

# 218004-Secure-IP-multicast implementaties

## Inhoud

---

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Terminologie](#)

[Any Source Multicast](#)

[Source-Specific Multicast](#)

[Relevante multicastprotocollen/pakkettypen](#)

[IGMP/MLD-pakketten](#)

[PIM-beheerpakketten](#)

[Multicast PIM-beheerpakketten](#)

[Unicast PIM-beheerpakketten](#)

[Auto-RP-pakketten](#)

[Multicast-servicedetectiepakketten voor Protocol \(MSDP\)](#)

[Bedreigingen in een multicasomgeving](#)

[Zones of Trust and Trust Boundaries](#)

[Threat - Overzicht](#)

[Basisbedreigingen tegen een router](#)

[Bedreigingen van de bronkant](#)

[Bedreigingen van de ontvangerzijde](#)

[Bedreigingen tegen een rendez-vous point en BSR](#)

[Multicast- en Unicast-beveiliging \(vergeleken\)](#)

[Overwegingen/filters voor status](#)

[Aanvallen vanuit multicastbronnen](#)

[Statusaanvallen](#)

[Door ontvanger geïnitieerde aanvallen](#)

[Beveiliging binnen een multicast-netwerk](#)

[Security voor netwerkelement](#)

[Toezicht op besturingsplane \(CoPP\)](#)

[Local Packet Transport Service \(LPTS\)](#)

[Multicastspecifieke beveiliging](#)

[Limieten route](#)

[Netwerk security](#)

[Multicastgroepen uitschakelen](#)

[PIM-beveiliging](#)

[PIM-buurcontrole](#)

[Filters die betrekking hebben op RP/PIM-SM](#)

[Auto-RP-filters](#)

[Inter-Domain Filters en MSDP](#)

---

## [Afzender/bron problemen](#)

[Op pakketfilter gebaseerde toegangscontrole - controlebronnen](#)

[PIM-SM-broncontrole](#)

## [Problemen met ontvangers - Control IGMP/MLD](#)

### [Toegangsbeheer](#)

[Globale en Per Interface IGMP-limieten](#)

[Routebeperkingen per interface](#)

### [Multicast en IPSec](#)

[Inleiding om VPN te kopen](#)

[Gebruik GET VPN om multicast dataplane verkeer te versleutelen](#)

[Gebruik GET VPN om verkeer van besturingsplane te verifiëren](#)

### [Conclusies](#)

### [Gerelateerde informatie](#)

---

# Inleiding

Dit document beschrijft algemene richtlijnen over best practices om een IP-multicast netwerkinfrastructuur te beveiligen.

## Voorwaarden

### Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- IP-multicast

### Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

## Achtergrondinformatie

Dit document behandelt enkele basisconcepten, terminologie en behandelt de vermelde onderwerpen:

- Mechanismen om een specifiek platform en het netwerk in het algemeen te beveiligen.
- Alle Source Multicast- (ASM) en Source Specific Multicast-modellen (SSM).
- Multicast Virtual Private Network (MVPN)-beveiliging.

- Architectuur voor Group Encrypted Transport (GET) Virtual Private Network (VPN) die vertrouwelijkheid en integriteit biedt voor multicast-gegevensvlak of besturingsplantverkeer.

## Terminologie

In IP multicast zijn er twee klassieke servicemodellen:

1. Elke bronmulticast (ASM)
2. Source Specific Multicast (SSM)

In ASM, sluit de ontvanger zich aan bij een groep G via een het lidmaatschapsrapport van de Groep van Internet van het Protocol (IGMP) of van de Multicast Luisterontdekking (MLD) om de groep aan te duiden. Dit rapport vraagt verkeer door om het even welke bron naar groep G wordt verzonden, en vandaar de naam "om het even welke bron die." In SSM daarentegen sluit de ontvanger zich aan bij een specifiek kanaal dat wordt gedefinieerd door een bron S, die naar een groep G stuurt. Elk van deze servicemodellen wordt hieronder in detail beschreven.

### Any Source Multicast

Het ASM-model wordt gekenmerkt door twee protocolklassen: "dense mode flood-and-prune" en "sparse mode expres":

#### i) Dense Mode Flood-and-Prune Protocols (DVMRP/MOSPF/PIM-DM)

In dense mode protocollen, alle routers in het netwerk zijn bewust van alle bomen, hun bronnen en ontvangers. Protocollen zoals het Vector Multicast Routing Protocol van de Afstand (DVMRP) en de Dichte van het Protocol Onafhankelijke Multicast (PIM) "actieve bron" informatie van de overstromingswijze over het gehele netwerk en bouwen bomen via de verwezenlijking van "Prune Staat" in delen van de topologie waar het verkeer voor een specifieke boom ongewenst is. Ze worden ook wel "flood-and-prune"-protocollen genoemd. In Multicast Open Shortest Path First (MOSPF) wordt informatie over ontvangers overstromd door het netwerk om de opbouw van bomen te ondersteunen.

De protocollen van de dichte wijze zijn ongewenst omdat elke boom die in één of ander deel van het netwerk wordt gebouwd middelgebruik (met convergentieeffect) op alle routers in het netwerk (of binnen het administratieve werkingsgebied, indien gevormd) altijd kan veroorzaken. Deze protocollen worden in de rest van dit artikel niet verder besproken.

#### ii) Expliciete join-protocollen (PIM-SM/PIM-biDir) in spaarstand

Met sparse mode-expliciete samenvoegingsprotocollen maken apparaten geen groepspecifieke status in het netwerk, tenzij een ontvanger een expliciet IGMP/MLD-lidmaatschapsrapport (of "samenvoegen") voor een groep heeft verzonden. Deze variant van ASM staat bekend om zijn schaal en is het multicast paradigma van focus.

Dit is de basis voor PIM-Sparse Mode, die de meeste multicast implementaties tot dit punt hebben

gebruikt. Dit is ook de basis voor Bidirectionele PIM (PIM-BiDir), die in toenemende mate wordt ingezet voor VEEL (bronnen) tot VEEL (ontvangers) toepassingen.

Deze protocollen worden de dunne wijze genoemd omdat zij IP multicast leveringsbomen met een "dunne"ontvangerpopulatie efficiënt steunen en tot een controlevliegtuigstaat slechts op routers in de weg tussen bronnen en ontvangers, en in PIM-SM/BiDir, het Rendezvous Point (RP) leiden. Ze maken nooit status in andere delen van het netwerk. De staat in een router wordt slechts uitdrukkelijk gebouwd wanneer het ontvangt toetreedt van een stroomafwaartse router of een ontvanger, vandaar de naam "expliciet toetreedt protocollen".

Zowel PIM-SM als PIM-BiDir maken gebruik van "GEDEELDE BOMEN", waarmee verkeer vanuit elke bron naar een ontvanger kan worden doorgestuurd. De multicast staat op een gedeelde boom wordt bedoeld als (\*,G) staat, waar \* een wilde kaart voor OM HET EVEN WELKE BRON is. Bovendien ondersteunt PIM-SM de creatie van een toestand die betrekking heeft op verkeer vanuit een specifieke bron. Deze staan bekend als SOURCE TREES, en de bijbehorende staat wordt aangeduid als (S,G)-staat.

### Source-Specific Multicast

SSM is het model dat wordt gebruikt wanneer de ontvanger (of een proxy) (S,G) "joins" verstuurt om aan te geven dat hij verkeer wil ontvangen dat door bron S naar groep G wordt gestuurd. Dit is mogelijk met IGMPv3/MLDv2 "INCLUDEER"-modemlidmaatschapsrapporten. Dit model wordt het Source Specific Multicast (SSM)-model genoemd. SSM mandateert het gebruik van expliciet-sluit zich aan bij protocol tussen routers. Het standaardprotocol hiervoor is PIM-SSM, wat simpelweg de subset is van PIM-SM die gebruikt wordt om (S,G) bomen te maken. Er zijn geen gedeelde bomen (\*,G) staat in SSM.

Multicastontvangers kunnen zich dus "aansluiten" bij een ASM-groep G, of "toetreden" (of zich nauwkeuriger "abonneren" op) tot een SSM-kanaal (S,G). Om herhaling van de term "ASM-groep of SSM-kanaal" te voorkomen, wordt de term (multicast) stroom gebruikt, wat impliceert dat de stroom een ASM-groep of een SSM-kanaal kan zijn.

### Relevante multicastprotocollen/pakkettypen

Om een multicast netwerk te beveiligen is het belangrijk om de pakkettypes te begrijpen die algemeen worden ontmoet en hoe te tegen hen te beschermen. Er zijn drie belangrijke protocollen waarmee rekening moet worden gehouden:

1. IGMP/MLD
2. PIM
3. MSDP

In de volgende paragraaf wordt elk van deze protocollen besproken en worden de problemen

besproken die met elk ervan kunnen ontstaan.

## IGMP/MLD-pakketten

IGMP/MLD is het protocol dat door multicast-ontvangers wordt gebruikt om aan te geven dat zij voor een bepaalde multicast groep inhoud willen ontvangen. Internet Group Membership Protocol (IGMP) is het protocol dat in IPv4 wordt gebruikt en Multicast Listener Discovery (MLD) is het protocol dat in IPv6 wordt gebruikt.

Er zijn twee versies van IGMP die algemeen worden geïmplementeerd, IGMPv2 en IGMPv3. Er zijn ook twee versies van MLD die algemeen worden ingezet, MLDv1 en MLDv2.

IGMPv2 en MLDv1 zijn functioneel gelijkwaardig en IGMPv3 en MLDv2 zijn functioneel gelijkwaardig.

Deze protocollen worden in deze koppelingen gespecificeerd:

IGMPv2: [RFC 2236](#)

MLDv1: [RFC 3590](#)

IGMPv3 en MLDv2: [RFC 4604](#)

IGMPv2 en IGMPv3 is niet alleen een protocol maar ook een IPv4 IP-protocol (met name protocol nummer 2). Het wordt niet alleen gebruikt zoals beschreven in deze RFCs om multicast groepslidmaatschap te melden, maar ook door andere IPv4 multicast protocollen zoals DVMRP, PIM versie 1, mtrace en mrimf. Dit is belangrijk om te onthouden wanneer u probeert IGMP te filteren (bijvoorbeeld via Cisco IOS® ACL's). In IPv6 is MLD geen IPv6-protocol; in plaats daarvan wordt ICMPv6 gebruikt om MLD-pakketten te dragen. PIM versie 2 is hetzelfde protocoltype in IPv4 en IPv6 (protocolnummer 103).

## PIM-beheerpakketten

In deze paragraaf worden multicast- en unicast PIM-controlepakketten besproken. Auto-RP en Bootstrap Router (BSR), die manieren zijn om Rendezvous Points te selecteren en controlegroep-to-RP toewijzingen in PIM-SM netwerken te controleren, worden besproken.

### Multicast PIM-beheerpakketten

Multicast PIM Control-pakketten omvatten:

- PIM Hello - Het pakket van PIM Hello is een verbinding-lokaal bereik IP multicast pakket dat naar een router wordt verzonden in bijlage aan het zelfde netwerk om burenen te vestigen PIM.
- PIM Join/Prune - PIM Join/Prunes zijn link-local scope IP multicast-pakketten die worden verzonden om multicast status te maken / te verwijderen en alleen worden verzonden naar

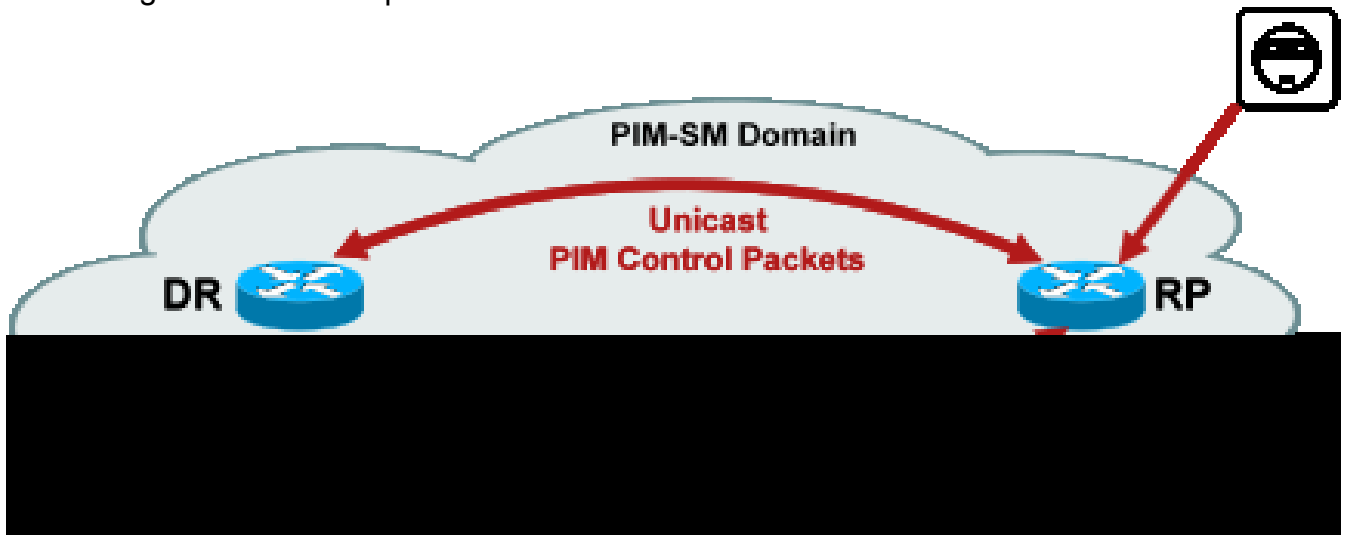
- PIM-buren. Zij zijn multicast binnen LAN om bewering, rapportonderdrukking, en andere PIM protocol details te vergemakkelijken, maar zij worden altijd gericht aan een specifieke buur.
- PIM DF-elected - PIM Designated Forwarder is de Bi-Dir PIM router verantwoordelijk voor (\*,G) JOINS verzonden naar de RP namens aangesloten ontvangers of downstream PIM buren. Voor gevallen waarin een PIM router een andere router detecteert die (\*,G) VERSTUURT OP hetzelfde segment voor dezelfde groep G, is er een verkiezing om de router met het beste pad naar de RP te bepalen.
  - PIM Assert - PIM Asserts zijn link-lokale IP multicast pakketten verzonden wanneer een PIM router gekoppeld is aan een netwerksegment dat actief pakketten doorstuurt voor een bepaalde (S,G) uit een bepaalde interface begint met het ONTVANGEN van pakketten voor die zelfde (S,G) op dezelfde interface waarop doorgestuurd worden. Deze gebeurtenis geeft de aanwezigheid aan van een andere router die denkt dat het de Single Forwarder (SF) voor deze (S,G) is. Het Assert mechanisme kiest daarvoor een unieke SF (S, G). De PIM SF router wordt verkozen om pakketten voor een bepaalde (S,G) stroom door te sturen. PIM staat voor verschillende routers toe om de rol van SF uit te voeren namens verschillende (S, G)'s, idealiter is er slechts één SF per (S, G). Verwar de SF niet met de aangewezen router. De aangewezen PIM router is de router die verantwoordelijk is voor Josef/PRUNES of SOURCE REGISTERS die naar de RP worden verzonden in een PIM-SM-netwerk.
  - PIM Bootstrap - PIM Bootstrap berichten worden verzonden in een PIMv2 netwerk om de dynamische verkiezing van een Rendezvous Point voor een bepaalde groep G te vergemakkelijken.

