制限



Mrouteの制限により、マルチキャストルーティングテーブルに入ることを許可されるmrouteの数にしきい値を設定できます。マルチキャストルートの制限が有効な場合、設定された制限を超えるマルチキャスト状態は作成されません。警告のしきい値もあります。mrouteの数が警告しきい値を超えると、syslog警告メッセージがトリガーされます。mrouteの制限では、状態を引き起こすそれ以降のパケットは廃棄されます。

MVRFごとにip multicast route-limitコマンドも使用できます。

SAPリッスンの無効化：no ip sap listen

sap listenコマンドにより、ルータはSession Announcement Protocol/Session Description Protocol(SAP/SDP)メッセージを受信します。SAP/SDPは、マルチキャストバックボーン(MBONE)の時代から存在するレガシープロトコルです。これらのメッセージは、将来または現在利用可能なマルチキャストコンテンツに関するディレクトリ情報を示します。これは、ルータのCPUおよびメモリリソースに対するDoSの原因となる可能性があるため、この機能を無効にする必要があります。

mrinfo情報へのアクセスの制御：「ip multicast mrinfo-filter」コマンド

mrinfoコマンド（Cisco IOSおよび一部のバージョンのMicrosoft WindowsとLinuxでも使用可能）は、さまざまなメッセージを使用してマルチキャストルータに情報を照会します。ip multicast mrinfo-filterグローバル設定コマンドを使用すると、この情報へのアクセスを送信元のサブセットに制限したり、情報を完全に無効にすることができます。

次の例では、192.168.1.1から送信されたクエリーを拒否し、その他のソースからのクエリーを許可しています。

```
ip multicast mrinfo-filter 51

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

この例では、 mrinfo 任意のソースからの要求：

```
ip multicast mrinfo-filter 52

access-list 52 deny any
```

注：予想されるとおり、どのACLでも、denyはパケットがフィルタリングされることを意味し、permitはパケットが許可されることを意味します。

mrinfoコマンドが診断目的で使用される場合、適切なACLを使用してip multicast mrinfo-filterコマンドを設定し、送信元アドレスのサブセットからのクエリーのみを許可することを強くお勧めします。mrinfoコマンドで提供される情報は、SNMPを介して取得することもできます。mrinfo要求の完全なブロック（デバイスのクエリからのすべてのソースをブロック）を強くお勧めします。

ネットワーク セキュリティ

このセクションでは、PIMマルチキャストおよびユニキャスト制御パケットと、Auto-RPおよびBSRを保護するさまざまな方法について説明します。

マルチキャストグループの無効化

ip multicast group-range/ipv6 multicast group rangeコマンドを使用すると、ACLによって拒否されたグループに対するすべての操作を無効にできます。

```
<#root>

ip multicast group-range

 <std-acl>

ipv6 multicast group-range

 <std-acl>
```

ACLによって拒否されたグループのいずれかに対してパケットが現れると、PIM、IGMP、MLD、MSDPなどのすべての制御プロトコルで廃棄され、データプレーンでも廃棄されます。したがって、これらのグループ範囲に対してIGMP/MLDキャッシュエントリ、PIM、Multicast Routing Information Base(RIB)/Multicast Forwarding Information Base(MFIB)状態は作成されず、すべてのデータパケットは即座に廃棄されます。

これらのコマンドは、デバイスのグローバルコンフィギュレーションで入力します。

ネットワーク外から発信されるすべてのマルチキャストトラフィックが制御されるように、このコマンドをネットワーク内のすべてのルータに、利用可能な場合は利用可能な場所で展開することを推奨します。これらのコマンドは、データプレーンとコントロールプレーンに影響すること

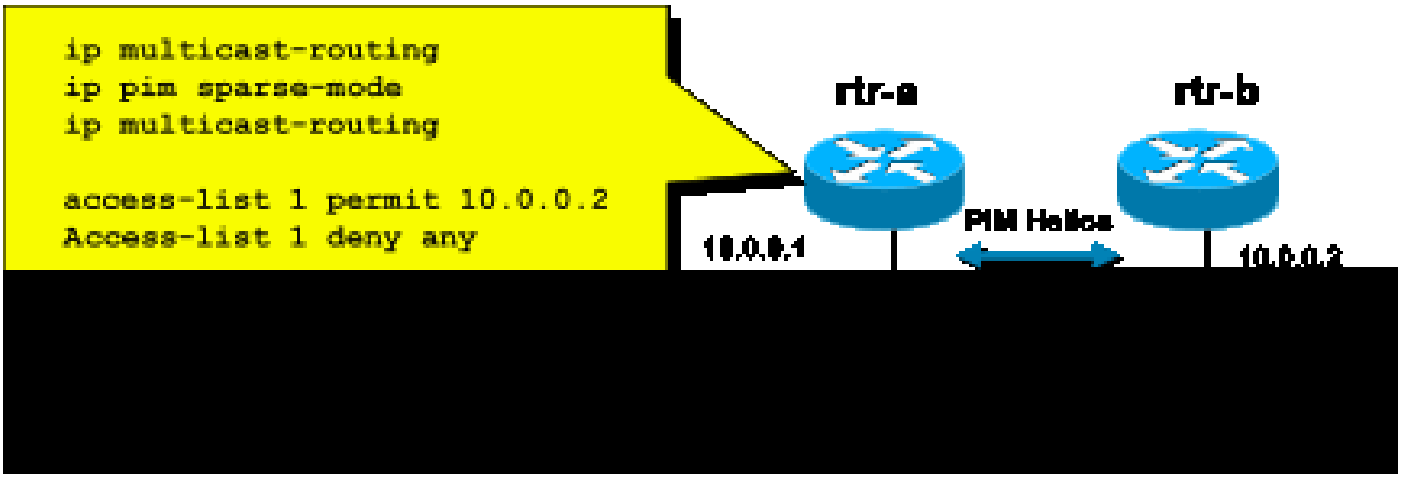
に注意してください。このコマンドを使用できる場合は、標準ACLよりもカバレッジが広いため、このコマンドを使用することを推奨します。

PIMセキュリティ

PIMネイバー制御

PIMネイバーシップを確立するには、PIMルータがPIM Helloを受信する必要があります。PIMネイバーシップは、代表ルータ(DR)選出、DRフェールオーバー、およびPIM Join/Prune/Assertメッセージの送受信の基盤でもあります。

図7:PIMネイバー制御



望ましくないネイバーを禁止するには、 IP PIMネイバーフィルタ コマンドを図7に示します。このコマンドは、Hello、Join/Pruneパケット、およびBSRパケットを含む、許可されていないすべてのネイバーPIMパケットをフィルタリングします。セグメント上のホストは、送信元IPアドレスをスプーフィングして、PIMネイバーを装う可能性があります。セグメントで送信元アドレスのスプーフィングを防ぐか、アクセススイッチでVLAN ACLを使用してホストからのPIMパケットを防ぐには、レイヤ2セキュリティメカニズム（IPソースガード）が必要です。ACLでキーワード「log-input」を使用すると、ACEに一致するパケットをログに記録できます。

PIM Join/PruneパケットはPIMネイバーに送信され、特定の(S,G)または(*,G)パスに対してそのネイバーを追加または削除します。PIMマルチキャストパケットは、存続可能時間(TTL)=1で送信されるリンクローカルマルチキャストパケットです。これらのパケットはすべて、既知のAll-PIM-Routersアドレス224.0.0.13に対するマルチキャストです。つまり、このような攻撃はすべて、攻撃を受けるルータと同じサブネット上で発生する必要があります。攻撃には、偽造されたHello、Join/Prune、およびAssertパケットが含まれます。

注:PIMマルチキャストパケットのTTL値を人為的に1より大きい値に増加または調整しても、問題は発生しません。All-PIM-Routersアドレスは常にルータでローカルに受信され、処理されます。通常のルータや正規のルータによって直接転送されることはありません。

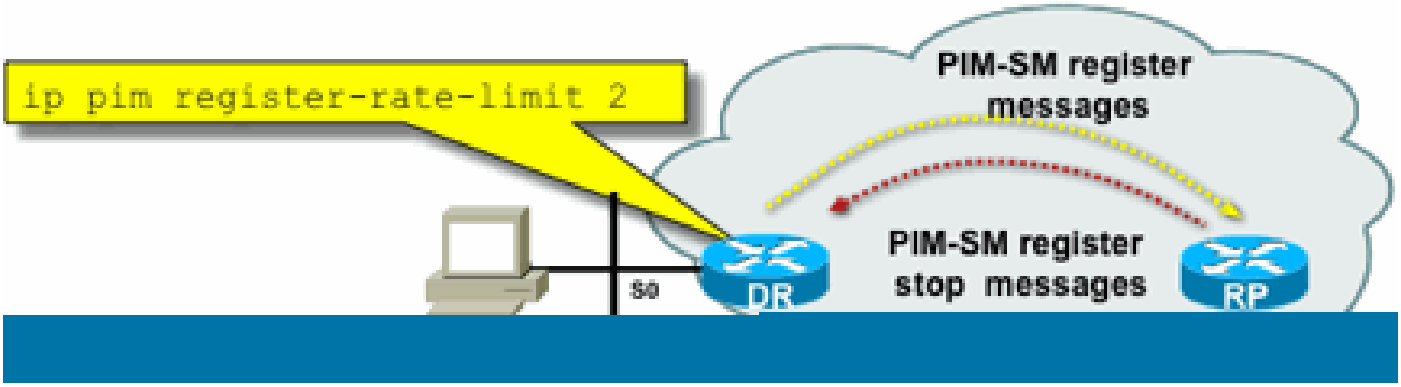
PIM-SM登録メッセージのフラッディングからRPを保護するために、DRはこれらのメッセージをレート制限する必要があります。ip pim register-rate-limitコマンドを使用します。

<#root>

ip pim register-rate-limit

 <count>

図8:PIM-SMレジスタトンネル制御



PIMユニキャストパケットを使用してRPを攻撃できます。したがって、RPは、インフラストラクチャACLによってこのような攻撃から保護できます。マルチキャストの送信側と受信側はPIMパケットを送信する必要がないため、PIMプロトコル（IPプロトコル103）は通常、サブスクライバエッジでフィルタリングできます。

自動RP制御 – RPアナウンスフィルタ

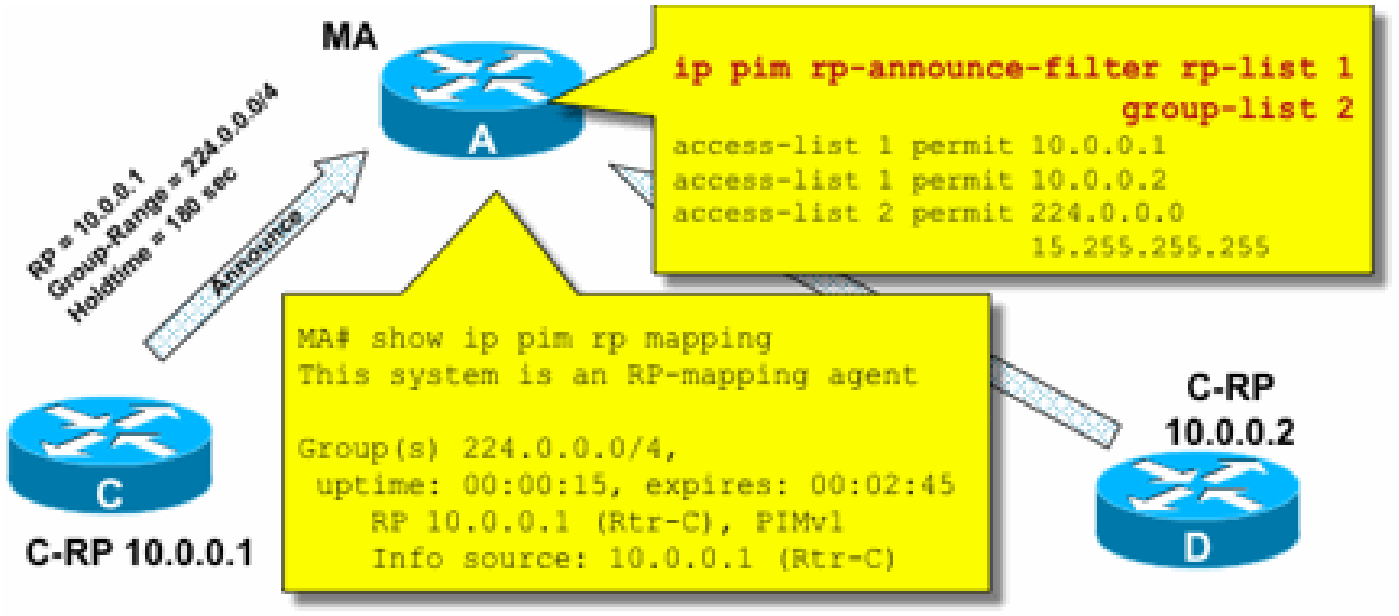
ip pim rp-announce filterコマンドは、可能な場合はAuto-RPで設定できる追加のセキュリティ対策です。

<#root>

ip pim rp-announce-filter

これは、どのルータがどのグループ範囲/グループモードの候補RPとして受け入れられるかを制御するためにMapping Agentで設定できます。