## Unicast PIM-beheerpakketten

Unicast PIM Control Packets zijn gericht naar of van de RP en omvatten:

- Source Register Packet - PIM Source Register Packets worden verzonden om een nieuwe multicast bron te registreren met een Rendezvous Point. Zodra een Bron multicast pakketten begint te verzenden, stuurt de Aangewezen router die aan het bronnetwerk is verbonden een unicastregisterstroom naar de RP om aan te geven dat er een actieve bron aanwezig is voor een multicast groep waarvoor de RP verantwoordelijk is. De pakketten van het bron Register worden verzonden als unicastinkapseling van de originele multicast stroom. PIM-registerberichten worden op procesniveau geschakeld en worden alleen verstuurd totdat de RP een register stopbericht verstuurt. Het effect van deze pakketten op de prestaties is evenredig met het debiet van de bron (per (S,G) stroom).
- Het Pakket van het Stop van het register - De Pakketten van het Stop van het PIM- Register worden verzonden van het Punt Rendezvous naar PIM DR. die het Bericht van het Register verzond. Register Stop-berichten worden verzonden zodra de RP multicast-pakketten natief uit de bron begint te ontvangen.
- BSR Kandidaat-Rendezvous Point Advertisement Packet - PIM BSR C-RP-Advertisement Pakketten worden naar de BSR gestuurd om een kandidaat RP te adverteren zodra de BSR is gekozen.

Afbeelding 1: PIM Unicast-pakketten



Aanvallen die zulke pakketten uitbuiten kunnen overal vandaan komen, omdat deze pakketten unicast zijn.

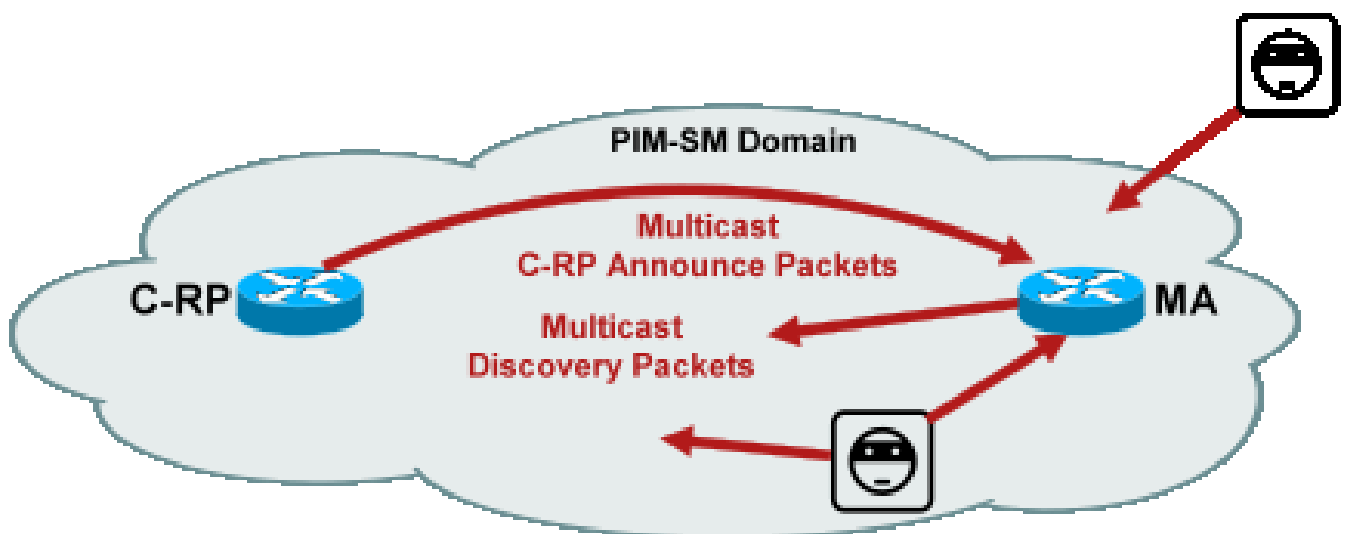
### Auto-RP-pakketten

Auto-RP is een door Cisco ontwikkeld protocol dat hetzelfde doel dient als PIMv2 BSR. Auto-RP is ontwikkeld voor BSR en ondersteunt alleen IPv4. BSR ondersteunt IPv4 en IPv6. De Mapping Agent in Auto-RP heeft dezelfde functie als de bootstrap router in BSR. In BSR, zijn de berichten van C-RP unicast aan de laarzentrekkerrouter. In Auto-RP worden berichten via multicast naar de Mapping Agent verzonden, die gemakkelijker filters aan de grens mogelijk maken, zoals later beschreven. Auto-RP wordt in detail beschreven op deze


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

In Cisco IOS worden AutoRP/BSR-pakketten altijd doorgestuurd en momenteel niet uitgeschakeld. Dit kan in het geval van Auto-RP een bijzondere blootstelling van de veiligheid opleveren.

Fig 2: Auto-RP-pakketten



---

 **Opmerking:** Hoewel Auto-RP wordt gebruikt als mechanisme voor PIM-SM RP-aankondiging en ontdekking, gebruikt het geen PIM-pakketten (IP protocol 103); in plaats daarvan gebruikt het User Datagram Protocol (UDP) poort 496 pakketten met multicast adressen.

---

Er zijn twee pakkettypes die door Auto-RP worden gebruikt:

- C-RP-aankondigt pakketten: deze pakketten zijn multicast voor alle Toewijzingsagenten en gebruiken een Internet Toegewezen Nummers Autoriteit (IANA) gereserveerd "bekend" adres (224.0.1.39). Ze worden door een C-RP gestuurd om het RP-adres en het groepsbereik aan te kondigen waarvoor die RP in staat is om als de RP te fungeren.
- C-RP Discovery-pakketten: deze pakketten zijn multicast voor alle PIM-routers en gebruiken een IANA gereserveerd "bekend" adres (224.0.1.40). Ze worden door de Auto-RP Mapping Agent verzonden om de specifieke C-RP aan te kondigen die wordt gekozen als de RP voor een bepaalde groepsbereik.

Elk van deze pakkettypes is bedoeld om door het netwerk te worden overstromd.

In Cisco IOS worden zowel 24.0.1.39 als 24.0.1.40 doorgestuurd in de PIM Dense Mode om een probleem te voorkomen waarbij geen eerdere kennis van de RP voor een groep beschikbaar is wanneer die groep wordt gebruikt om RP-informatie te distribueren. Dit is het enige aanbevolen gebruik van de PIM Dense Mode.

In Cisco IOS XR zijn Auto-RP-berichten het door:sturen van een omgekeerde pad (RPF) - overstromde hop door hop van buur naar buur. Daarom is het niet nodig om een PIM DM-routestatus te maken om Auto-RP in Cisco IOS XR te ondersteunen. Cisco IOS XR ondersteunt PIM-DM zelfs helemaal niet.

## Multicast-servicedetectiepakketten voor Protocol (MSDP)

MSDP is het IPv4-protocol waarmee een bron in het ene domein via hun respectievelijke rendez-vous points kan worden aangekondigd bij een ontvanger in een ander domein. MSDP wordt gespecificeerd in [RFC 3618](#).

Om informatie over actieve bronnen tussen PIM-domeinen te delen, wordt MSDP gebruikt. Als een bron actief wordt in één domein dan zorgt MSDP ervoor dat alle peer domeinen tijdig over deze nieuwe bron leren, wat ontvangers in andere domeinen in staat stelt om snel contact te maken met deze nieuwe bron als het gebeurt om verzonden te hebben naar een groep waarin ontvangers een belang hebben in. MSDP is nodig voor ASM/PIM-SM-multicast communicatie en werkt via een TCP-verbinding (Unicast Transport Control Protocol) die tussen RendezVous Points in de respectieve domeinen is geconfigureerd.

## Bedreigingen in een multicastomgeving



## Zones of Trust and Trust Boundaries

Dit deel van het document wordt georganiseerd door functionele entiteiten in het netwerk. Het bedreigingsmodel dat wordt besproken, krijgt vorm rond deze entiteiten. Bijvoorbeeld, verklaart deze documenten hoe een router in een multicast netwerk (van een multicast standpunt van mening) kan worden beveiligd, onafhankelijk van waar de router wordt opgesteld. Op dezelfde manier zijn er overwegingen hoe te om veiligheidsmaatregelen voor het hele netwerk, of maatregelen op een aangewezen router, rendez-vous punt, etc. op te stellen

De hier beschreven bedreigingen volgen ook deze logica, en worden georganiseerd door logische functie in het netwerk.

### Threat - Overzicht

Op een abstract niveau kan elke multicast-implementatie onderhevig zijn aan een aantal bedreigingen voor verschillende beveiligingsaspecten. De belangrijkste aspecten van beveiliging zijn vertrouwelijkheid, integriteit en beschikbaarheid.

- Bedreigingen tegen vertrouwelijkheid: In de meeste toepassingen is multicast-verkeer niet versleuteld en staat daarom voor iedereen open om te luisteren of vast te leggen op elke lijn of netwerkelement in het pad. In de sectie over GET VPN worden manieren besproken om multicast verkeer te versleutelen om dergelijke aanvallen te voorkomen.
- Bedreigingen tegen verkeersintegriteit: Zonder security op toepassingsniveau of netwerkgebaseerde beveiliging, zoals GET VPN, is multicast verkeer kwetsbaar voor wijziging tijdens de doorvoer. Dit is bijzonder belangrijk voor verkeer van besturingsplane dat multicast gebruikt, zoals OSPF, PIM en veel andere protocollen.
- Bedreigingen tegen netwerkindegriteit: zonder de beveiligingsmechanismen die in dit document worden beschreven, kunnen onbevoegde afzenders, ontvangers of gecompromitteerde netwerkelementen het multicast netwerk benaderen, verkeer verzenden en ontvangen zonder toestemming (diefstal van service) of netwerkbronnen overladen.
- Bedreigingen tegen beschikbaarheid: Er zijn een aantal mogelijkheden van de ontkenning van de dienst aanval die middelen aan wettige gebruikers niet ter beschikking kunnen stellen.

De volgende secties bespreken bedreigingen voor elke logische functie in het netwerk.

### Basisbedreigingen tegen een router

Er zijn een aantal fundamentele bedreigingen tegen een router die onafhankelijk zijn van of de

router multicast steunt en of de aanval multicast verkeer of protocollen impliceert.

De aanvallen van de ontkenning van de dienst (Dos) zijn de belangrijkste generische aanvalsvectoren in een netwerk. In principe kan elk netwerkelement met een aanval van Dos worden gericht, die het element met potentieel verder verlies of degradatie van de dienst voor wettige gebruikers kan overbelasten. Het is van het grootste belang dat u de basisaanbevelingen voor netwerkbeveiliging opvolgt die van toepassing zijn op unicast.

Het is het opmerken waard dat multicast aanvallen niet altijd opzettelijk, maar vaak toevallig zijn. De Witty-worm bijvoorbeeld, voor het eerst waargenomen in maart 2004, is een voorbeeld van een worm die zich verspreidt door willekeurige aanvallen op IP-adressen. Als gevolg van de volledige randomisatie van de adresruimte, werden multicast IP-bestemmingen ook beïnvloed door de worm. In vele organisaties, stortte een aantal eerste-hoprouters omdat de worm pakketten naar vele verschillende multicast bestemmingsadressen verzond. De routers, echter, waren niet scoped voor zulk een multicast verkeerslading met de bijbehorende staatsverwezenlijking, en effectief ervaren middeluitputting. Dit illustreert de noodzaak om multicast verkeer te beveiligen, zelfs als multicast niet in een onderneming wordt gebruikt.

Generieke bedreigingen tegen routers zijn onder meer:

- Packet-overstromingen van elk type; bijvoorbeeld tegen hardwarepaden zoals trage paden (punt) en softwarepaden zoals beheer- of besturingsplantpoorten, die Secure Shell (SSH), Telnet, BGP-protocol (BGP), OSPF, Network Time Protocol (NTP) omvatten, enzovoort
- Inbraken in de router, met daaropvolgende exploitatie van functies op de router; zwakke Telnet- of SSH-wachtwoorden en zwakke Simple Network Management Protocol (SNMP)-communitystrings zijn een veel voorkomend probleem in moderne netwerken.
- Operationele problemen zoals misconfiguraties of aanvallen met voorkennis kunnen de beveiliging van het gehele netwerk en het bijbehorende verkeer in gevaar brengen.