図9:Auto-RP - RPアナウンスフィルタ



Auto-RP制御 – Constrain Auto-RPメッセージ

AutoRPパケット、RP-announce(224.0.1.39)、またはRP-discover(224.0.1.40)を特定のPIMドメインに制限するには、multicast boundaryコマンドを使用します。

<#root>

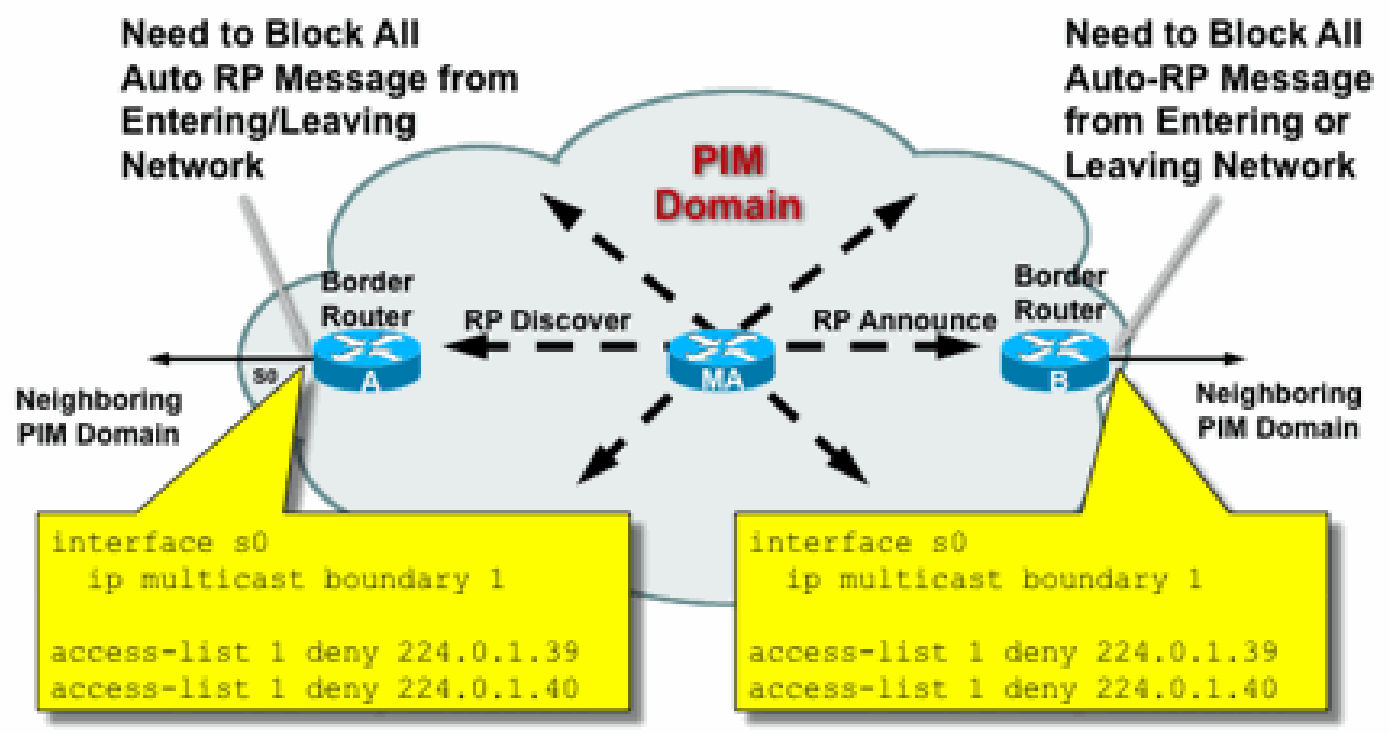
ip multicast boundary

access-list 1 deny 224.0.1.39

access-list 1 deny 224.0.1.40

224.0.1.39 (RP-announce) 224.0.1.40 (RP-discover)

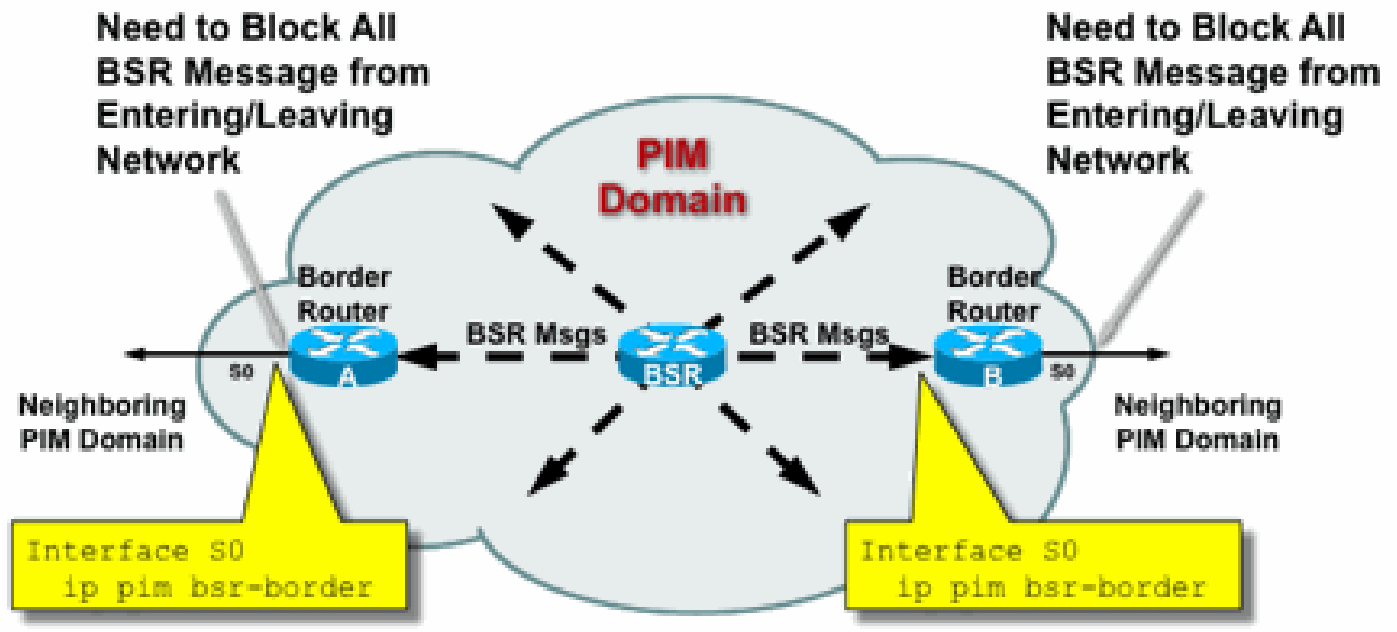
図10：マルチキャスト境界コマンド



BSR制御 – BSRメッセージの制約

ip pim bsr-border PIMドメインの境界でBSRメッセージをフィルタリングします。BSRメッセージはリンクローカルマルチキャストによってホップバイホップで転送されるため、ACLは必要ありません。

図11:BSRの境界



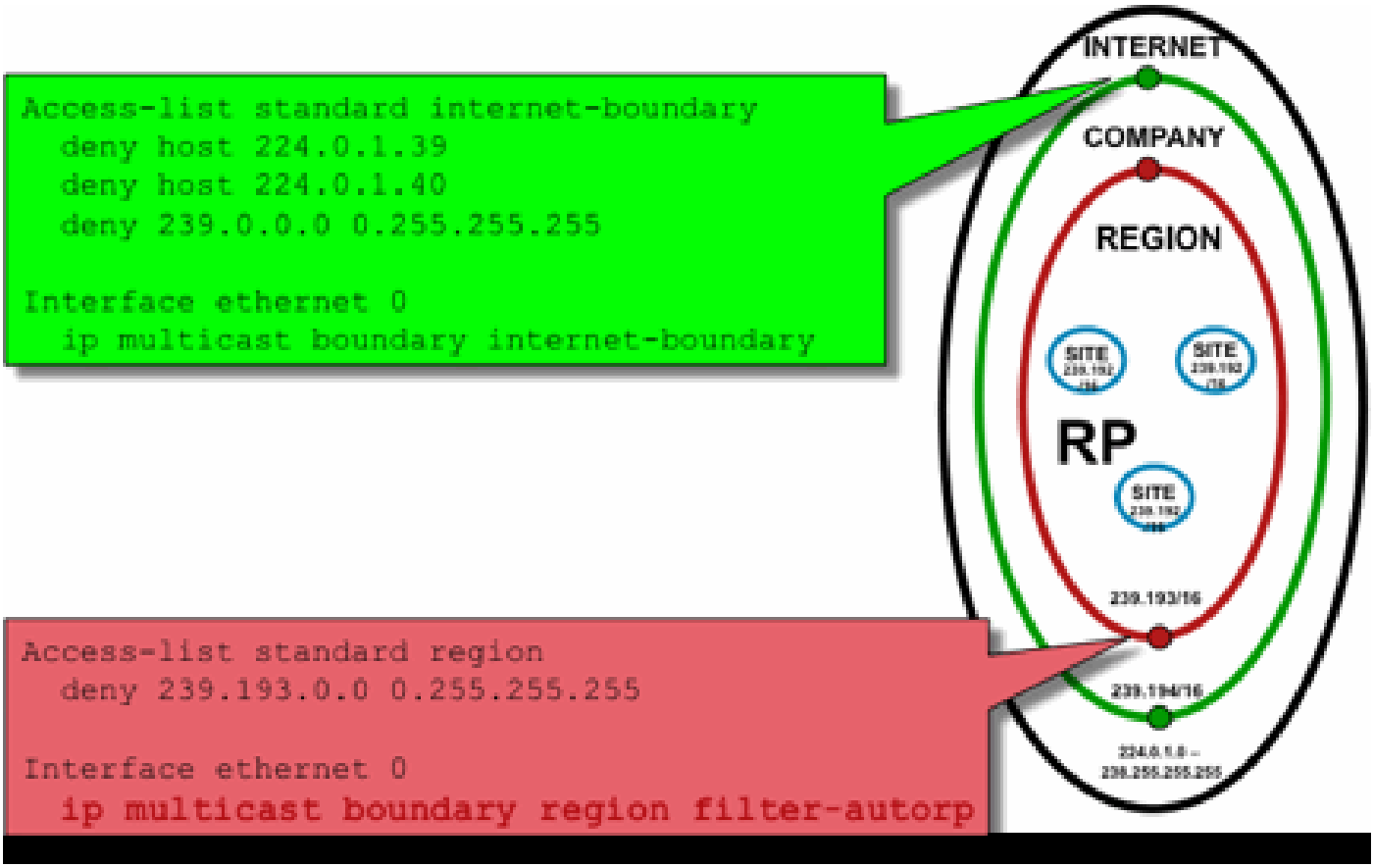
RP/PIM-SM関連のフィルタ

この最後のセクションでは、PIM-SPおよびRPコントロールプレーンパケットに対するフィルタと、Auto-RP、BSR、およびMSDPメッセージについて説明します。

Auto-RPフィルタ

図12に、アドレススコープと組み合わせたAuto-RPフィルタの例を示します。領域をバインドする2つの異なる方法が示されています。Auto-RPの観点からは、2つのACLは同等です。

図12:Auto-RPフィルタ/スコープ



Auto-RP用のインターフェイス境界フィルタの概念は、Auto-RPアナウンスがサポートするリージョンにのみ確実に到達するようにすることです。地域、会社、およびインターネット全体のスコープが定義され、それぞれのスコープにはRPとAuto-RPアドバタイズメントがあります。管理者は、リージョナルRPがリージョナルルータに認識され、Company RPがリージョナルルータとCompanyルータに認識され、インターネットRPがグローバルに使用可能であるようにすることだけを希望します。スコープのレベルを上げることができます。

図に示すように、Auto-RPパケットをフィルタリングするには、2つの根本的に異なる方法があります。インターネット境界によってAuto-RP制御グループ（224.0.1.39と224.0.1.40）が明示的に呼び出され、その結果、すべてのAuto-RPパケットがフィルタリングされます。この方式は、Auto-RPパケットがパススルーされない管理ドメインのエッジで使用できます。Region boundary(LBC)は、filter-auto-rpキーワードを使用して、Auto-RPパケット内のrpからグループ範囲へのアナウンスを調べます。アナウンスがACLによって明示的に拒否される場合、そのアナウンスはパケットが転送される前にAuto-RPパケットから削除されます。この例では、エンタープライズ全体のRPがリージョン内で認識されるのに対し、リージョン全体のRPは、リージョンからエンタープライズの他の部分までの境界でフィルタリングされます。

ドメイン間フィルタとMSDP

この例では、ISP1はPIM-SM中継プロバイダーとして機能します。ネイバーとのMSDPピアリングのみをサポートし、境界ルータでは(S,G)トラフィックのみを受け入れ、(*,G)トラフィックは受け入れません。

ドメイン間（通常は自律システム間）では、次の2つの基本的なセキュリティ対策を講じる必要があります。

1. multicast boundaryコマンドを使用して、データプレーンを保護します。これにより、マルチキャストトラフィックは定義されたグループ（および潜在的な送信元）に対してのみ受け入れられます。
2. ドメイン間コントロールプレーントラフィック(MSDP)を保護します。これは、MSDPコンテンツ制御、状態制限、およびネイバー認証など、いくつかの個別のセキュリティ対策で構成されます。

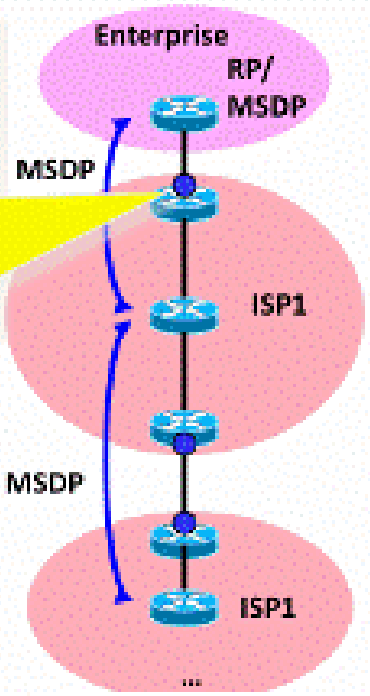
図13は、ISP1の境界ルータの1つでインターフェイスフィルタを設定する例を示しています。

multicast boundaryコマンドを使用して、「host 0.0.0.0」および管理スコープアドレスに対するフィルタによって、ドメイン境界のインヒビット(*,G)結合でデータプレーンを保護するには、次の手順を実行します。

図13：ドメイン間(*,G)フィルタ

```
ip access-list extended interdomain-am-edge
  deny   ip  host 0.0.0.0 any
  deny   ip  any          239.0.0.0 0.255.255.255
  permit ip  any          any

Interface ethernet 0
  ip multicast boundary interdomain-am-edge out
  ip multicast boundary interdomain-am-edge in
```



コントロールプレーンを保護するには、次の3つの基本的なセキュリティ対策によってMSDPを強化します。

1) MSDP SAフィルタ

MSDP SAフィルタを介してMSDPメッセージの内容をフィルタすることは「ベストプラクティス

」です。このフィルタの主な目的は、インターネット全体のアプリケーションではなく、送信元ドメインを越えて転送する必要のないアプリケーションやグループに対して、マルチキャスト状態が伝搬されないようにすることです。理想的には、セキュリティの観点から、フィルタは既知のグループ（および潜在的な送信者）のみを許可し、未知の送信者やグループをすべて拒否します。

通常、許可されたすべての送信者またはグループ（あるいはその両方）を明示的にリストすることはできません。グループごとに1つのRPを持つPIM-SMドメインに対しては、デフォルトの設定フィルタを使用することをお勧めします（MSDPメッシュグループはありません）。

```
!--- 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
         !
```

できるだけ厳密に、インバウンドとアウトバウンドの両方向でフィルタリングすることを推奨します。

MSDP SAフィルタの推奨事項の詳細については、
https://www.cisco.com/c/en/us/support/docs/ip/ip-multicast/13717-49.htmlを参照してください。

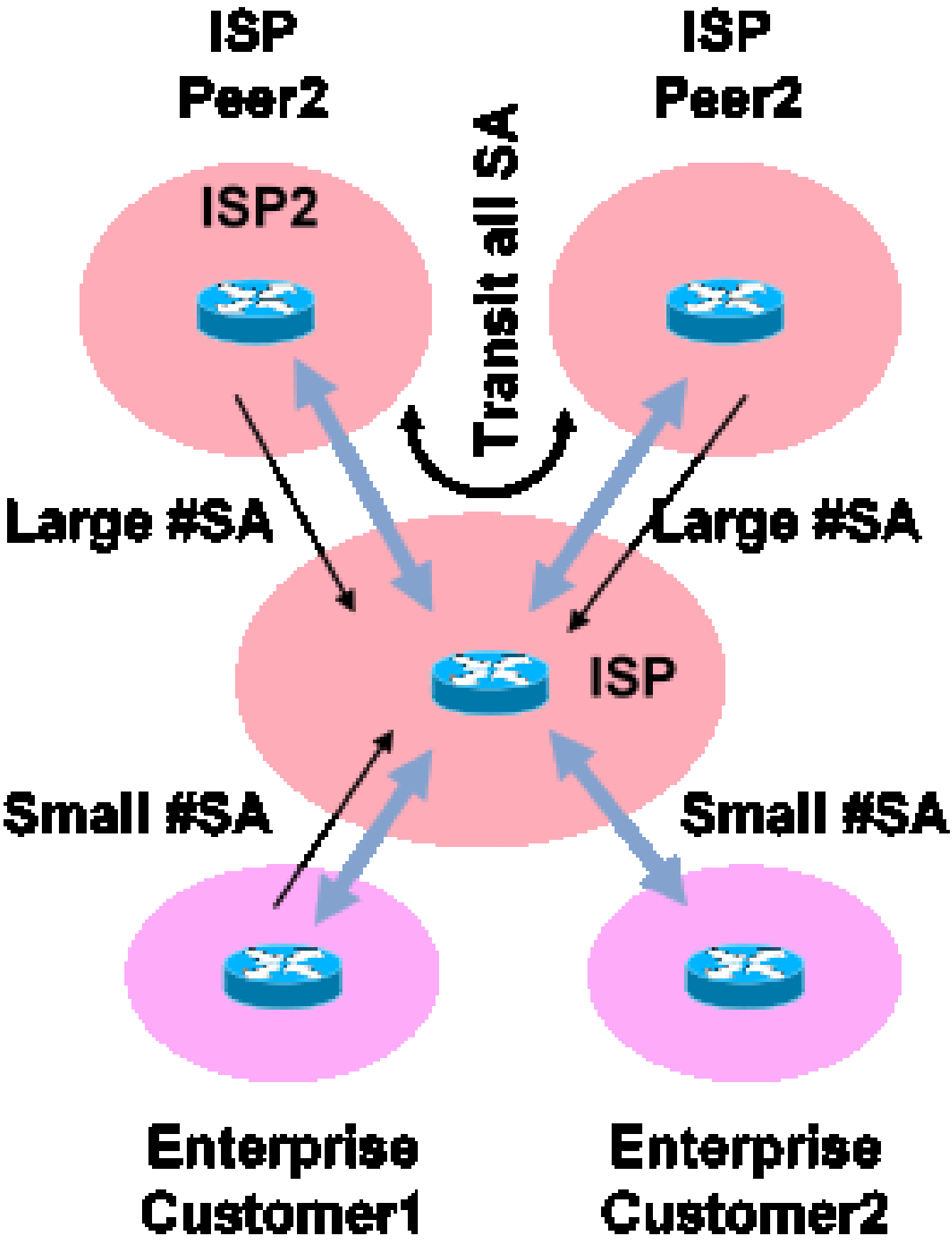
2) MSDP状態の制限

複数の自律システム(AS)間でMSDPが有効な場合は、ネイバーから「Source-Active」(SA)メッセージを受信するため、ルータに組み込まれる状態の量を制限することをお勧めします。ip msdp sa-limitコマンドを使用できます。

<#root>

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

図14:MSDPコントロールプレーン



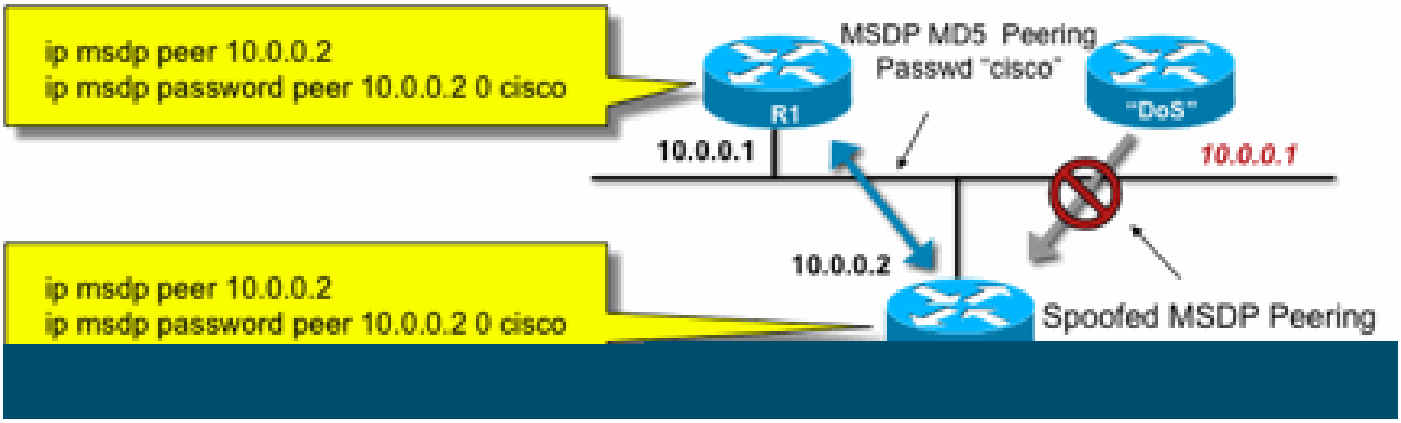
ip msdp sa-limitコマンドを使用すると、MSDPピアから受け入れられたSAメッセージが原因で発生するSA状態の数を制限できます。簡単な経験則に基づく推奨事項には、次のようなものがあります。

- stub-neighborからの小さな制限
- 中継ネイバーからの大きな制限(インターネットでの最大#SAsなど)
- トランジットISP：プラットフォームがサポートできる最大#SAsを設定します。

3) MSDP MD5ネイバー認証

MSDPピアでMessage-Digest Algorithm(MD5)パスワード認証を使用することを推奨します。これは、RFC 6691で説明されているBGPの保護に相当するTCP MD5シグニチャオプションを使用します。

図15:MSDP MD5ネイバー認証



次の3つのMSDPセキュリティの推奨事項では、異なる目標を追求しています。

- ネイバー認証（MD5を使用）により、信頼できるMSDPピアだけがメッセージを送信できます。
- SAフィルタにより、信頼できるMSDPピアでも、事前に合意された送信元/グループポリシーに従ったSAアナウンスしか送信できないことが保証されます。
- さらに、SA制限により、正規のピアからの正規の(S,G)アナウンスがあっても、使用可能なメモリを使い果たすことができなくなります。

送信者/送信元の問題

送信側で発生するマルチキャストセキュリティの問題の多くは、適切なユニキャストセキュリティメカニズムを使用して軽減できます。推奨されるベストプラクティスは、次のユニキャストセキュリティメカニズムの数です。

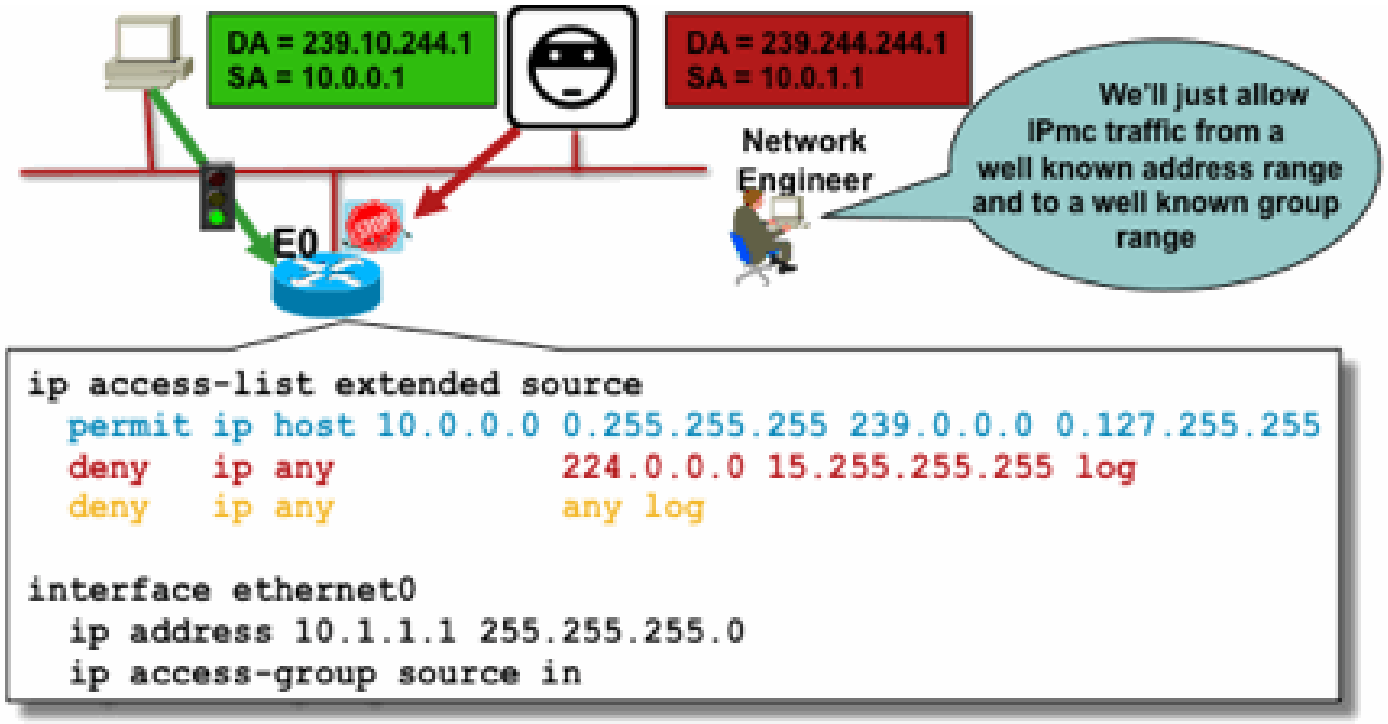
- 送信元アドレスのスプーフィング保護（アクセスレイヤ用のユニキャストリバースパス転送、uRPFまたはACL、およびIPソースガード）
- インフラストラクチャACL(deny ip any (to) <core address space>)

このような対策は、コアへの標的型攻撃をブロックするために使用できます。これにより、たとえば、RPへのPIMユニキャストパケットを使用した攻撃などの問題も解決されます。RPはネットワークの「内部」であるため、インフラストラクチャACLによって保護されます。

パケットフィルタベースのアクセス制御：送信元の制御

図16に示す例では、フィルタはファーストホップマルチキャストルータ（代表ルータ）のLANインターフェイス(E0)に設定されています。フィルタは、「source」と呼ばれる拡張アクセスコントロールリスト(ACL)によって定義されます。このACLは、送信元LANに接続されている代表ルータ(DR)の送信元インターフェイスに適用されます。実際には、マルチキャストトラフィックの性質により、送信元がアクティブになるすべてのLAN側インターフェイスで同様のフィルタを設定する必要があります。ソースアクティビティが発生する場所を正確に知ることはできないため、このようなフィルタをネットワーク内のすべての入力ポイントに適用することをお勧めします。

図16：制御ソース



このフィルタの目的は、特定の送信元アドレスまたは送信元アドレスの範囲から特定のグループまたはグループアドレスの範囲へのトラフィックを防止することです。このフィルタは、PIMがmrouteを作成する前に機能し、ステートの制限に役立ちます。

これは標準データプレーンACLです。これはハイエンドプラットフォームのASICに実装され、パフォーマンスの低下は発生しません。データプレーンACLは、不要なトラフィックによるコントロールプレーンへの影響を最小限に抑えるため、直接接続された送信元にはコントロールプレーンよりも推奨されます。また、パケットの送信先となる宛先（IPマルチキャストグループアドレス）を制限することも非常に効果的です。これはルータコマンドであるため、スプーフィングされた送信元IPアドレスを克服することはできません（このセクションの前半を参照）。したがって、追加のレイヤ2(L2)メカニズムを提供するか、特定のローカルエリアネットワーク/仮想ローカルエリアネットワーク(LAN/VLAN)に接続できるすべてのデバイスに対して一貫したポリシーを提供することを推奨します。

注:ACLの「log」キーワードは、特定のACLエントリに対するヒットを理解するのに非常に便利です。ただし、これはCPUリソースを消費するため、注意して処理する必要があります。また、ハードウェアベースのプラットフォームでは、ACLログメッセージはCPUによって生成されるため、CPUへの影響を考慮する必要があります。

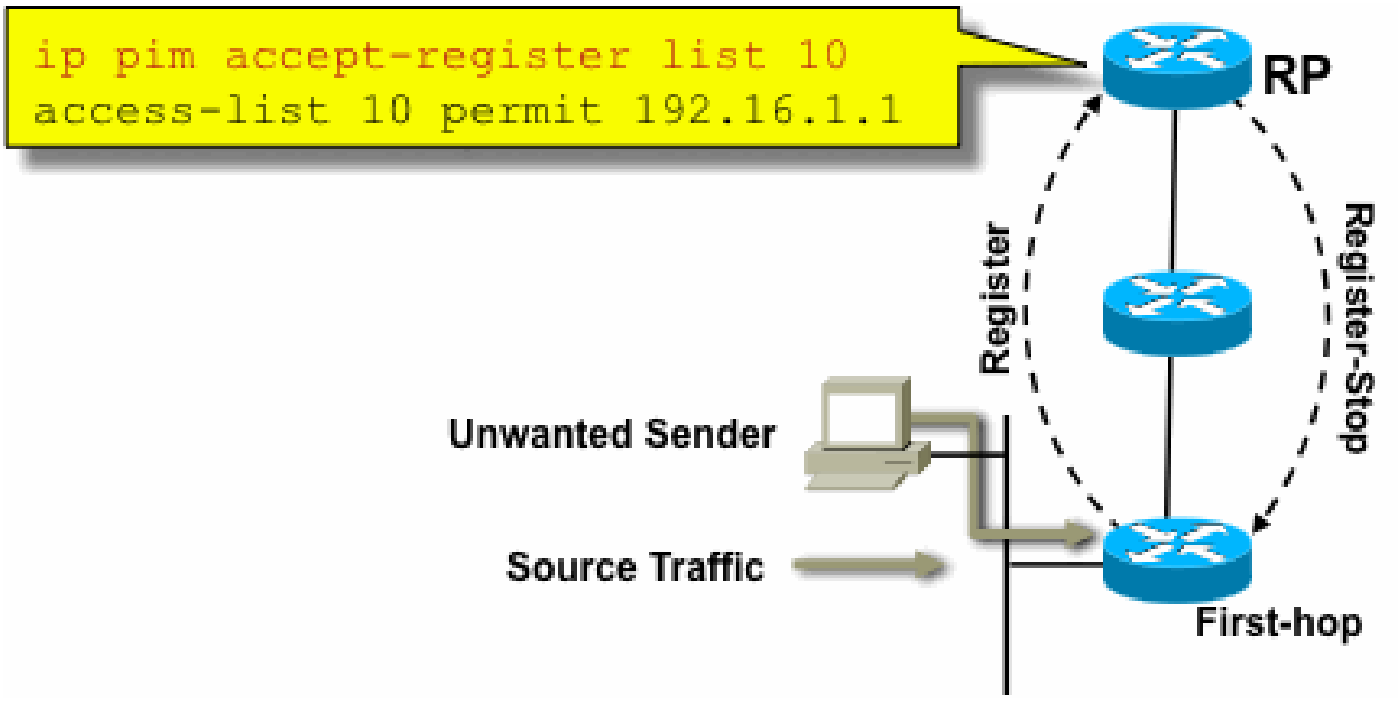
PIM-SMソース制御

セキュリティの観点から見たASM/PIM-SMアーキテクチャの実際の利点の1つは、ランデブーポイント(RP)により、あらゆるグループ範囲のネットワーク内のすべての送信元に対して単一の制御ポイントが提供されることです。これは、accept-registerフィルタと呼ばれるデバイスで利用できます。このフィルタのコマンドは次のとおりです。

<#root>

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

図17:PIM-SMソース制御



PIM-SMネットワークでは、このコマンドで不要なトラフィックの送信元を制御できます。送信元トラフィックがファーストホップルータに到達すると、ファーストホップルータ(DR)は(S,G)状態を作成し、PIMソースレジスタメッセージをRPに送信します。送信元がaccept-registerフィルタリスト（RPで設定）にリストされていない場合、RPは登録を拒否し、即座にRegister-Stopメッセージをに返します。

この例では、送信元アドレスだけをフィルタリングする単純なACLがRPに適用されています。RPで拡張ACLを使用して、送信元とグループをフィルタリングすることもできます。

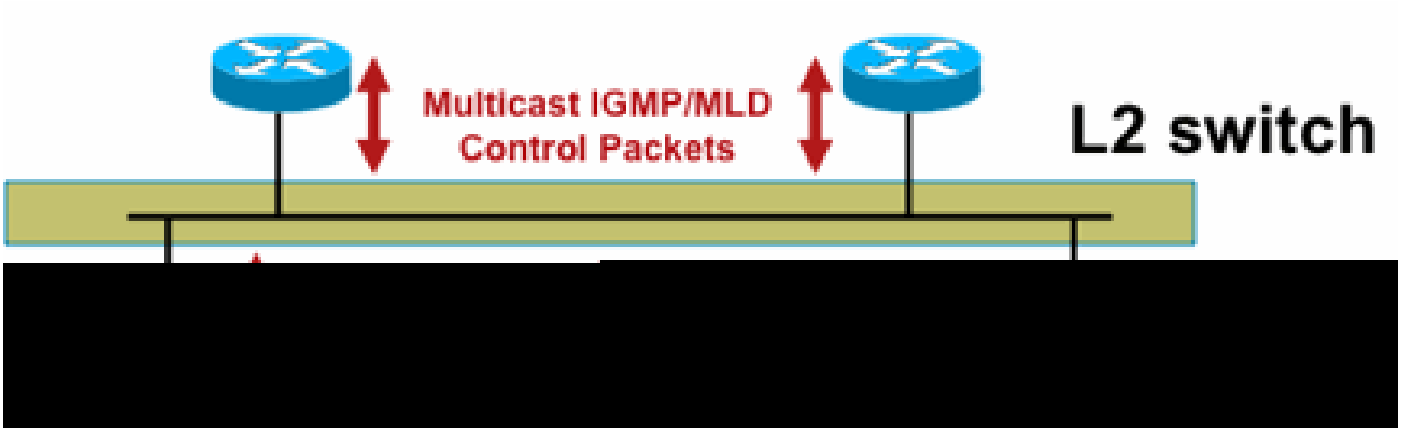
RPでpim accept-registerコマンドを使用すると、PIM-SM(S,G)状態が発信元のファーストホップルータで引き続き作成されるため、発信元フィルタには欠点があります。その結果、送信元に対してローカルで、送信元とRPの間に位置するレシーバでトラフィックが発生する可能性があります。さらに、pim accept-registerコマンドはRPのコントロールプレーンで動作します。これは、疑似の登録メッセージでRPを過負荷状態にし、DoS状態を引き起こすために使用される可能性があります。

pim accept-registerコマンドは、RPに対して、その他の方法（すべてのDR上での単純なデータプレーンACLの適用など）に加えて、ネットワークへのすべての入力点に対して適用することを推奨します。 DR上の入力ACLは完全に設定され運用されているネットワークでは十分ですが、エッジルータで設定ミスが発生した場合のセカンダリセキュリティメカニズムとしてRP上でpim accept-registerコマンドを設定することを推奨いたします。同じ目標を持つ階層化されたセキュリティメカニズムは「多層防御」と呼ばれ、セキュリティの一般的な設計原則です。

レシーバの問題 – コントロールIGMP/MLD

ほとんどのレシーバの問題は、IGMP/MLDレシーバプロトコルの相互作用の領域に分類されます。

図18：制御IGMP



IGMPまたはMLDパケットがフィルタリングされる場合は、次の点に注意してください。

- IPv4:IGMPはIPv4プロトコルタイプ（IPv4プロトコル2）です。
- IPv6:MLDはICMPv6プロトコルタイプのパケットで伝送される

IGMPプロセスは、IPマルチキャストが有効になると同時に、デフォルトで有効になります。IGMPパケットはこれらのプロトコルも伝送するため、マルチキャストが有効になるたびに次のプロトコルがすべて有効になります。

- PIMv1:PIMv1はPIMの最初のバージョンであり、移行のためにCisco IOSでは常に有効になっています。現在の導入ではすべてPIMv2を使用します。
- Mrinfo:Mrinfoは、マルチキャストネイバーを表示するためにCisco IOSが継承したUNIXコマンドです。Ciscoでは、mrinfoコマンドの代わりにSNMPを使用することを推奨しています。
- DVMRP:DVMRPは、スケーリング特性が非常に限られているレガシーの高密度モードディ

スタンスベクタープロトコルです。DVMRPに対するCisco IOSのサポートは廃止されたか、すでに廃止されています。
- Mtrace - Mtraceはユニキャストの「traceroute」に相当するマルチキャストで、便利なツールです

詳細については、「IANAのInternet Group Management Protocol(IGMP)タイプ番号」を参照してください。