Wanneer multicast is ingeschakeld op een router, moet deze worden beveiligd naast unicast. Het gebruik van IP-multicast verandert het fundamentele bedreigingsmodel niet; het maakt echter aanvullende protocollen (PIM, IGMP, MLD, MSDP) mogelijk die onderhevig kunnen zijn aan aanvallen, die specifiek moeten worden beveiligd. Wanneer unicastverkeer in deze protocollen wordt gebruikt, is het bedreigingsmodel identiek aan andere protocollen die door de router worden uitgevoerd.

Het is belangrijk om op te merken dat multicast verkeer niet op dezelfde manier kan worden gebruikt als unicast verkeer om een router aan te vallen omdat multicast verkeer fundamenteel "ontvanger gedreven" is en niet op een verre bestemming kan worden gericht. Een aanvalsdoel moet expliciet worden "aangesloten" bij de multicast-stroom. In de meeste gevallen (Auto-RP is de belangrijkste uitzondering) luisteren routers alleen naar en ontvangen ze "link local" multicast

verkeer. Link Local Traffic wordt nooit doorgestuurd. Daarom kunnen aanvallen op een router met multicast pakketten alleen voortkomen uit direct verbonden aanvallers.


## Bedreigingen van de bronkant

Multicastbronnen, of pc's of videoservers soms niet onder dezelfde administratieve controle staan als het netwerk. Vanuit het oogpunt van de netwerkexploitant wordt de afzender dan ook meestal als onbetrouwbaar behandeld. Gezien de krachtige mogelijkheden van PC's en servers, en hun complexe beveiligingsinstellingen, die vaak onvolledig zijn, vormen de zenders een aanzienlijke bedreiging tegen elk netwerk, inclusief multicast. Deze bedreigingen omvatten:

- Layer 2-aanvallen: Er zijn een breed scala aan aanvalsformulieren op Layer 2 om verschillende soorten aanvallen uit te voeren. Deze zijn zowel van toepassing op unicast als op multicast. Aangezien deze aanvalsvormen niet specifiek voor multicast zijn, worden zij niet meer in detail in dit document besproken. Zie voor meer informatie het boek van Cisco Press "LAN Switch Security", ISBN-10: 1-58705-467-1.
- Aanvallen met multicast verkeer: Zoals eerder beschreven, is het moeilijk om aanvallen met multicast verkeer te voeren aangezien de eerste-hop router geen multicast verkeer doorstuurt tenzij er een luisteraar voor de groep is. Echter, de eerste hop kan worden aangevallen op verschillende manieren met multicast pakketten:
  - Netwerkverzadigingsaanvallen: een aanvaller kan een segment overspoelen met multicast-pakketten, over het gebruik van de beschikbare bandbreedte, wat kan leiden tot een DoS-conditie.
  - Multicaststatenaanvallen: De router van de eerste hop wordt overspoeld met multicastpakketten, die tot teveel staat, en een gevolgvoorwaarde van de DoS-aanval kunnen leiden.
  - Een afzender kan proberen de PIM DR te worden, via PIM hellos die worden verzonden. In dergelijke gevallen wordt er geen verkeer naar of van het netwerk doorgestuurd.
  - PIM PDF-kiespakketten voor een BiDir-PIM PDF kunnen worden gespoofd. In dergelijke gevallen wordt er geen verkeer naar of van het netwerk doorgestuurd.
  - Een afzender kan parodie AutoRP RP-ontdekking of BSR bootstrap berichten. Dit zou effectief een nep-RP aankondigen, en een PIM-SM/BiDir service neerhalen of ontwrichten.
  - Een afzender kan unicastaanvallen, zoals PIM bronregister/register-stop berichten, of kon BSR aankondigen pakketten verzenden en een nep BSR aankondigen.
  - Een afzender kan naar elke geldige multicast groep verzenden, tenzij dit wordt gefilterd. Als een bronadres wordt gespoofd en niet verhinderd bij de rand, kan de afzender het bron IP adres van een wettige afzender gebruiken, en inhoud in delen van het netwerk met voeten treden.
  - Multicast-aanvallen tegen besturingsplatformprotocollen: een aantal protocollen die niet aan multicast zijn gekoppeld, zoals OSPF en Dynamic Host Configuration Protocol (DHCP), gebruiken multicast-pakketten die kunnen worden gebruikt om deze protocollen aan te vallen

- Masquerading: Er zijn een aantal aanvalsvormen waar een afzender kan doen alsof hij een andere afzender is. IP-adressen van gespoofde bronnen zijn zo'n aanvalsvorm.
- Diefstal van de dienst: Tenzij de afzenders worden gecontroleerd, is het mogelijk om de multicast dienst van de afzender onwettig te gebruiken.

---

 Opmerking: hosts verzenden of ontvangen normaal geen PIM-pakketten. De gastheer die dit doet kan waarschijnlijk een aanval proberen.

---

## Bedreigingen van de ontvangerzijde

De ontvanger is doorgaans ook een platform met een aanzienlijke CPU-voeding en bandbreedte, en maakt een aantal aanvalsformulieren mogelijk. Deze zijn grotendeels identiek aan de bedreigingen aan de afzenderkant. Layer 2-aanvallen blijven een belangrijke aanvalsvector. Fake-ontvangers en diefstal van service zijn ook mogelijk aan de ontvangerzijde, behalve dat de aanvalsvector meestal IGMP (of Layer-2-aanvallen, zoals vermeld) is.

## Bedreigingen tegen een rendez-vous point en BSR

PIM-SM RP's en PIM-BSR's zijn cruciale punten in een multicast netwerk en zijn daarom waardevolle doelwitten voor een aanvaller. Wanneer geen van beide de eerste-hop router is, kunnen slechts de vormen van de unicastaanval, die PIM unicast omvat, direct tegen die elementen worden gericht. De bedreigingen tegen RP's en BSR's omvatten:

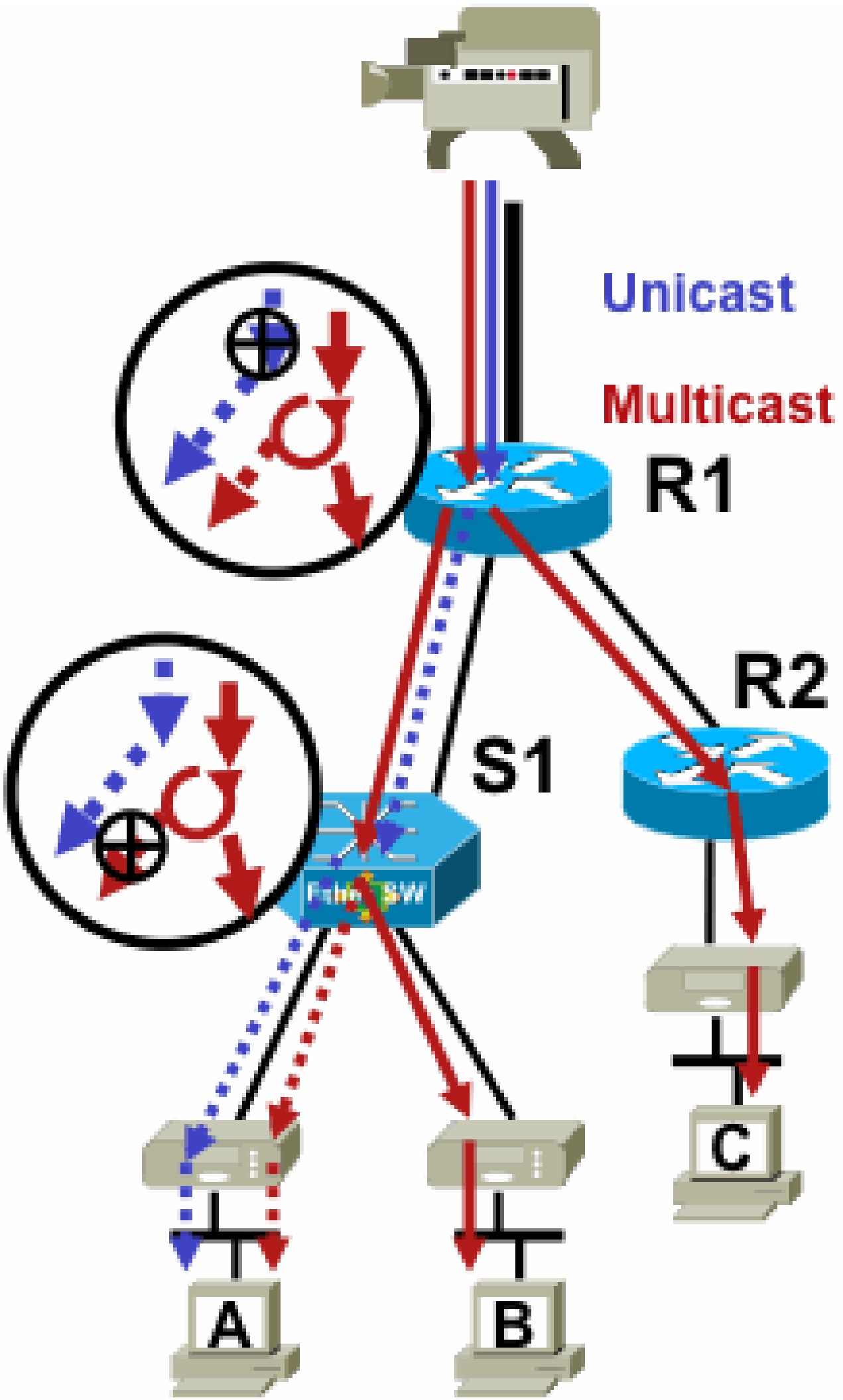
- Alle generische aanvalsvormen, zoals die in de sectie "Basis Bedreigingen Tegen een router" worden beschreven.
- PIM unicast-aanvallen, mogelijk met gespoofde IP-adressen, maken DoS-aanvallen mogelijk, via PIM-register of register-stop-berichten die door een kwaadaardig apparaat worden verzonden.

## Multicast- en Unicast-beveiliging (vergeleken)


### Overwegingen/filters voor status

Overweeg de topologie in Figuur 3, die een bron, drie ontvangers (A, B, C), een switch (S1), en twee routers (R1 en R2) toont. De blauwe lijn vertegenwoordigt een unicaststroom en de rode lijn vertegenwoordigt een multicaststroom. Alle drie de ontvangers zijn lid van de multicast flow.

Fig 3: replicatie in routers en Switches



---

 In zulke gevallen kunnen bronnen de router aanvallen door multicast verkeersoverdracht naar meerdere PIM-BiDir groepen, wat (\*,G) statusvorming veroorzaakt. De Catalyst 6500-switch ondersteunt bijvoorbeeld wel (\*,G/M) toestanden).

---

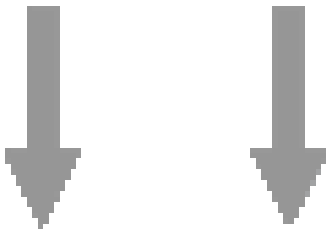
### Door ontvanger geïnitieerde aanvallen

De aanvallen kunnen uit multicast ontvangers voortkomen. Elke ontvanger die een IGMP/MLD-rapport verstuurt, maakt doorgaans een status aan op de router van de eerste hop. Er is geen gelijkwaardig mechanisme in unicast.

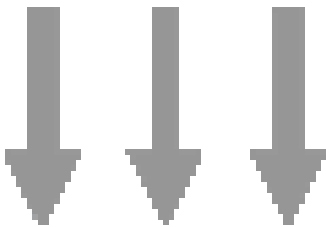
Fig 5: Expliciet doorsturen van verkeer op basis van verbindingen aan ontvangerzijde

**Source(s)**

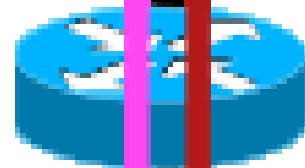
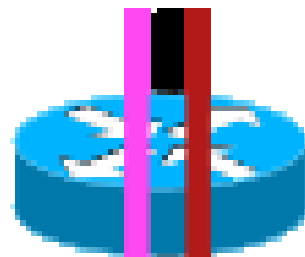
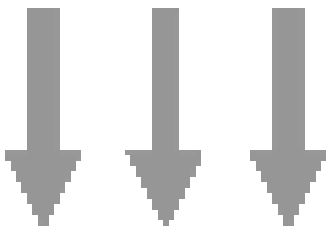
**3. State**



**State**



**State**



**RP**

**2.**



1. Een multicast-ontvanger kan proberen zich aan te sluiten bij een stroom waarvoor hij niet is geautoriseerd en probeert inhoud te ontvangen die hij niet-geautoriseerd is om te ontvangen.
2. Een multicast-ontvanger kan de beschikbare netwerkbandbreedte potentieel overladen door de belangstelling voor veel groepen of kanalen. Dit soort aanval wordt een gedeelde bandbreedte aanval tegen andere potentiële ontvangers van content.
3. Een multicast-ontvanger kan proberen een aanval te lanceren op routers of switches. Er kan een groot aantal IGMP-rapporten worden gegenereerd, waardoor een grote hoeveelheid multicast-boomstatus kan worden gecreëerd en mogelijk routercapaciteit kan worden overbelast. Dit kan op zijn beurt resulteren in een toename van multicast conversietijden of in een DoS op de router.

Verschillende manieren om dit soort aanvallen te verzachten in de volgende sectie, Security binnen een Multicast Network.

## Beveiliging binnen een multicast-netwerk

### Security voor netwerkelement


Beveiliging is geen puntfunctie, maar een intrinsiek onderdeel van elk netwerkontwerp. Als zodanig moet op elk punt in het netwerk rekening worden gehouden met de veiligheid. Het is van het grootste belang dat elk netwerkelement op de juiste wijze wordt beveiligd. Eén mogelijk aanvalsscenario dat op iedere technologie van toepassing is, is een router die door een indringer is omgedraaid. Zodra een indringer controle van een router heeft, kan de aanvaller een aantal verschillende aanvalsscenario's in werking stellen. Elk netwerkelement moet daarom op passende wijze worden beveiligd tegen elke vorm van basisaanval, en tegen specifieke multicast-aanvallen.