```
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
```

ユニキャストIGMPパケット（IGMP/UDLR用）は、攻撃パケットである可能性が高く、有効なIGMPプロトコルパケットではないため、フィルタリングできます。ユニキャストIGMPパケットは、単方向リンクおよびその他の例外条件をサポートするCisco IOSでサポートされています。

偽造されたIGMP/MLDクエリーパケットは、予想よりも低いIGMPバージョンになる可能性があります。

特に、低いIGMPバージョンで送信されたクエリによって、このクエリを受信するすべてのホストが低いバージョンに戻される可能性があるため、ホストはIGMPクエリを送信しないことが理想的です。IGMPv3/SSMホストが存在する場合は、SSMストリームを「攻撃」できます。IGMPv2の場合、これは長いリーブ遅延を引き起こす可能性があります。

単一のIGMPクエリアを持つ非冗長LANが存在する場合、ルータは受信したIGMPクエリーをドロップする必要があります。

冗長または共通のパッシブLANが存在する場合は、IGMPスヌーピング対応のスイッチが必要です。この場合に役立つ特定の機能が2つあります。

- ルータガード
- IGMP Minimum Versionコマンド

ルータガード

スイッチがそのポートでマルチキャストルータ制御パケット（IGMP General Query、PIM Hello、またはCGMP Hello）を受信すると、すべてのスイッチポートがマルチキャストルータポートになる可能性があります。スイッチポートがマルチキャストルータポートになると、すべてのマルチキャストトラフィックがそのポートに送信されます。これは「ルータガード」で防ぐこ

とができます。ルータガード機能では、IGMPスヌーピングをイネーブルにする必要はありません。

ルータガード機能を使用すると、指定したポートをマルチキャストホストポートに指定できます。マルチキャストルータ制御パケットを受信しても、ポートはルータポートになることはできません。

これらのパケットタイプは、ルータガードが有効になっているポートで受信されると廃棄されます。

- IGMPクエリーメッセージ
- IPv4 PIMv2メッセージ
- IGMP PIMメッセージ(PIMv1)
- IGMP DVMRPメッセージ
- ルータポートグループ管理プロトコル(RGMP)メッセージ
- Cisco Group Management Protocol(CGMP)メッセージ

これらのパケットが廃棄されると、ルータガードによってパケットが廃棄されたことを示す統計情報が更新されます。

IGMPの最小バージョン

許可するIGMPホストの最小バージョンを設定できます。たとえば、すべてのIGMPv1ホスト、またはすべてのIGMPv1およびIGMPv2ホストを拒否できます。このフィルタは、メンバシップレポートにのみ適用されます。

ホストが一般的な「パッシブ」LAN（IGMPスヌーピングをサポートしていないスイッチや、そのスイッチ用に設定されていないスイッチなど）に接続されている場合、このような誤ったクエリに対してルータが実行できることは、その後トリガーされる「古いバージョン」のメンバシップレポートを無視すること以外に何もありません。自分自身をフォールバックさせません。

IGMPクエリはすべてのホストに対して可視である必要があるため、「有効なルータ」からのIGMPクエリを認証するために、静的キーIPSecなどの事前共有キーでハッシュベースのメッセージ認証(HMAC)メカニズムを使用することはできません。2つ以上のルータが共通のLANセグメントに接続されている場合は、IGMPクエリアを選択する必要があります。この場合、使用できる唯一のフィルタは、クエリーを送信する他のIGMPルータの送信元IPアドレスに基づくip access-groupフィルタです。

「通常の」マルチキャストIGMPパケットを許可する必要があります。

このフィルタをレシーバポートで使用すると、「正常な」IGMPパケットだけを許可し、既知の「不良」パケットをフィルタリングできます。

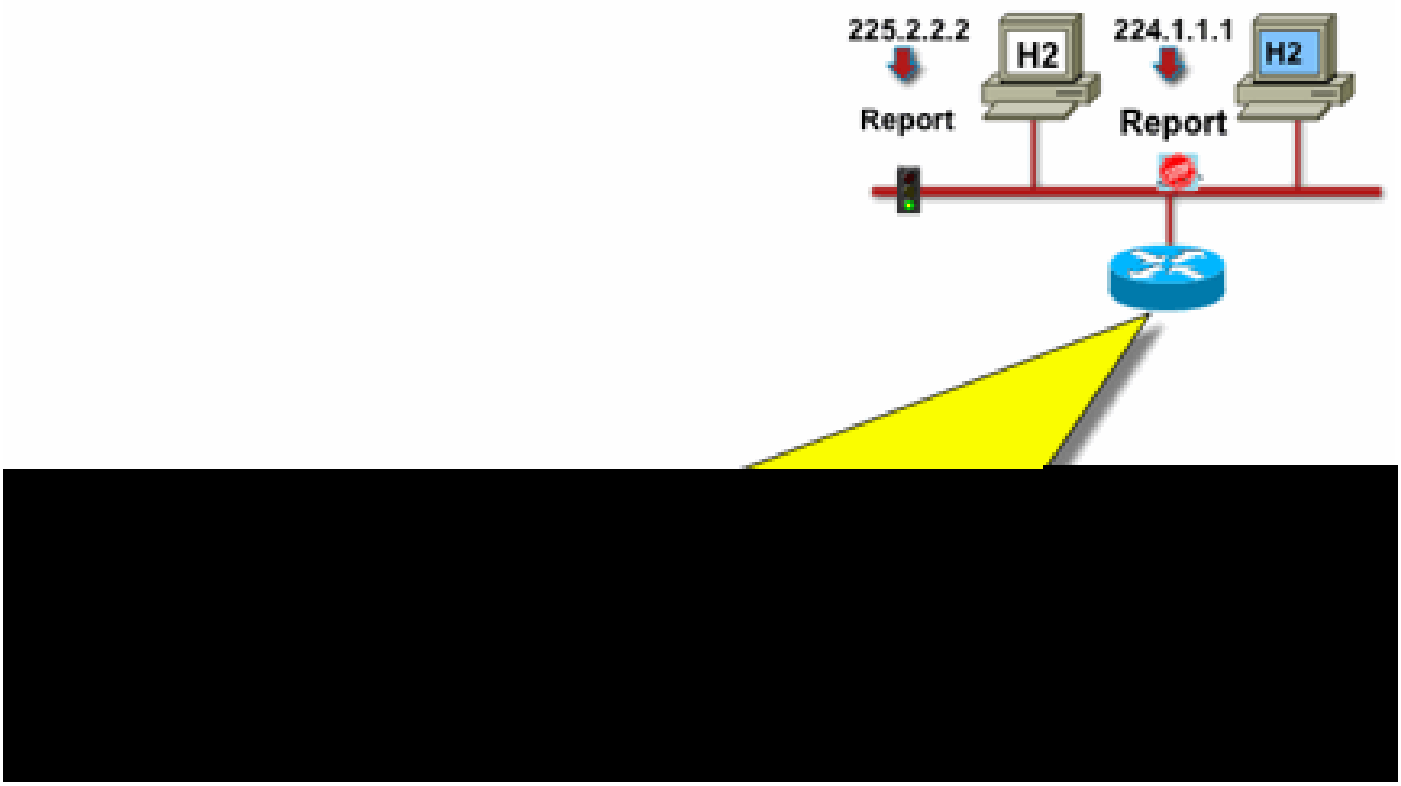
```
ip access-list extended igmp-control
   <snip>
   deny   igmp any any  pim        ! No PIMv1
   deny   igmp any any  dvmrp      ! No DVMRP packets
   deny   igmp any any  host-query ! Do not use this command with redundant routers.
                                   ! In that case this packet type 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：このタイプのIGMPフィルタは、受信ACLまたはCoPPで使用できます。どちらのアプリケーションでも、ルーティングや管理プレーンプロトコルなど、処理される他のトラフィックのフィルタと組み合わせる必要があります。