### Toezicht op besturingsplane (CoPP)

CoPP is de evolutie van router ACL's (rACL's) en is beschikbaar op de meeste platforms. Het principe is hetzelfde: alleen verkeer dat bestemd is voor de router wordt gecontroleerd door CoPP.

Het servicebeleid maakt gebruik van dezelfde syntaxis als elke kwaliteit van het servicebeleid, met beleidskaarten en class-maps. Daarom breidt het de functionaliteit van rACL's (vergunningen/ontkennen) uit met snelheidsbegrenzers voor bepaald verkeer naar het controlevlak.

---

 **Opmerking:** voor bepaalde platforms, zoals de Catalyst 9000 Series switches, is CoPP standaard ingeschakeld en de beveiliging is niet vervangen. Zie [CoPP handleiding](#) voor aanvullende informatie.

---

Als u beslist om rACLs of CoPP aan te passen, aan te passen of aan te maken in een actief



netwerk, moet voorzichtigheid in acht worden genomen. Aangezien beide functies de mogelijkheid hebben om al het verkeer naar het besturingsplane te filteren, moeten alle vereiste besturings- en beheerplatformprotocollen expliciet worden toegestaan. De lijst van vereiste protocollen is groot, en het kan gemakkelijk zijn om minder voor de hand liggende protocollen zoals het Terminal Access Controller Access Control System (TACACS) te overzien. Alle niet-standaard ACL- en CoPP-configuraties moeten altijd worden getest in een laboratoriumomgeving voordat ze worden geïmplementeerd op productienetwerken. Bovendien moeten initiële implementaties alleen beginnen met een vergunningenbeleid. Dit maakt validatie van onverwachte hits met ACL-hit tellers mogelijk.

In een multicastomgeving moeten de vereiste multicastprotocollen (PIM, MSDP, IGMP, enzovoort) worden toegestaan in rACL of CoPP om goed te kunnen functioneren. Het is belangrijk om te onthouden dat het eerste pakket in een multicast stream van de bron in een PIM-SM-scenario wordt gebruikt als een regelvliegtuig-pakket, om te helpen multicast status te creëren, omhoog op het besturingsplane van het apparaat. Daarom is het belangrijk om relevante multicastgroepen toe te staan in rACL of CoPP. Aangezien er een aantal platformspecifieke uitzonderingen zijn, is het belangrijk om relevante documentatie te raadplegen en elke geplande configuratie te testen vóór de implementatie.

## Local Packet Transport Service (LPTS)

Op Cisco IOS XR fungeert Local Packet Transport Service (LPTS) als een policer van verkeer naar het besturingsplane van de router, vergelijkbaar met CoPP op Cisco IOS. Bovendien, ontvang verkeer, dat unicast en multicast verkeer omvat, kan worden gefiltreerd en tarief beperkt.

## Multicastspecifieke beveiliging

In een multicast-netwerk moet elk netwerkelement worden beveiligd met multicast-specifieke beveiligingsfuncties. Deze worden in deze sectie geschetst, voor generische routerbescherming. De eigenschappen die niet op elke router, maar slechts in specifieke plaatsen in het netwerk worden vereist, en de eigenschappen die interactie tussen routers (zoals authenticatie PIM) vereisen worden besproken in de volgende sectie.

## Limieten route

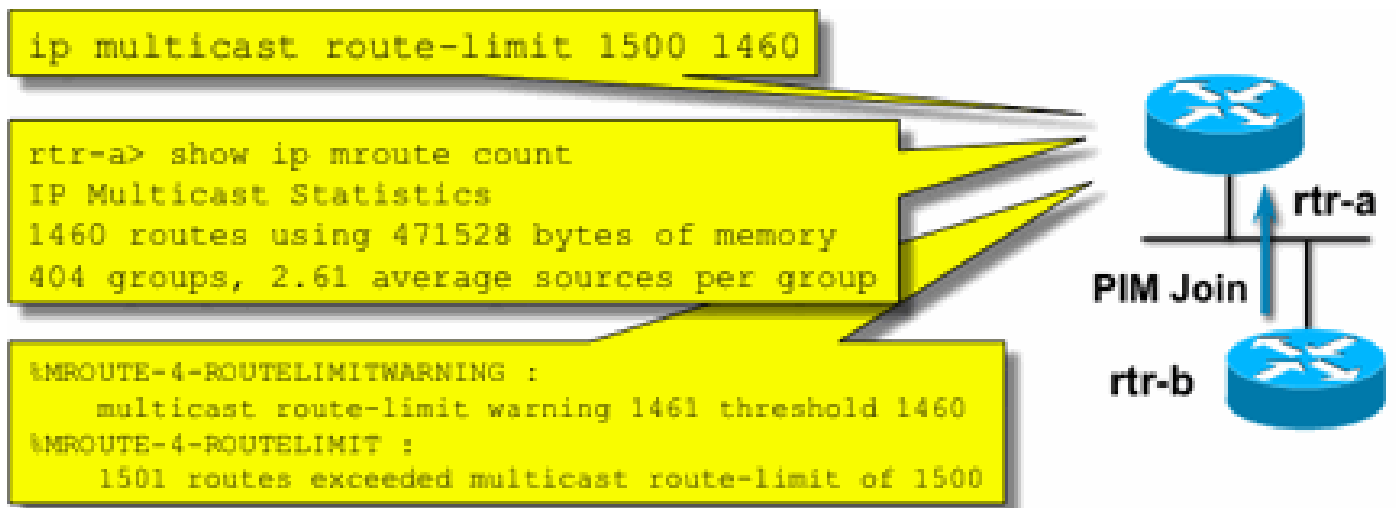
De route limietopdracht beperkt de hoeveelheid multicast routes wereldwijd op een router, en helpt om DoS-aanvallen te voorkomen.

```
<#root>
```

```
ip multicast route-limit
```

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

Fig 6: limieten route



De limieten van Mroute staan het instellen van een drempel op het aantal routes toe die in de multicast routingstabel zijn toegestaan. Als een multicast routelimit is ingeschakeld, wordt er geen multicast status gecreëerd buiten de ingestelde limiet. Er is ook een waarschuwingdrempel. Wanneer het aantal routes de waarschuwingdrempel overschrijdt, worden de syslog waarschuwingsberichten teweeggebracht. Bij de route limiet elke verdere pakketten die de status zou veroorzaken worden verworpen.

De opdracht IP multicast route-limit is ook beschikbaar per MVRP.

SAP uitschakelen Luister: geen ip sap luisteren

De sap-luisteropdracht zorgt ervoor dat een router Sessieaankondigingsprotocol/Session Description Protocol (SAP/SDP)-berichten ontvangt. SAP/SDP is een legacy protocol dat dateert van de dagen van de multicast backbone (MBONE). Deze berichten geven directoryinformatie aan over multicast-inhoud die in de toekomst of op dit moment beschikbaar is. Dit kan een bron zijn van een DoS tegen router CPU en geheugenbronnen, en daarom moet deze functie worden uitgeschakeld.

Controle toegang tot minfo informatie - de "ip multicast minfo-filter" opdracht

De minfo opdracht (beschikbaar op Cisco IOS en ook op sommige versies van Microsoft Windows en Linux) gebruikt verschillende berichten om een multicast router voor informatie te vragen. Het globale configuratiebevel van het ip multicast minfo-filter kan worden gebruikt om toegang tot deze informatie tot een ondergroep van bronnen te beperken, of het geheel onbruikbaar te maken.

Dit voorbeeld ontkent vragen afkomstig uit 192.168.1.1, terwijl vragen uit een andere bron zijn toegestaan:


```
ip multicast minfo-filter 51
```

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

Dit voorbeeld ontkent mrinfo verzoeken uit ongeacht welke bron:

```
ip multicast mrinfo-filter 52
access-list 52 deny any
```

---

 **Opmerking:** zoals met elke ACL wordt verwacht, betekent ontkennen dat het pakket wordt gefilterd, terwijl een vergunning betekent dat het pakket is toegestaan.

---

Als de mrinfo opdracht wordt gebruikt voor diagnostische doeleinden, wordt het sterk aanbevolen om de ip multicast mrinfo-filter opdracht te configureren met een geschikte ACL om vragen alleen toe te staan van een subset van bronadressen. De informatie die door de opdracht mrinfo wordt verschaft, kan ook worden opgehaald via SNMP. Complete blokken van mrinfo verzoeken (blokkeer elke bron uit vragen van het apparaat) wordt ten zeerste aanbevolen.

## Netwerk security

In deze paragraaf worden verschillende manieren besproken om PIM multicast- en unicast-controlepakketten te beveiligen, evenals Auto-RP en BSR.

### Multicastgroepen uitschakelen

De opdrachten voor ip multicast groepsbereik/ipv6 multicast groepsbereik kunnen worden gebruikt om alle bewerkingen voor groepen die door de ACL worden ontkend, uit te schakelen:

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

Als pakketten verschijnen voor een van de groepen die door de ACL worden ontkend, worden ze in alle controleprotocollen gedropt, waaronder PIM, IGMP, MLD, MSDP, en worden ook op het gegevensvlak gedropt. Daarom worden er nooit voor deze groepsbereiken geen IGMP/MLD-cacheingangen, PIM-, Multicast Routing Information Base/Multicast Forwarding Information Base (MRIB/MFIB)-status gecreëerd en worden alle gegevenspakketten onmiddellijk gedropt.

Deze opdrachten worden ingevoerd in de globale configuratie van het apparaat.

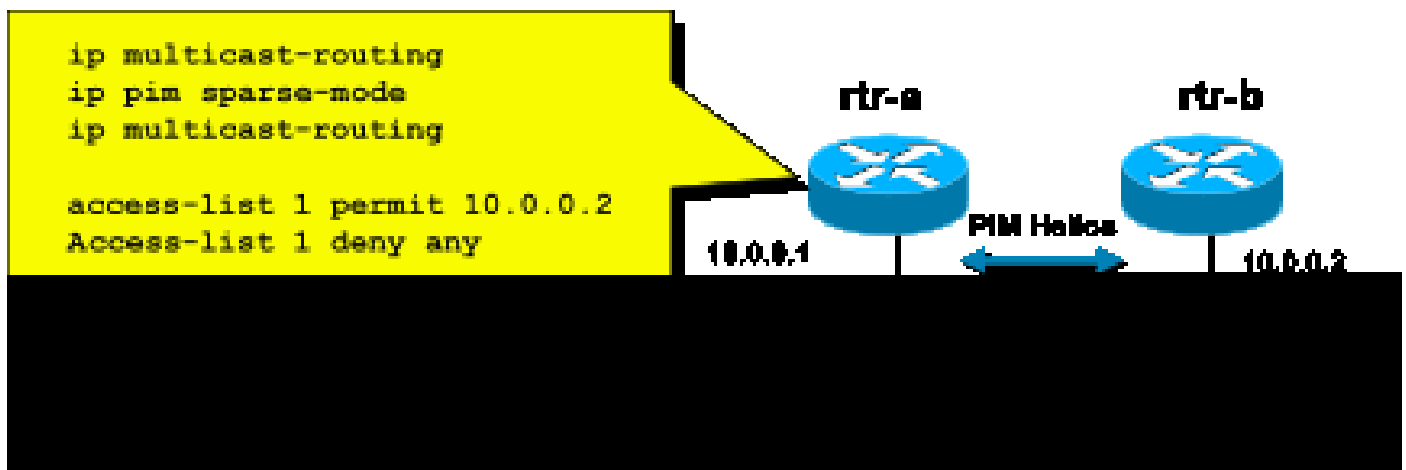
De aanbeveling is om dit bevel op alle routers in het netwerk, wanneer en waar beschikbaar op te stellen, zodat al multicast verkeer dat buiten het netwerk voortkomt wordt gecontroleerd. Let op dat deze opdrachten van invloed zijn op het gegevensvlak en het bedieningsvlak. Waar beschikbaar, biedt deze opdracht een uitgebreidere dekking dan standaard ACL's en heeft de voorkeur.

## PIM-beveiliging

### PIM-buurcontrole


Een PIM-router moet PIM Hellos ontvangen om PIM Neighbourship te kunnen opzetten. PIM Neighbourship is ook de basis voor de selectie van de aangewezen router (DR), en DR failover evenals verzenden/ontvangen PIM Join/Prune/Assert berichten.

Fig 7: PIM Neighbour Control



Om ongewenste burens te remmen, gebruikt u de IP-pim buurfilter opdracht weergegeven in afbeelding 7. Dit commando filters van alle niet-toegestane burens PIM-pakketten, waaronder Hellos, Join/Prune-pakketten, en BSR-pakketten. Hosts op het segment kunnen het bron IP adres om pretenderen te zijn de PIM buur. Layer 2-beveiligingsmechanismen (met name IP-bronbeveiliging) zijn vereist om te voorkomen dat bronadressen worden gebruikt door een poefpoging op een switch of om VLAN-ACL's in de access point te gebruiken om te voorkomen dat PIM-pakketten op hosts worden verzonden. Het sleutelwoord "log-input" kan in ACL's worden gebruikt om pakketten te registreren die overeenkomen met ACE.