図19：ホスト受信側のアクセス制御



受信側へのトラフィックをフィルタリングするには、データプレーントラフィックではなく、コントロールプレーンプロトコルIGMPをフィルタリングします。IGMPはマルチキャストトラフィックを受信するために必要な前提条件であるため、データプレーンフィルタは必要ありません。

特に、レシーバが参加できる（コマンドが設定されているインターフェイスに接続される）マルチキャストフローを制限できます。この場合は、ip igmp access-group / ipv6 mld access-groupコマンドを使用します。

<#root>

ip igmp access-group / ipv6 mld access-group

ASMグループの場合、このコマンドは宛先アドレスに基づいてのみフィルタリングします。その後、ACLの送信元IPアドレスは無視されます。IGMPv3/MLDv2を使用するSSMグループでは、送信元と宛先のIPをフィルタリングします。

次の例では、すべてのIGMPスピーカに対して特定のグループをフィルタリングします。

```
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
```

次の例では、特定のグループの特定のIGMPスピーカ（したがって、特定のマルチキャスト受信側）をフィルタリングします。

```
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: ASMグループの場合、ソースは無視されます。

アドミッション制御

アクセスコントロールは、ネットワークの状態に関係なく、特定のフローに対してバイナリ、yes、またはnoのいずれかの応答を提供します。コントラストによるアドミッション制御は、送信者/受信者がアクセス制御メカニズムに合格した場合に使用できるリソースの数を制限します。マルチキャスト環境でのアドミッション制御に役立つさまざまなデバイスが用意されています。

グローバルおよびインターフェイスごとのIGMP制限

対象となるマルチキャスト受信側に最も近いルータでは、グローバルおよびインターフェイスごとの両方に参加するIGMPグループの数を制限できます。ip igmp limit/ipv6 mld limitコマンドを使用できます。

<#root>

ip igmp limit

```
 <n> [ except <ext-acl> ]

ipv6 mld limit

 <n> [ except <ext-acl> ]
```

この制限は、常にインターフェイスごとにグローバルに設定することを推奨します。いずれの場合も、この制限はIGMPキャッシュ内のエントリの数を指します。

次の2つの例は、このコマンドを使用して、家庭用ブロードバンドネットワークのエッジでグループ数を制限する方法を示しています。

例1：受信したグループをSDRアナウンスと1つの受信チャネルだけに制限する

セッションディレクトリ(SDR)は、一部のマルチキャスト受信者に対するチャネルガイドとして機能します。詳細については、RFC 2327を参照してください。

一般的な要件は、SDグループと1チャネルを受信するようにレシーバを制限することです。次の設定例を使用できます。

```
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
```

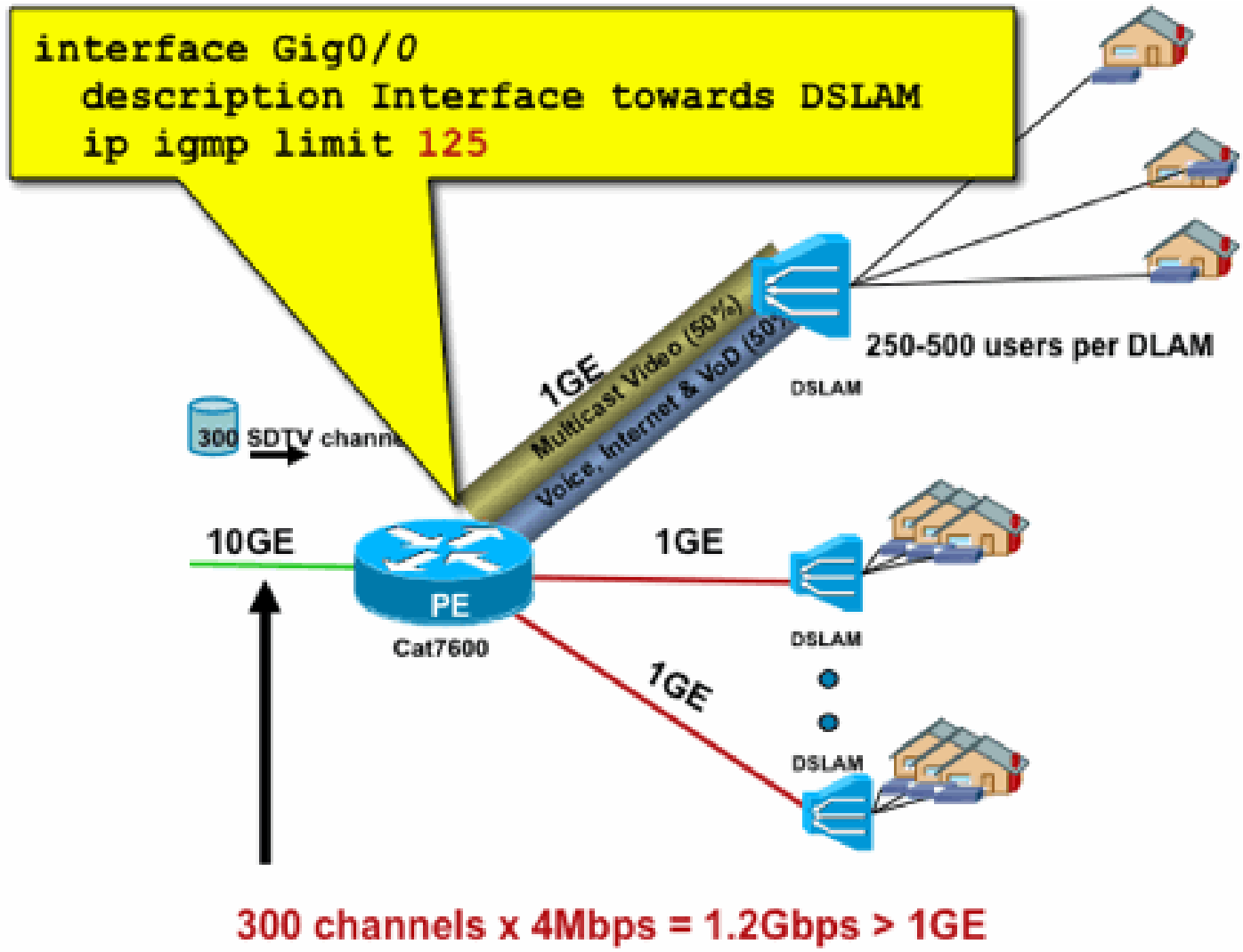
この例のアクセスリストでは、チャネルガイドのみが指定されています。グローバルip igmp limitコマンドでは、各IGMPソースが1つのチャネルに制限されていますが、常に受信可能なチャネルガイドは含まれていません。interfaceコマンドはグローバルコマンドを上書きし、このインターフェイスでチャネルガイドに加えて2つのチャネルを受信できるようにします。

例2：アグリゲーションDSLAMリンクのアドミッション制御

このコマンドは、帯域幅アドミッション制御の形式を提供するためにも使用できます。たとえば、それぞれ4 Mbpsの300のSDTVチャネルを配信する必要があり、Digital-Subscriber-Line-Access-Multiplexer(DSLAM)への1 Gbpsのリンクがある場合、TV帯域幅を500 Mbpsに制限し、残りはインターネットやその他の用途に使用するようにポリシーを決定できます。この場合、IGMPの状態を500 Mbps/4 Mbps = 125 IGMPの状態に制限できます。

この場合、次の設定を使用できます。

図20インターフェイスごとのIGMP制限の使用：Agg-DSLAMリンクでのアドミッション制御



インターフェイスごとのmroute制限

インターフェイスごとのmroute状態制限の有効化は、より一般的なアドミッション制御の形式です。発信インターフェイスのIGMPおよびPIM状態を制限するだけでなく、着信インターフェイスの状態制限の手段も提供します。

ip multicast limitコマンドを使用します。

<#root>