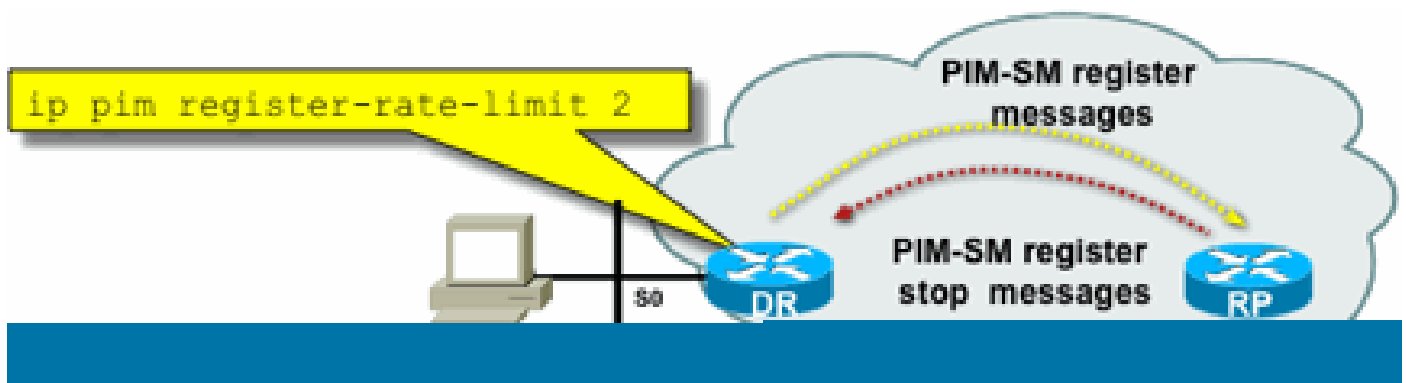
Het PIM Join/Prune-pakket wordt naar een PIM-buur verzonden om die buur toe te voegen of te verwijderen uit een bepaald (S,G) of (\*,G) pad. PIM multicast-pakketten zijn link-lokale multicast pakketten die met een Time-To-Live (TTL)=1 worden verzonden. Al deze pakketten zijn multicast naar het bekende All-PIM-Routers adres: 224.0.0.13 . Dit betekent dat al dergelijke aanvallen op zelfde Subnet moeten voortkomen zoals de router die wordt aangevallen. De aanvallen kunnen gesmeed Hello, Join/Prune, en Assert pakketten omvatten.

 **Opmerking:** een kunstmatige verhoging of aanpassing van de TTL-waarde in PIM multicast-pakketten naar een hogere waarde dan 1 leidt niet tot problemen. Het adres van alle-PIM-Routers wordt altijd lokaal op een router ontvangen en behandeld. Het wordt nooit rechtstreeks doorgestuurd door normale en legitieme routers.

Om de RP te beschermen tegen een mogelijke vloed van PIM-SM-registerberichten, moet de DR deze berichten te beoordelen. Gebruik de opdracht `ip pim register-rate-limit`:

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

Fig 8: Tunnelbeheer PIM-SM registreren



PIM unicastpakketten kunnen worden gebruikt om de RP aan te vallen. Daarom kan de RP worden beschermd door infrastructurele ACL's tegen dergelijke aanvallen. Vergeet niet dat multicast afzenders en ontvangers nooit PIM-pakketten hoeven te verzenden, zodat het PIM-protocol (IP-protocol 103) meestal kan worden gefilterd op de rand van de abonnee.

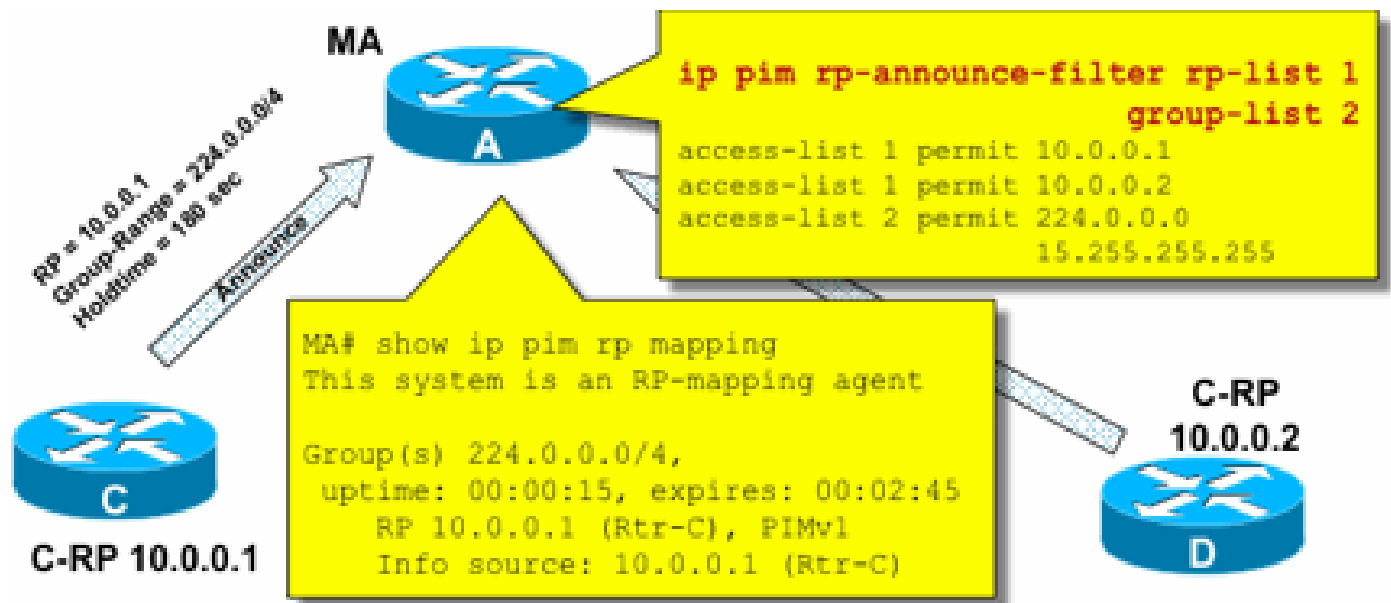
#### Auto-RP Control - RP Announce Filter

De opdracht `filter` voor `IP-pim rp-aankondigen` is een extra beveiligingsmaatregel die indien mogelijk met Auto-RP kan worden geconfigureerd:

```
<#root>  
ip pim rp-announce-filter
```

Dit kan worden geconfigureerd op de Mapping Agent om te bepalen welke routers worden geaccepteerd als kandidaat-RP's voor welke groepsbereik / groepsmodus.

Fig 9: Auto-RP - RP Announce Filter



### Auto-RP-controle - Auto-RP-berichten beperken

Gebruik de opdracht `multicast border` om AutoRP-pakketten, RP-aankondigen (224.0.1.39) of RP-discovery (224.0.1.40) te beperken tot een bepaald PIM-domein:

```
<#root>
```

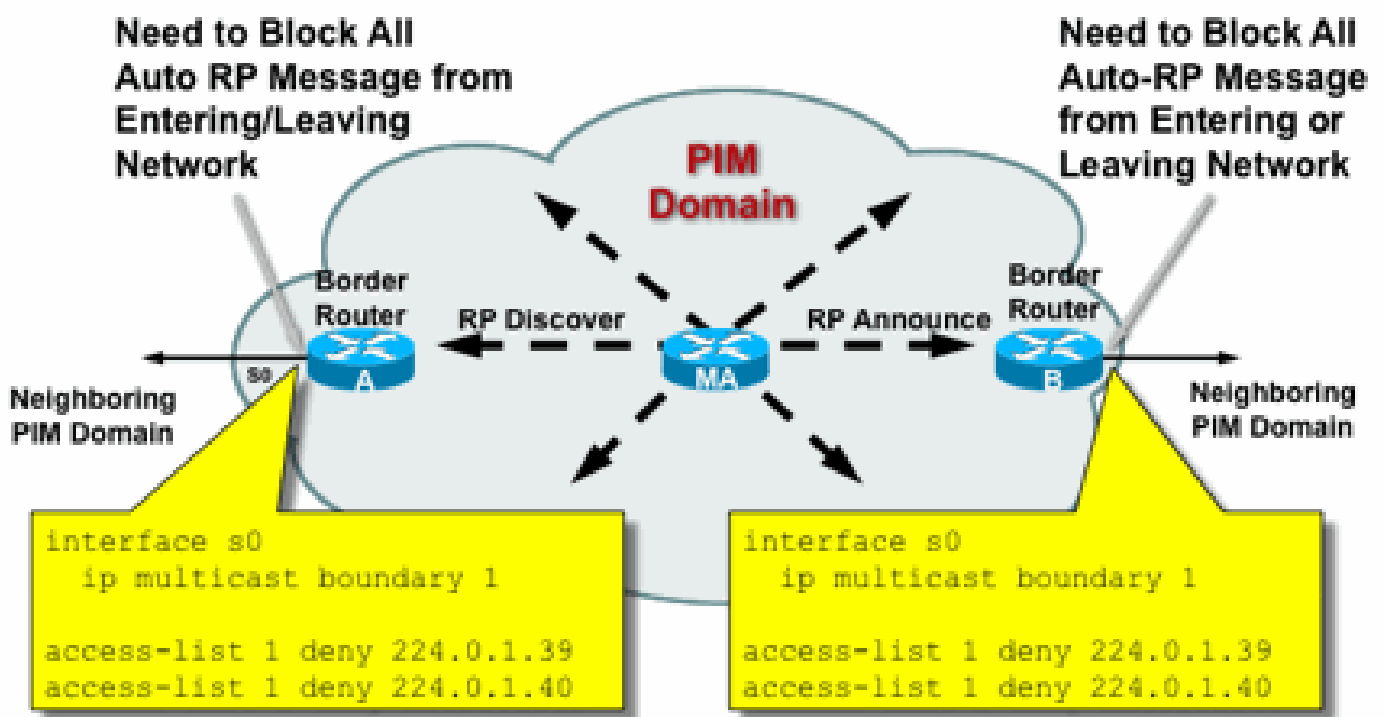
```
ip multicast boundary
```

```
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)

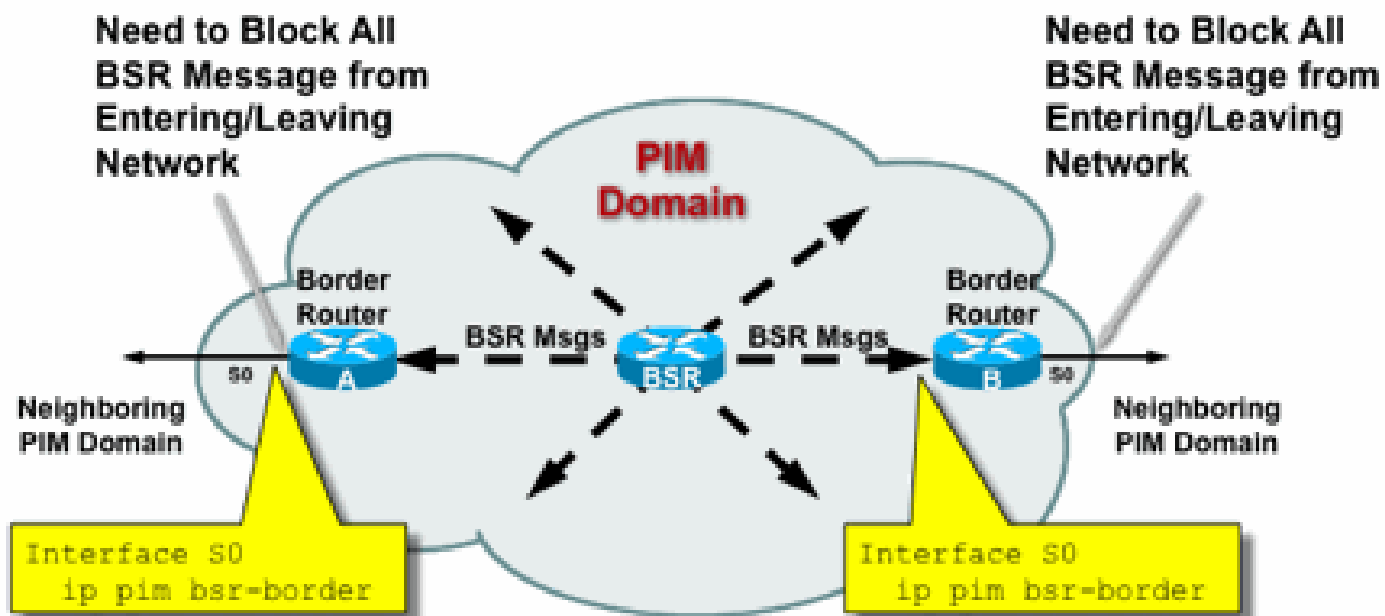
Afbeelding 10: Opdracht Multicast-grens



### BSR-controle - BSR-berichten beperken

Gebruik de IP pim bsr-border opdracht om BSR-berichten te filteren op de rand van een PIM-domein. Geen ACL is nodig aangezien de BSR-berichten hop-door-hop met link lokale multicast worden doorgestuurd.

Afbeelding 11: BSR-grens



## Filters die betrekking hebben op RP/PIM-SM

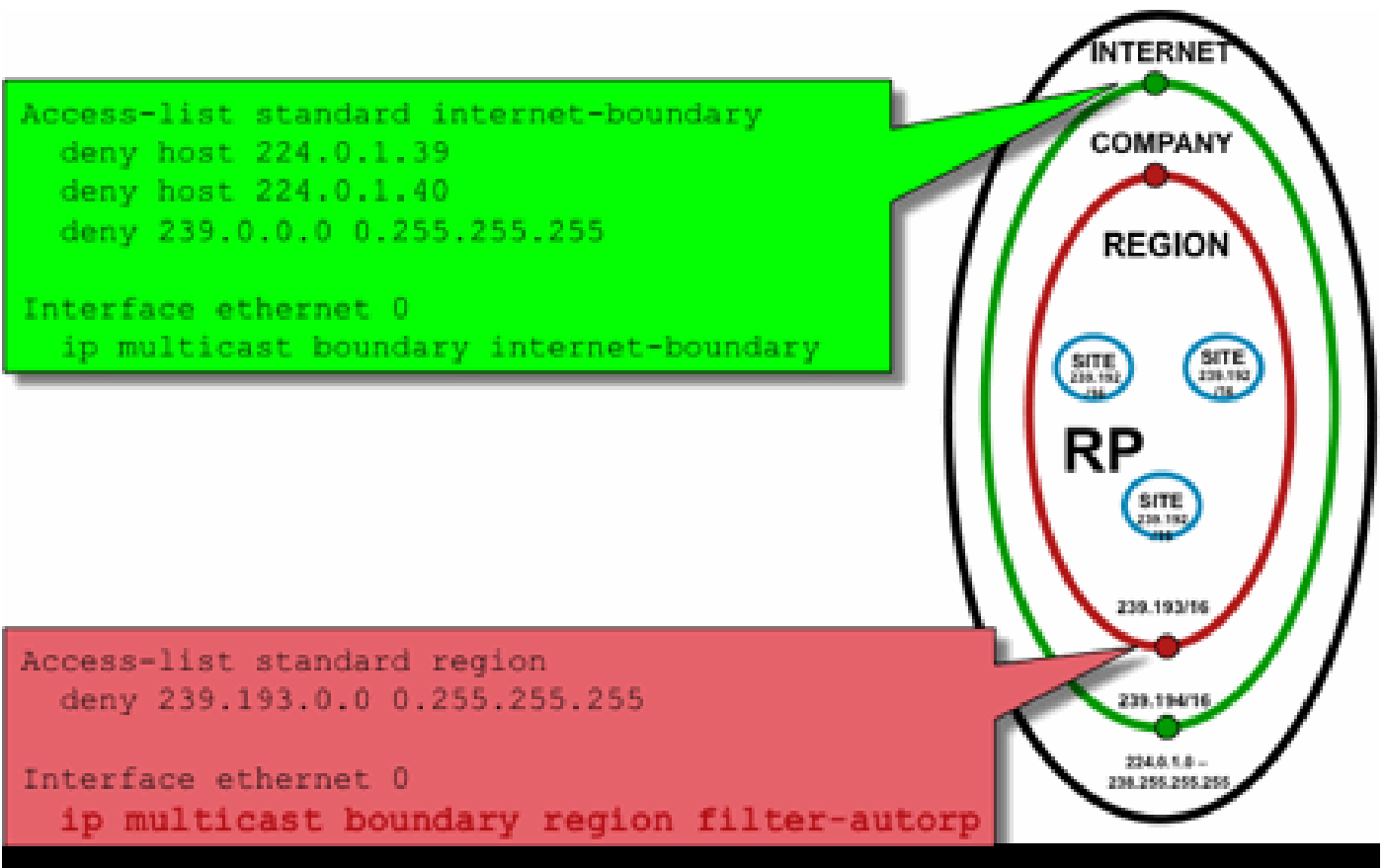
Als onderdeel van deze laatste sectie worden filters tegen PIM-SP- en RP-besturingsvliegtuigpakketten en Auto-RP-, BSR- en MSDP-berichten besproken.

### Auto-RP-filters

Afbeelding 12 toont een voorbeeld van Auto-RP-filters in combinatie met adresscopen. Er worden twee verschillende manieren getoond om een regio aan elkaar te binden. De twee ACL's zijn gelijkwaardig vanuit een Auto-RP-perspectief.

Fig 12: Auto-RP filters / Scopes





Het idee van de filters van de interfacegrens voor Auto-RP is ervoor te zorgen dat de auto-rp aankondigingen slechts de gebieden bereiken die zij hebben gesteund. Regionale, bedrijfs- en internetbrede toepassingsgebieden worden gedefinieerd, en in elk geval zijn er RP's en Auto-RP-advertenties in elke scope. Beheerders willen alleen dat de regionale referentiepunten bekend zijn bij de regionale routers, dat de bedrijfsplannen bekend zijn bij de regionale routers en de bedrijfsrouters, en dat alle internetreferentiepunten wereldwijd beschikbaar zijn. Verdere niveaus van toepassingsgebieden zijn mogelijk.

Zoals getoond in de foto, zijn er twee fundamenteel verschillende manieren om Auto-RP-pakketten te filteren: De internetgrens roept expliciet de auto-rp-controlegroepen (224.0.1.39 en 224.0.1.40), die resulteren in filters tegen alle Auto-RP-pakketten. Deze methode kan worden gebruikt op de rand van een administratief domein, waar geen Auto-RP-pakketten worden doorgegeven. De grens van het Gewest gebruikt het filter-auto-rp sleutelwoord om een onderzoek van de rp-aan-groep-bereik aankondigingen binnen Auto-RP pakketten te veroorzaken. Wanneer een aankondiging uitdrukkelijk door ACL wordt ontkend, wordt het verwijderd uit het pakket auto-RP alvorens het pakket door:sturen. In het voorbeeld kunnen de referentieprijzen voor de hele onderneming binnen de regio's bekend worden gemaakt, terwijl de referentieprijzen voor de hele regio worden gefilterd op de grens van de regio tot de rest van de onderneming.

## Inter-Domain Filters en MSDP

In dit voorbeeld werkt ISP1 als een PIM-SM-doorvoerprovider. Ze ondersteunen alleen MSDP-peering met burens en ze accepteren alleen (S, G), maar geen (\*, G) verkeer op de grensrouters.

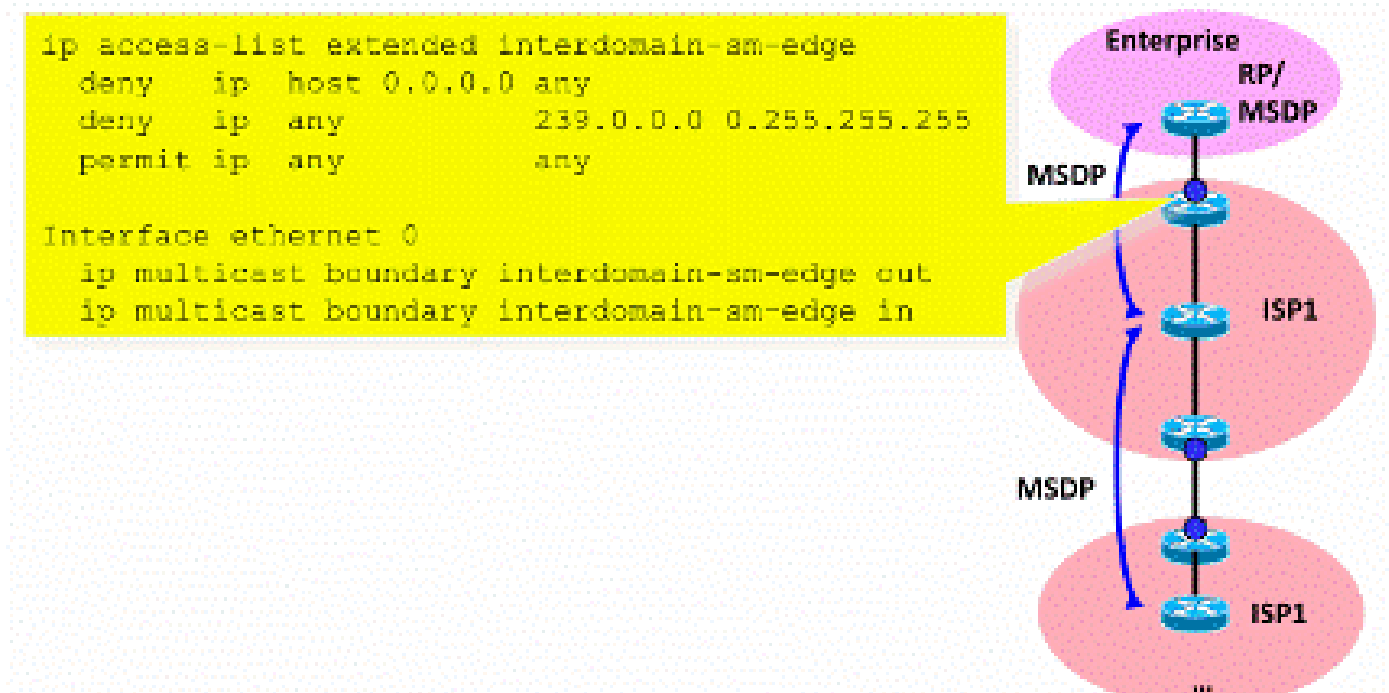
In interdomainsystemen (meestal tussen autonome systemen) zijn er twee basisveiligheidsmaatregelen te nemen:

1. Beveilig het gegevensvlak, door het multicast grensbevel. Dit zorgt ervoor dat multicast verkeer alleen wordt geaccepteerd voor gedefinieerde groepen (en mogelijk bronnen).
2. Beveilig het verkeer met een interdomeinbesturingsplane (MSDP). Dit bestaat uit een aantal afzonderlijke beveiligingsmaatregelen: MSDP-contentcontrole, staatsbeperking en buurverificatie.

Afbeelding 13 biedt voorbeeldconfiguratie van een interfacefilter op een van de grensrouters van ISP1.

Om het gegevensvlak op de domeingrens te beveiligen, remt u (\*,G) door filters tegen "host 0.0.0.0" en administratief scoped adressen via het multicast border-commando:

Afbeelding 13: Filter voor interdomeinen (\*,G)



Om het bedieningsvliegtuig te beveiligen, verhardt MSDP via drie fundamentele veiligheidsmaatregelen:

#### 1) MSDP SA-filters

Het is een "best common practice" om de inhoud van MSDP berichten via MSDP SA filters te filteren. Het belangrijkste idee van dit filter is om propagatie van multicast staat voor toepassingen

en groepen te vermijden die geen toepassingen voor het hele internet zijn en niet buiten het brondomein hoeven te worden doorgestuurd. Idealiter staan de filters uit veiligheidsoogpunt alleen bekende groepen toe (en mogelijk afzenders) en ontkennen ze onbekende afzenders en/of groepen.

Het is gewoonlijk niet mogelijk om alle toegestane afzenders en/of groepen expliciet op te sommen. aanbevolen wordt om het standaardconfiguratiefilter voor PIM-SM-domeinen te gebruiken met één RP voor elke groep (geen MSDP-mesh-groep):