```
ip multicast limit [ rpf | out | connected ]
```

```
<ext-acl> <max>
```

状態は、入力インターフェイスと出力インターフェイスで個別に制限できます。直接接続された送信元の状態は、「connected」キーワードを使用して制限することもできます。次に、このコマンドの使用例を示します。

例1:Agg-DSLAMリンクの出力アドミッション制御

この例では、300のSD TVチャネルがあります。各SDチャネルが4 Mbpsを必要とし、合計が500 Mbps以下であると仮定します。最後に、Basic、Extended、Premiumの各バンドルをサポートする必要があることも想定します。帯域幅割り当ての例：

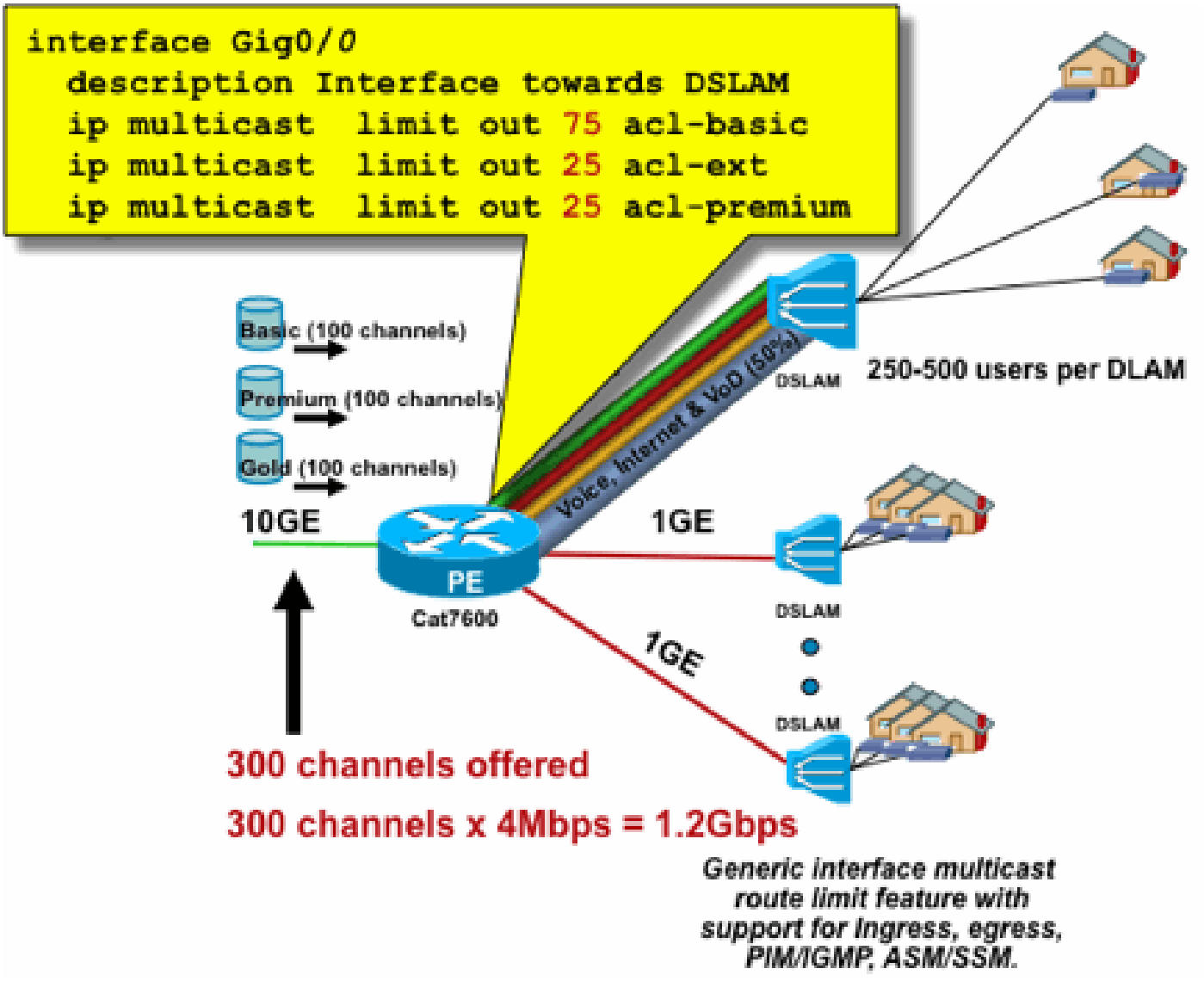
- 60 %/300 Mbpsベーシック
- 20 %/100 Mbps拡張
- 20 %/100 Mbps Premium

次に、チャネルごとに4 Mbpsを使用し、DSLAMアップリンクを次のように制限します。

- 基本的な75の状態
- 拡張25ステート
- プレミアム25州

PEAggからのDSLAMに面する発信インターフェイスの制限を設定します。

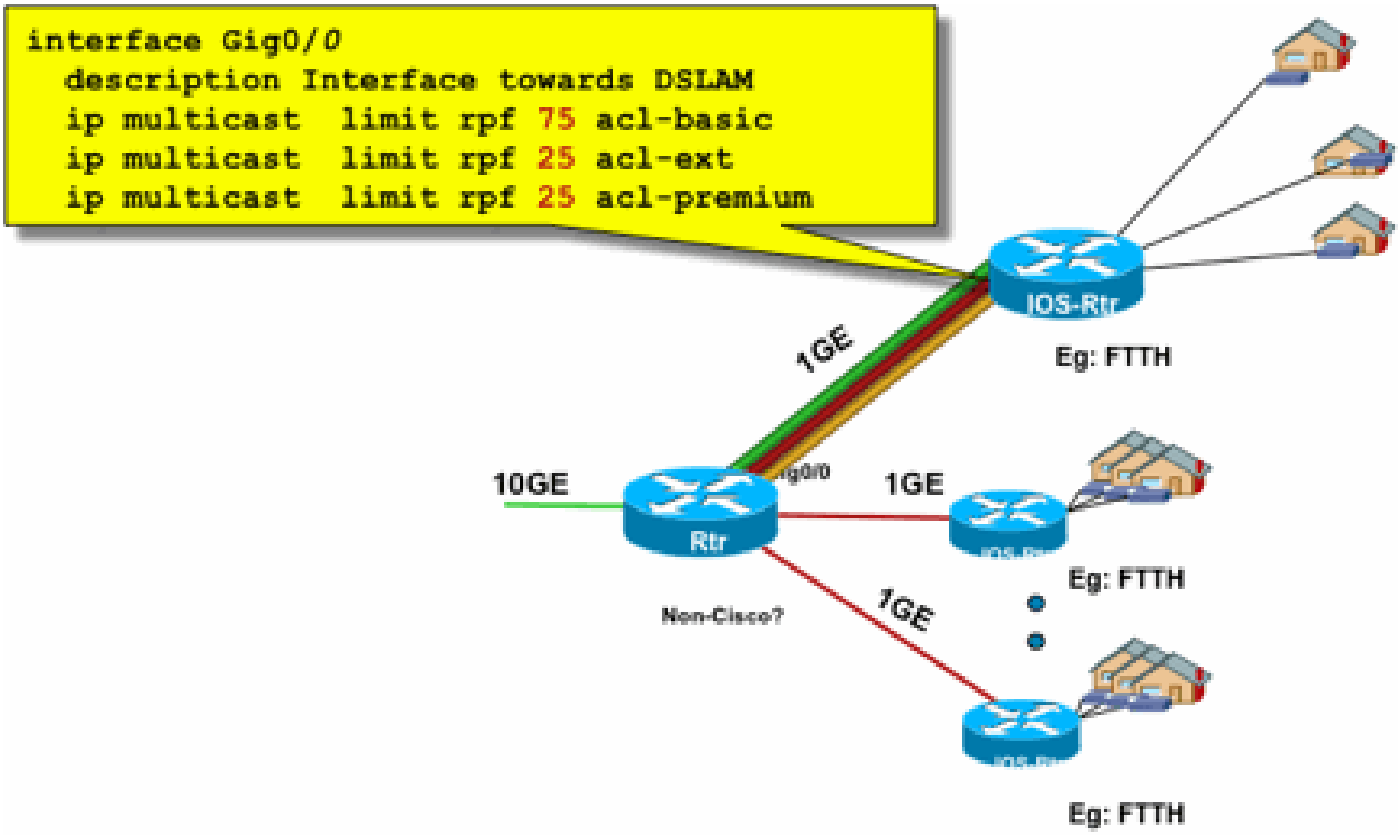
図21：インターフェイスごとのmroute制限の使用、Agg-DSLAMリンクでのアドミッション制御



例2:Agg-DSLAMリンクの入力アドミッション制御

アップストリームデバイスの発信インターフェイスの「out」制限の代わりに、ダウンストリームデバイスのRPFインターフェイスでRPF制限を使用できます。これは実質的に前の例と同じ結果になり、ダウンストリームデバイスがCisco IOSデバイスでない場合に役立つ可能性があります。

図22：インターフェイスごとのmroute制限の使用、入力アドミッション制御



例3 – 帯域幅ベースの制限

複数のコンテンツプロバイダー間のアクセス帯域幅をさらに分割し、各コンテンツプロバイダーにDSLAMへのアップリンクの帯域幅の公平な共有を提供できます。この場合は、ip multicast limit costコマンドを使用します。

<#root>

ip multicast limit cost

<ext-acl> <multiplier>

このコマンドを使用すると、ipマルチキャスト制限の拡張ACLに一致する任意の状態に「コスト」（「乗数」で指定した値を使用）を属性にすることができます。

このコマンドはグローバルコマンドであり、複数の同時コストを設定できます。

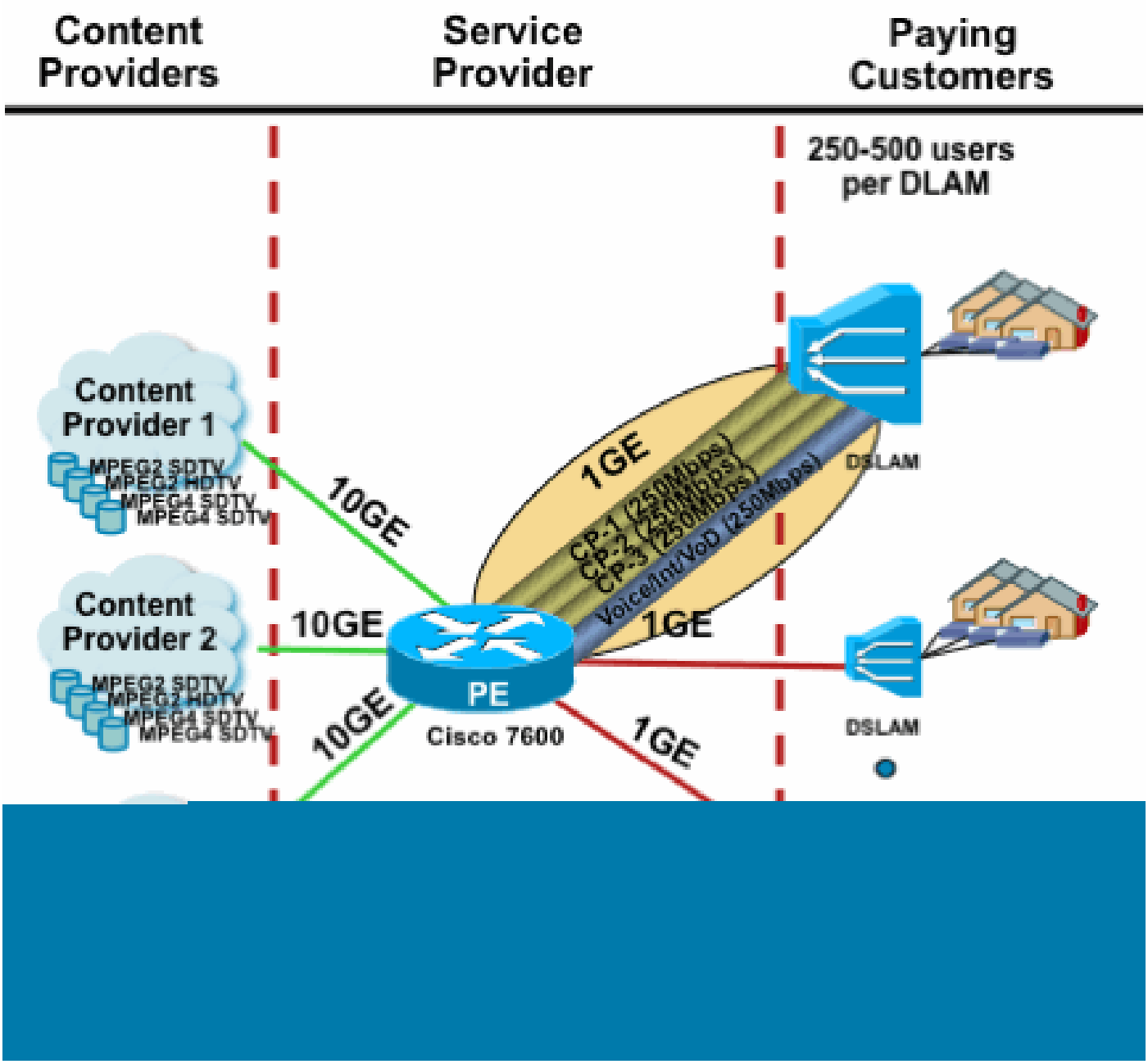
この例では、ネットワークへの各プロバイダーへの公平なアクセスを持つ3つの異なるコンテンツプロバイダーをサポートする必要があります。さらに、この例では、さまざまなタイプのMoving Picture Experts Group(MPEG)ストリームをサポートする必要があります。

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

この場合、次の設定を使用して、各ストリームタイプに帯域幅コストを割り当て、残りの750 Mbpsを3つのコンテンツプロバイダー間で共有できます。

```
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
```

図23：インターフェイスごとのMroute状態制限のコスト係数



マルチキャストおよびIPSec

GET VPNの概要

ユニキャストと同様に、マルチキャストトラフィックも、機密性や整合性を保護するために保護する必要がある場合があります。このようなサービスが必要になる可能性のある主な領域は、次の2つです。

- マルチキャストストリームの暗号化（たとえば、マルチキャストを使用する多数の受信者に機密データをストリーミングするバンキングアプリケーションなど）：これはデータプレーンのセキュリティです。
- マルチキャスト、OSPF、またはPIMを使用するコントロールプレーンプロトコルの暗号化

。これはコントロールプレーンセキュリティです。

プロトコルとしてのIPSec [RFC 6040、7619、4302、4303、5282]は、ユニキャストトラフィック（RFCによる）に限定されています。ここでは、2つのユニキャストピア間で「セキュリティアソシエーション」(SA)が確立されます。マルチキャストトラフィックにIPSecを適用する方法の1つは、GREトンネル内でマルチキャストトラフィックをカプセル化し、次にユニキャストであるGREトンネルにIPSecを適用することです。新しいアプローチでは、グループのすべてのメンバー間で確立された単一のセキュリティアソシエーションを使用します。これを実現する方法は、Group Domain of Interpretation(GDOI)[RFC 6407]で定義されています。

GDOIに基づいて、シスコはGroup Encryption Transport(GET)VPNと呼ばれるテクノロジーを開発しました。このテクノロジーは、「draft-ietf-msec-ipsec-extensions」のドキュメントで定義されている「アドレス保存を使用したトンネルモード」を使用します。GET VPNでは、まずグループのすべてのメンバー間でグループセキュリティアソシエーションが確立されます。その後、トラフィックはESP（カプセル化されたセキュリティペイロード）またはAH（認証ヘッダー）のいずれかで保護されます。AHでは、アドレスが保持されたトンネルモードが使用されます。

要約すると、GET VPNは、元のヘッダーのアドレス情報を使用するマルチキャストパケットをカプセル化し、グループポリシーに関連して内部パケットをESPなどで保護します。

GET VPNの利点は、マルチキャストトラフィックがセキュリティカプセル化メカニズムの影響を受けないことです。ルーテッドIPヘッダーアドレスは、元のIPヘッダーと同じままです。マルチキャストトラフィックは、GET VPNを使用する場合と使用しない場合で同じ方法で保護できます。

GET VPNノードに適用されるポリシーは、Group Key Serverで一元的に定義され、すべてのグループノードに配布されます。したがって、すべてのグループノードは同じポリシーを持ち、同じセキュリティ設定がグループトラフィックに適用されます。標準IPSecと同様に、暗号化ポリシーは、どのタイプのトラフィックをどの方法で保護する必要があるかを定義します。これにより、GET VPNをさまざまな目的で使用できます。

GET VPNを使用したマルチキャストデータプレーントラフィックの暗号化

ネットワーク全体の暗号化ポリシーがグループキーサーバに設定され、GET VPNエンドポイントに配布されます。このポリシーには、IPSecポリシー（IPSecモード – ここではトンネルモードとヘッダーの保持）、および使用するセキュリティアルゴリズム（AESなど）が含まれています。また、ACLの定義に従って、セキュリティで保護できるトラフィックを記述したポリシーも含まれています。

GET VPNは、マルチキャストおよびユニキャストトラフィックに使用できます。ユニキャストトラフィックを保護するポリシーは、次のようにACLで定義できます。

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

これにより、10/8からの送信元IPと10/8への宛先IPを持つすべてのトラフィックが暗号化されます。10/8から別のアドレスへのトラフィックなど、他のすべてのトラフィックはGET VPNによって無視されます。

マルチキャストトラフィックに対するGET VPNの適用は、技術的には同じです。たとえば、次のアクセスコントロールエントリ(ACE)を使用して、任意の送信元から各マルチキャストグループへのトラフィックを保護できます。

```
permit ip any 239.192.0.0 0.0.255.255
```

このポリシーは、すべての送信元(「any」)と、239.192で始まるすべてのマルチキャストグループに一致します。他のマルチキャストグループへのトラフィックは保護されません。

注：暗号ACLの構築には細心の注意を払う必要があります。管理トラフィック、またはGET VPNドメインの外部から発信され、内部で終端するトラフィック（つまり、1つの暗号化エンドポイントのみを通過するトラフィック）は、GDOIポリシーから除外する必要があります。

一般的な間違いは次のとおりです。

- permit ip any 224.0.0.0 0.255.255.255：これにより、OSPFトラフィックと、ピアルータを宛先とするその他のコントロールプレーントラフィックも暗号化されます（たとえば、 ）。
- 管理トラフィックは、ネットワーク内で終端する暗号化ポリシーから除外されません。これには、GDOIトラフィック自体も含まれます。

GET VPNを使用したコントロールプレーントラフィックの認証

一般に、メッセージが信頼できるピアから発信されるようにするために、ルーティングプロトコルなどのコントロールプレーントラフィックを認証することがベストプラクティスです。これは、BGPなどのユニキャストを使用するコントロールプレーンプロトコルでは比較的簡単です。ただし、多くのコントロールプレーンプロトコルはマルチキャストトラフィックを使用します。例としては、OSPF、RIP、PIMなどがあります。完全なリストについては、IANAのIPv4 Multicast Address Space Registryを参照してください。

これらのプロトコルの中には、Routing Information Protocol（RIP；ルーティング情報プロトコル）やEnhanced Interior Group Routing Protocol(EIGRP)などの認証機能が組み込まれているものもあれば、IPSecを使用してこの認証機能を提供しているものもあります（OSPFv3、PIMなど）。後者の場合、GET VPNはこれらのプロトコルを保護するためのスケーラブルな方法を提供します。ほとんどの場合、この要件はプロトコルメッセージ認証、つまり信頼できるピアからメッセージが送信されたことの確認です。ただし、GET VPNではこのようなメッセージの暗号化も可能です。

このようなコントロールプレーントラフィックを保護（通常は認証のみ）するには、トラフィックをACLで記述し、GET VPNポリシーに含める必要があります。詳細は保護するプロトコルによ

って異なります。ここでは、ACLに入力GET VPNノード（カプセル化されている）のみを通過するトラフィックが含まれているか、または出力ノードも含まれているかに注意する必要があります。

PIMプロトコルを保護する基本的な方法は2つあります。

- permit ip any 224.0.0.13 0.0.0.0：これは「すべてのPIMルータ」マルチキャストグループです。ただし、ユニキャストPIMメッセージは保護されません
- permit pim any any：マルチキャストとユニキャストのどちらを使用するかにかかわらず、PIMプロトコルを保護します

注：コマンドは、概念の説明に役立つ例として提供されています。 たとえば、BSRやAuto-RPなど、PIMのブートストラップに使用される特定のPIMプロトコルを除外する必要があります。導入に依存する特定の利点や不便な点がある方法はありません。詳細については、GET VPNでPIMを保護する方法に関する特定の資料を参照してください。

まとめ

マルチキャストは、ネットワーク内でますます一般的なサービスになっています。家庭向け/家庭用ブロードバンドネットワークでのIPTVサービスの出現と、世界の金融市場の多くで電子取引アプリケーションに向かう動きは、マルチキャストを絶対的な要件にする要件のほんの2つの例です。マルチキャストには、設定、運用、および管理に関するさまざまな課題が伴います。重要な課題の1つはセキュリティです。

このドキュメントでは、マルチキャストを保護できるさまざまな方法について説明しました。

- まず、全体的なマルチキャストコントロールプレーンとデータプレーンについて説明し、ユニキャストとの違いによって新たなセキュリティ上の課題が生じる仕組みについて説明します。
- 次に、マルチキャストネットワークで発生する主要なプロトコル、特にIGMP、PIM、およびMSDPについて詳しく調べました。それぞれのケースで、セキュリティ上の脅威の説明と、これらの脅威に対する緩和策として推奨されるベストプラクティスが提供されています。
- また、特定のビデオフローに必要な帯域幅の量に比べて帯域幅が制限されるブロードバンドエッジネットワークなど、特定のアプリケーションでマルチキャストを保護する方法を示す特定の例もあります。
- 最後に、GET VPNアーキテクチャは、セキュアなVPNを配信するためのIPSecとマルチキャストを統合する方法として説明されました。

マルチキャストセキュリティを考慮して、ユニキャストとの違いを覚えておいてください。マルチキャスト送信はダイナミックステートの作成に基づき、マルチキャストではダイナミックパケットレプリケーションが行われ、マルチキャストではPIM JOIN/PRUNEメッセージに応答して単方向ツリーが構築されます。この環境全体のセキュリティには、Cisco IOSコマンドの豊富なフレームワークの理解と導入が含まれます。これらのコマンドの大部分は、CoPPなどのパケットに対して配置されるプロトコル動作、状態（マルチキャスト）、またはポリサーの保護に重点を置いています。 これらのコマンドを正しく使用すれば、IPマルチキャストに対して堅牢な保護サー

ビスを提供できます。

要約すると、このドキュメントでは次の複数のアプローチについて説明しています。

1. SSMの広範な使用：これは(S,G)フォワーディングの使用も可能にする最も単純なPIMモードです。
2. ASMサービスが必要な場合は、堅牢なサービスを提供できることを確認します。静的に定義されたRPを使用すると、動的なRPアナウンスよりも安全なコントロールプレーンが提供されます。Auto-RPとBSRの方がより柔軟です
3. PIM-SMが有効になっている場合は、RPへの登録トンネルなど、特定の脆弱性の領域を調べ、DRが常に適切に保護されていることを確認します。CoPPは、これらの分野で非常に役立ちます。
4. ドメイン間ASMサービスが必要な場合は、BiDir PIMを展開できるかどうかを検討します。
5. グローバルなmroute/igmpステート制限の使用 – プラットフォームの機能と、通常の状況および最悪のシナリオで必要となる予想される最大ステート量を理解します。プラットフォームの機能に制限を設けることで、ネットワークを最大限に動作させることができます。
6. 基本フィルタ：rACL/CoPPおよびインフラストラクチャACL。アクセスレイヤでPIMをブロックします。

IPマルチキャストは、さまざまなアプリケーションサービスを提供するためのエキサイティングでスケーラブルな手段です。ユニキャストと同様に、さまざまなエリアでセキュリティを確保する必要があります。このドキュメントでは、IPマルチキャストネットワークの保護に使用できる基本的な構成要素について説明します。

関連情報

- エンタープライズIPマルチキャストアドレス割り当てのガイドライン
- IPv4 IGMPフィルタの設定
- Group Encrypted Transport VPN

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。