```
!--- 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
    !
```

Het wordt aanbevolen om zo strikt mogelijk en in beide richtingen, inkomend en uitgaand te filteren.

Gebruik voor meer informatie over aanbevelingen voor MSDP SA-filters:

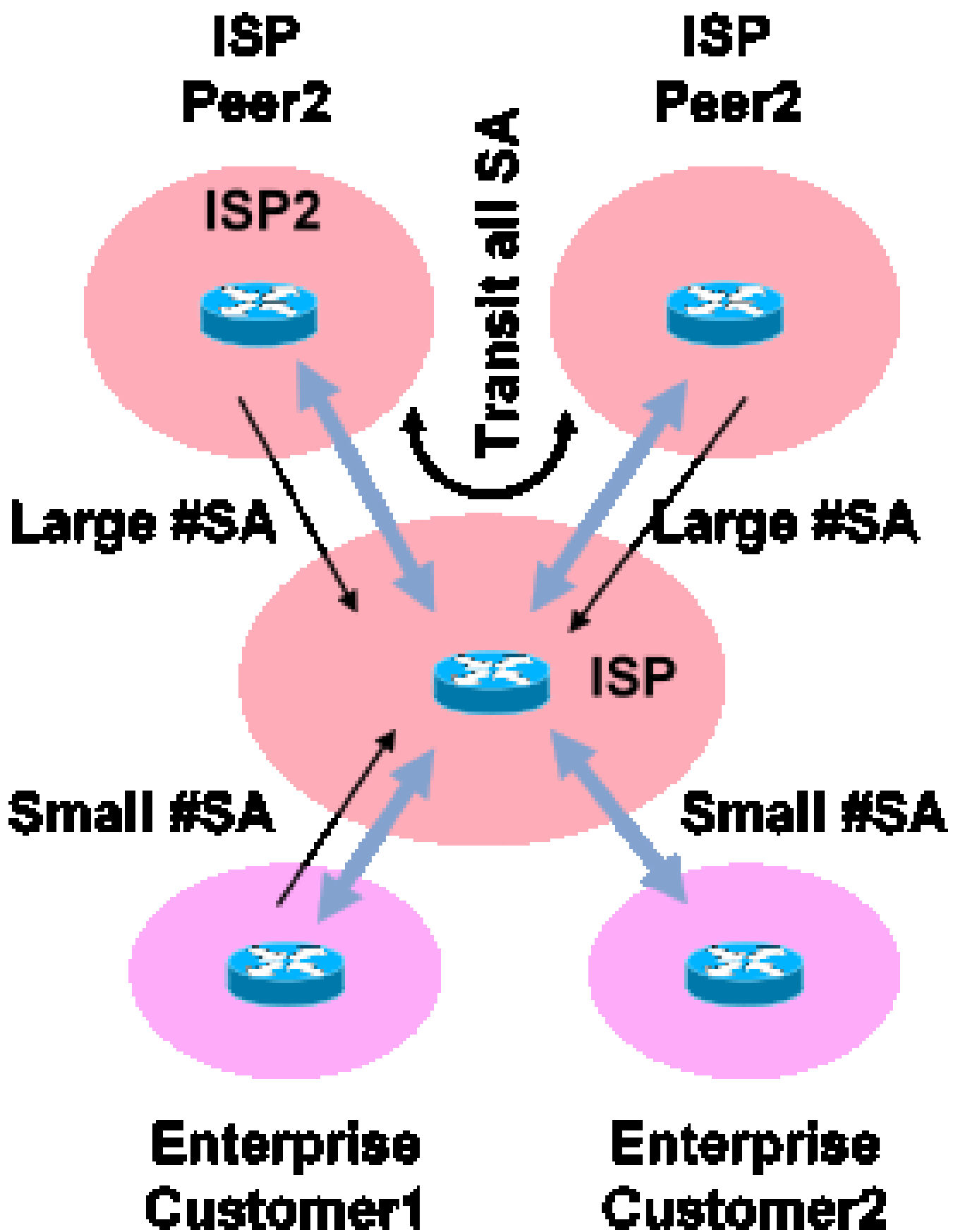
<https://www.cisco.com/c/en/us/support/docs/ip/ip-multicast/13717-49.html>

## 2) Beperking van MSDP-status

Wanneer MSDP is ingeschakeld tussen meerdere autonome systemen (AS), wordt aanbevolen de hoeveelheid status te beperken die in de router is ingebouwd vanwege "Source-Active" (SA)-berichten die van burens worden ontvangen. U kunt de opdracht `IP msdp sa-limit` gebruiken:

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

Fig 14: MSDP-besturingsplane



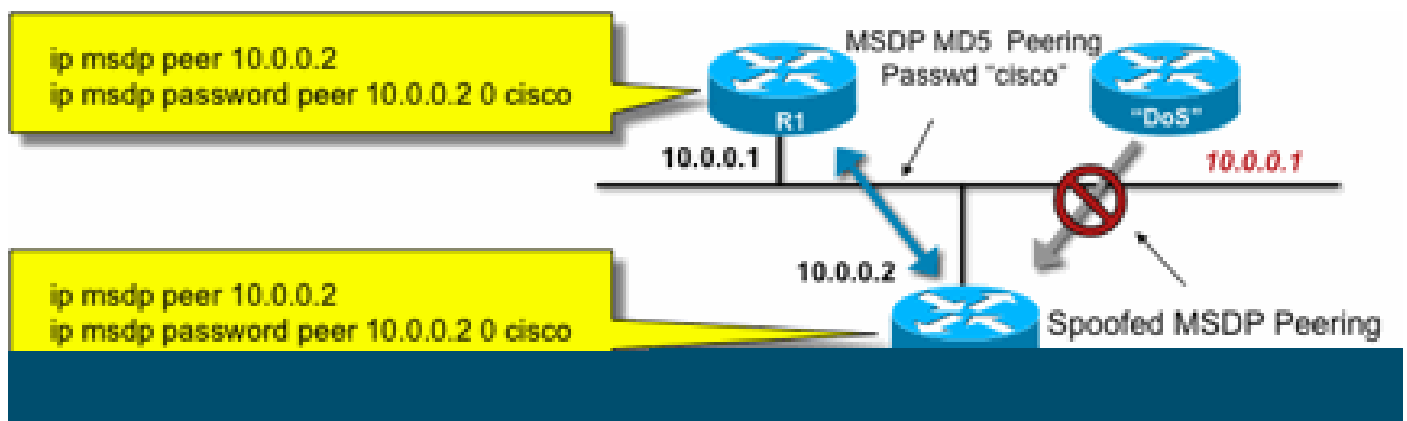
Met de ip msdp sa-limit opdracht kunt u het aantal SA-staten beperken die zijn gemaakt vanwege SA-berichten die zijn geaccepteerd door een MSDP-peer. Enkele eenvoudige aanbevelingen voor een vuistregel zijn:

- Kleine limiet van stub-buurman
- Grote limiet voor transit-buurman (bijvoorbeeld maximum #SAs in internet)
- Transit ISP - configureer maximaal #SAs uw platform kan ondersteunen

### 3) MSDP MD5-buurverificatie

Aanbevolen wordt om de wachtwoordverificatie met Message-Digest Algorithm (MD5) op MSDP-peers te gebruiken. Hierbij wordt de TCP/MD5-handtekeningsoptie gebruikt die equivalent is aan het gebruik dat in [RFC 6691](#) is beschreven om BGP te beveiligen.

Afbeelding 15: MSDP MD5-buurverificatie



Deze drie MSDP-beveiligingsaanbevelingen hebben verschillende doelstellingen:

- Buurverificatie (met MD5) zorgt ervoor dat alleen vertrouwde MSDP-peers berichten kunnen verzenden.
- De SA-filters zorgen ervoor dat zelfs een vertrouwde MSDP-peer alleen SA-aankondigingen kan verzenden die in overeenstemming zijn met vooraf overeengekomen bron/groepsbeleid.
- De SA-limiet zorgt er verder voor dat zelfs met legitieme (S,G) aankondigingen van legitieme peers het beschikbare geheugen niet kan worden uitgeput.

## Afzender/bron problemen

Vele multicast veiligheidskwesties die bij de afzender voortkomen kunnen met aangewezen unicast veiligheidsmechanismen worden verlicht. Een aantal unicast beveiligingsmechanismen worden aanbevolen best practices hier:

- Bescherming tegen bronadres (Unicast Reverse Path Forwarding, uRPF of ACL en IP-bronbeveiliging voor de toegangslaag)
- ACL's voor infrastructuur (IP geen (naar) <ruimte voor kernadres> ontkennen)

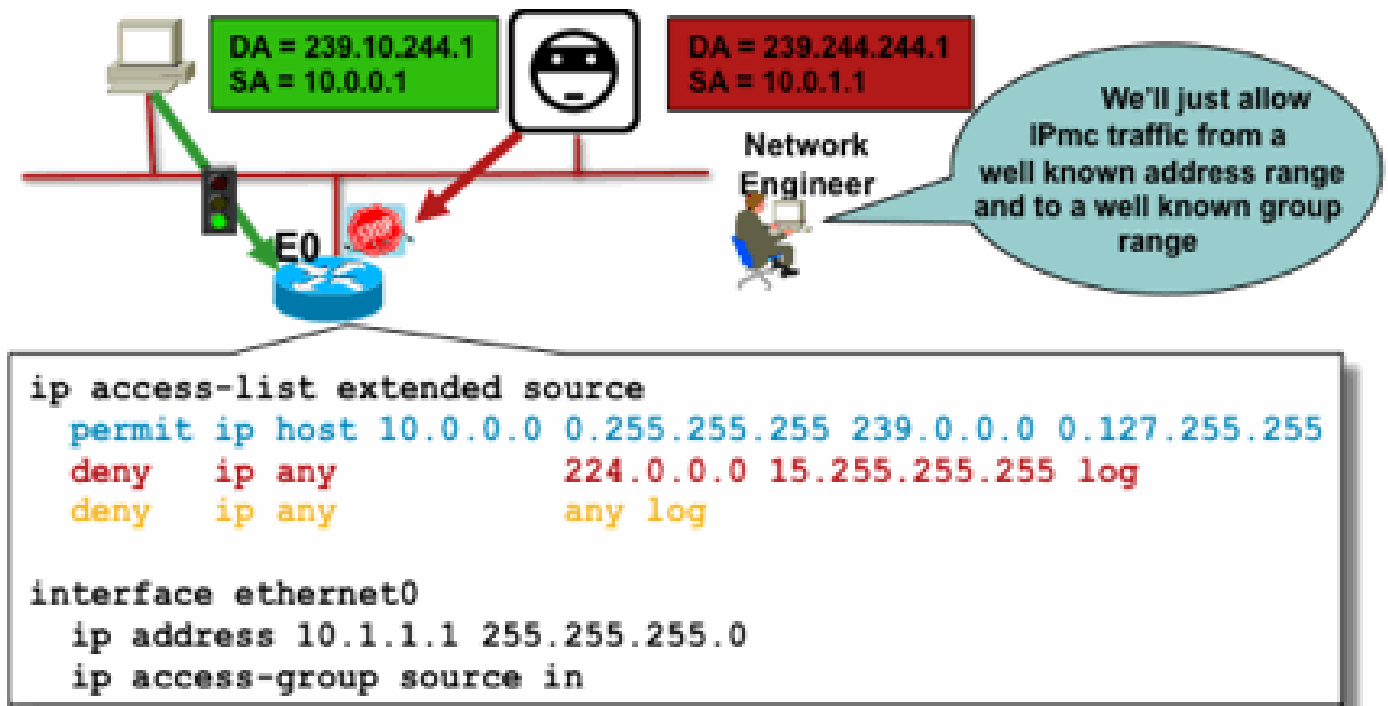
Dergelijke maatregelen kunnen worden gebruikt om gerichte aanvallen op de kern te blokkeren. Dit zou bijvoorbeeld ook problemen oplossen zoals aanvallen die PIM unicastpakketten gebruiken voor de RP, die "binnen" het netwerk is en daarom beschermd zou worden door de infrastructuur

ACL.

## Op pakketfilter gebaseerde toegangscontrole - controlebronnen

In het voorbeeld in afbeelding 16 wordt het filter geconfigureerd op de LAN-interface (E0) van de eerste-hop multicast router (Aangewezen router). Het filter wordt gedefinieerd door een uitgebreide toegangscontrolelijst met de naam "bron". Deze ACL wordt toegepast op de broninterface van de aangewezen router die op de bron-LAN is aangesloten. In feite, vanwege de aard van multicast verkeer, zou er een gelijkaardig filter kunnen moeten zijn dat op alle LAN-onder ogen ziende interfaces wordt gevormd waarop de bronnen actief zouden kunnen worden. Aangezien het niet in alle gevallen mogelijk is om precies te weten waar de bronactiviteit plaatsvindt, wordt aanbevolen om dergelijke filters op alle ingangspunten in het netwerk toe te passen.


Fig 16: Controlebronnen



Het doel van dit filter is verkeer van een specifieke bron of een waaier van bronadressen aan een specifieke groep of een waaier van groepsadressen te verhinderen. Deze filter werkt voordat PIM enige routes creëert en helpt de status te beperken.

Dit is een standaard ACL-gegevensvlak. Dit wordt geïmplementeerd op ASIC's op high-end platforms en er wordt geen prestatieverlies opgelegd. Gegevensvlak-ACL's worden aanbevolen en krijgen de voorkeur boven controlevlak voor direct verbonden bronnen omdat zij de impact van ongewenste verkeersintensiteit minimaliseren. Het is ook zeer effectief om de bestemming (IP multicast groepsadressen) te beperken waarnaar pakketten kunnen worden verzonden. Aangezien dit een routerbevel is, kan het geen bron-IP adres overwinnen dat wordt gespoofd (zie vroeger deel van deze sectie). Daarom wordt aangeraden om ofwel extra Layer 2 (L2)-

mechanismen te leveren, ofwel een consistent beleid voor alle apparaten die verbinding kunnen maken met een bepaald lokaal netwerk/virtueel lokaal netwerk (LAN/VLAN).

 Opmerking: het sleutelwoord "log" in een ACL is erg handig om hits te begrijpen tegen een specifieke ACL-ingang; dit gebruikt echter CPU-bronnen en moet met zorg worden verwerkt. Ook worden op hardwaregebaseerde platformen ACL-logberichten gegenereerd door een CPU, en daarom moet rekening worden gehouden met de CPU-impact.

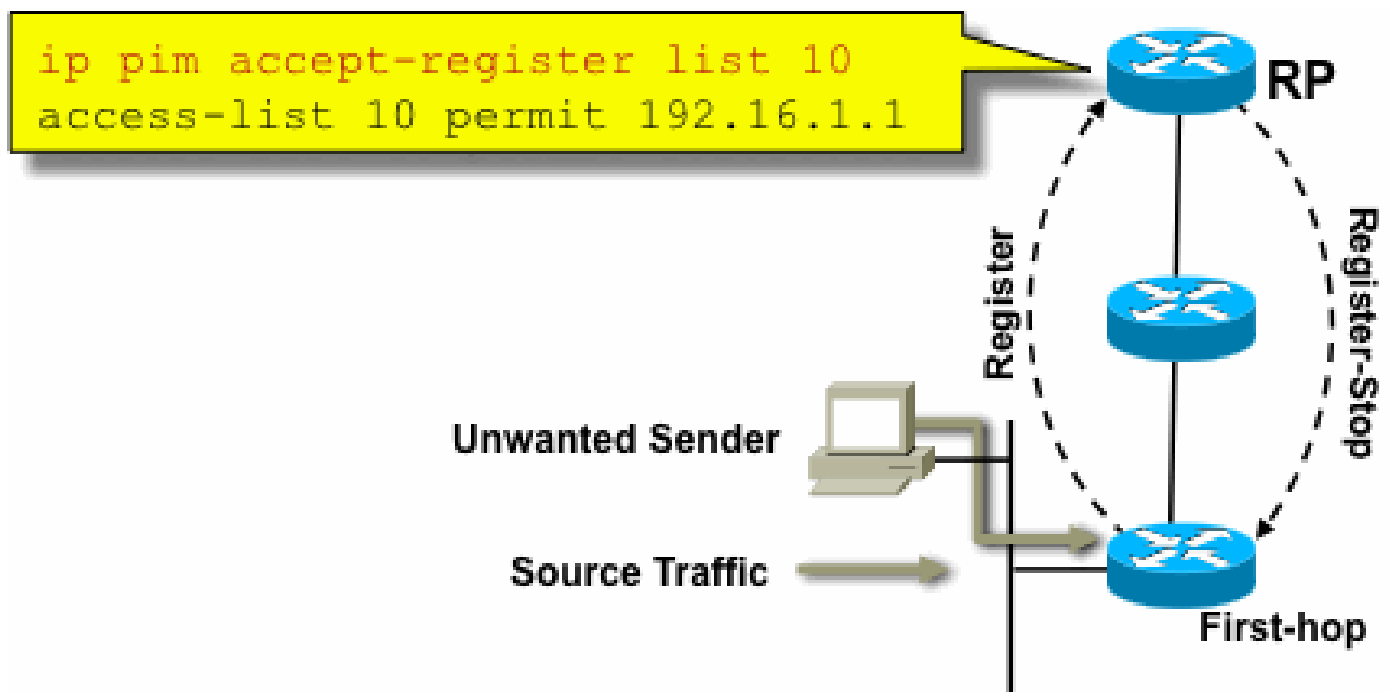
## PIM-SM-broncontrole

Een van de werkelijke voordelen van de ASM / PIM-SM architectuur vanuit veiligheidsoogpunt is het feit dat het Rendezvous Point voor alle bronnen in het netwerk voor elke groepsbereik één controlepunt geeft. Dit kan worden benut met een apparaat dat acceptatie-register filter wordt genoemd. De opdracht voor dit filter is als volgt:

```
<#root>
```

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

Fig 17: PIM-SM-broncontrole



In een PIM-SM-netwerk kan een ongewenste verkeersbron met deze opdracht worden bestuurd. Wanneer het bronverkeer de router van de eerste hop raakt, leidt de router van de eerste hop (DR) tot (S, G) staat en verzendt een PIM BronRegister bericht naar RP. Als de bron niet vermeld is in de acceptatie-register filterlijst (geconfigureerd op de RP), dan verwerpt de RP het Register



en stuurt een onmiddellijk Register-Stop bericht terug naar de DR.

In het getoonde voorbeeld, is eenvoudige ACL toegepast op de RP, die filters alleen op het bronadres. Het is ook mogelijk om de bron EN de groep te filteren met behulp van een uitgebreide ACL op de RP.

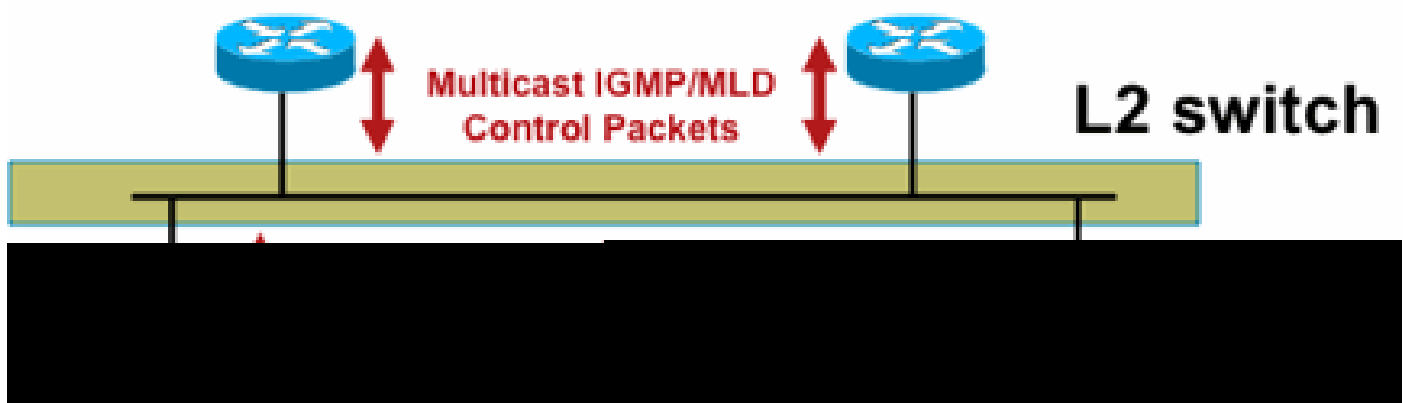
Er zijn nadelen met bronfilters omdat met de pim accepteer-register opdracht op de RP, PIM-SM (S,G) status nog steeds op de eerste-hop router van de bron wordt gecreëerd. Dit kan resulteren in verkeer bij ontvangers lokaal aan de bron en gelegen tussen de bron en de RP. Bovendien werkt de pim accepteer-register commando op het controlevlak van de RP. Dit kan worden gebruikt om de RP te overladen met nep-register berichten, en mogelijk een DoS-conditie veroorzaken.

Het wordt aanbevolen om de pim acceptatie-register opdracht op de RP toe te passen naast andere methoden, zoals de toepassing van eenvoudige dataplatform ACL's op alle DR's, op alle ingangspunten in het netwerk. Terwijl toegang ACLs op DR. in een perfect gevormd en bediend netwerk voldoende zou zijn, wordt het geadviseerd om het pim acceptatie-register bevel op RP als secundair veiligheidsmechanisme in het geval van misconfigurations op de randrouters te vormen. Gelaagde veiligheidsmechanismen met hetzelfde doel worden "verdediging in de diepte" genoemd, en is een gemeenschappelijk ontwerp-principe in veiligheid.

## Problemen met ontvangers - Control IGMP/MLD

De meeste ontvangerproblemen vallen binnen het domein van de interacties van het IGMP/MLD-ontvangerprotocol.

Afbeelding 18: Control IGMP



Wanneer IGMP- of MLD-pakketten worden gefilterd, onthoud deze punten:

- IPv4: IGMP is een IPv4-protocoltype (IPv4 protocol 2)
- IPv6: MLD wordt meegeleverd in pakketten met protocoltypen ICMPv6

Het IGMP-proces wordt standaard ingeschakeld zodra IP-multicast is ingeschakeld. IGMP-pakketten dragen ook deze protocollen, en daarom worden al deze protocollen ingeschakeld wanneer multicast is ingeschakeld:

- PIMv1 - PIMv1 was de eerste versie van PIM en is altijd ingeschakeld in Cisco IOS voor migratiedoeleinden. Huidige implementaties maken allemaal gebruik van PIMv2.
- Mrinfo - Mrinfo is een Unix-opdracht die Cisco IOS heeft geërfd om multicast-buren weer te geven. Cisco raadt het gebruik van SNMP aan in plaats van de opdracht mrinfo.
- DVMRP - DVMRP is een legacy dense mode afstandvectorprotocol met zeer beperkte schalingkenmerken. Cisco IOS-ondersteuning voor DVMRP is teruggetrokken of is al afgekeurd.
- Mtrace - Mtrace is het multicast-equivalent van unicast "traceroute" en is een handig hulpmiddel

Zie [IGMP-typenummers \(Internet Group Management Protocol\) van Iran voor](#) meer informatie

```
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
```

Unicast IGMP-pakketten (voor IGMP/UDLR) kunnen worden gefilterd, aangezien dit waarschijnlijk aanvalspakketten zijn en geen geldige IGMP-protocolpakketten. Unicast IGMP-pakketten worden ondersteund door Cisco IOS ter ondersteuning van unidirectionele links en andere uitzonderingsvoorwaarden.

Gesmede IGMP/MLD-querypakketten kunnen resulteren in een lagere IGMP-versie dan verwacht.

In het bijzonder sturen hosts idealiter nooit IGMP-queries omdat een query verzonden met een lagere IGMP-versie alle hosts die deze query ontvangen kan veroorzaken om terug te keren naar de lagere versie. In aanwezigheid van IGMPv3 / SSM-hosts kan dit de SSM-stromen "aanvallen". In het geval van IGMPv2 kan dit resulteren in langere verloftijden.

Als er een niet-redundante LAN met één IGMP-query aanwezig is, moet de router IGMP-vragen die zijn ontvangen, laten vallen.

Als er een redundante / gemeenschappelijke passieve LAN bestaat, is een switch die IGMP-spiegeling kan uitvoeren vereist. Er zijn 2 specifieke functies die in dit geval kunnen helpen:

- Routerbewaker
- Minimale IGMP-versie, opdracht

Routerbewaker

Elke routerpoort kan een multicast routerpoort worden als de switch een multicast routerbeheerpakket (IGMP algemene query, PIM Hello of CGMP Hello) op die switch ontvangt. Wanneer een switch poort een multicast routerpoort wordt, wordt al het multicast verkeer naar die poort verzonden. Dit kan worden voorkomen met "Router Guard". De functie Router Guard vereist niet dat IGMP-spionage is ingeschakeld.

Met de functie Router Guard kan een gespecificeerde poort worden aangewezen als een multicast hostpoort. De poort kan geen routerpoort worden, zelfs als multicast routerbeheerpakketten worden ontvangen.

Deze pakkettypes worden verworpen als zij op een poort worden ontvangen die Router Guard heeft ingeschakeld:

- IGMP-query-berichten
- IPv4 PIMv2-berichten
- IGMP PIM-berichten (PIMv1)
- IGMP DVMRP-berichten
- RGMP-berichten (Router-Port Group Management Protocol)
- Cisco Group Management Protocol (CGMP)-berichten

Wanneer deze pakketten worden vernietigd, worden de statistieken bijgewerkt die erop wijzen dat de pakketten wegens Router Guard worden gelaten vallen.

#### Minimale IGMP-versie

Het is mogelijk om de minimumversie van toegestane IGMP-hosts te configureren. U kunt bijvoorbeeld alle IGMPv1-hosts of alle IGMPv1- en IGMPv2-hosts verbieden. Dit filter is alleen van toepassing op lidmaatschapsrapporten.

Als de hosts zijn aangesloten op een gemeenschappelijk "passief" LAN (bijvoorbeeld een switch die IGMP-controle niet ondersteunt of niet daarvoor is geconfigureerd), is er ook niets dat een router kan doen aan dergelijke foutieve vragen anders dan de "oude versie"-lidmaatschapsrapporten negeren die dan worden geactiveerd en niet zelf terugvallen.

Aangezien IGMP-vragen zichtbaar moeten zijn voor alle hosts, is het niet mogelijk om een op hash gebaseerd mechanisme voor berichtverificatie (HMAC) te gebruiken met een vooraf gedeelde sleutel, zoals statische sleutel IPsec, om IGMP-vragen te verifiëren via "geldige routers". Als twee of meer routers zijn gekoppeld aan een gemeenschappelijk LAN-segment, moet u een IGMP-querier kiezen. In dat geval is het enige filter dat kan worden gebruikt een IP-toegangsgroepfilter op basis van het IP-adres van de andere IGMP-router die vragen verstuurt.

"Normale" multicast IGMP-pakketten moeten worden toegestaan.

Deze filter kan op ontvangerpoorten worden gebruikt om alleen "goede" IGMP-pakketten toe te staan en bekende "slechte" pakketten te filteren:

```
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

```


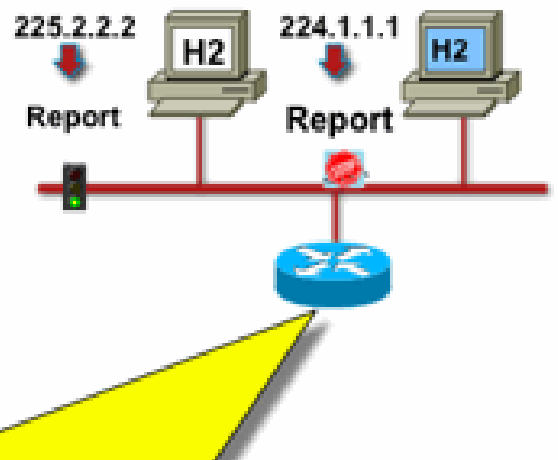
 **Opmerking:** dit type IGMP-filter kan worden gebruikt voor het ontvangen van ACL's of CoPP. In beide toepassingen moet het worden gecombineerd met filters voor ander verkeer dat wordt verwerkt, zoals routing en beheer van vliegtuigprotocollen.

Fig. 19: toegangscontrole voor hostontvanger



Als u verkeer naar een ontvanger wilt filteren, filtert u niet het dataplatform-verkeer, maar wel het Control plane-protocol IGMP. Aangezien IGMP een noodzakelijke voorwaarde is om multicast verkeer te ontvangen, zijn geen filters van het gegevensvliegtuig vereist.

In het bijzonder, kon u beperken welke multicast stroomontvangers kunnen toetreden (verbonden

aan de interface dat het bevel wordt gevormd). Gebruik in dit geval de opdracht `ip igmp access-group / ipv6 mld access-group`:

```
<#root>
```

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

Voor ASM-groepen, deze opdracht alleen filters gebaseerd op het doeladres. Het IP-bronadres in de ACL wordt vervolgens genegeerd. Voor SSM-groepen die IGMPv3 / MLDv2 gebruiken, filtert deze op bron- en bestemmings-IP.

Dit voorbeeld filtert een gegeven groep voor alle IGMP-luidsprekers:

```
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
```

Dit voorbeeld filtert specifieke IGMP-luidsprekers (vandaar specifieke multicast-ontvangers) voor een bepaalde groep:

```
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
```



Opmerking: voor ASM-groepen wordt de bron genegeerd.

---

## Toegangsbeheer

Toegangsbeheer levert een binair, ja of neen antwoord voor bepaalde stromen, onafhankelijk van de toestand van het netwerk. De toegangscontrole door contrast beperkt het aantal middelen dat een afzender/ontvanger kan gebruiken, veronderstellen zij de toegangscontrolemechanismen overgingen. Verschillende apparaten zijn beschikbaar om te helpen met toegangscontrole in een multicast omgeving.

### Globale en Per Interface IGMP-limieten

Bij de router die het dichtst bij geïnteresseerde multicast ontvangers staat, is er de mogelijkheid om het aantal IGMP-groepen te beperken die zich zowel wereldwijd als per interface aansluiten. U kunt de opdrachten voor de grenswaarde van ip igmp/ipv6-mld gebruiken:

```
<#root>
```

```
ip igmp limit
```

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

```
ipv6 mld limit
```

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

Aanbevolen wordt deze limiet altijd per interface en ook wereldwijd te configureren. In elk geval verwijst de grenswaarde naar het aantal ingangen in de IGMP-cache.

De volgende twee voorbeelden laten zien hoe deze opdracht kan worden gebruikt om het aantal groepen aan de rand van een breedbandnetwerk in woningen te beperken.

Voorbeeld 1 - Beperk ontvangen groepen tot alleen de SDR aankondigingen plus één ontvangen kanaal

Session Directory (SDR) fungeert als kanaalgids voor sommige multicastontvangers. Zie [RFC 2327](#) voor meer informatie.

Een gemeenschappelijke eis is het beperken van ontvangers om de SD-groep plus één kanaal te ontvangen. Deze voorbeeldconfiguratie kan worden gebruikt:

```
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
```

De toegangslijst in dit voorbeeld specificeert alleen de kanaalgids; de globale ip igmp limiet opdracht beperkt elke IGMP bron tot een enkel (1) kanaal, maar omvat niet de kanaalgids, die altijd kan worden ontvangen. Het interfacebevel treedt het globale bevel met voeten en laat twee (2) kanalen toe om, naast de kanaalgids, op deze interface worden ontvangen.

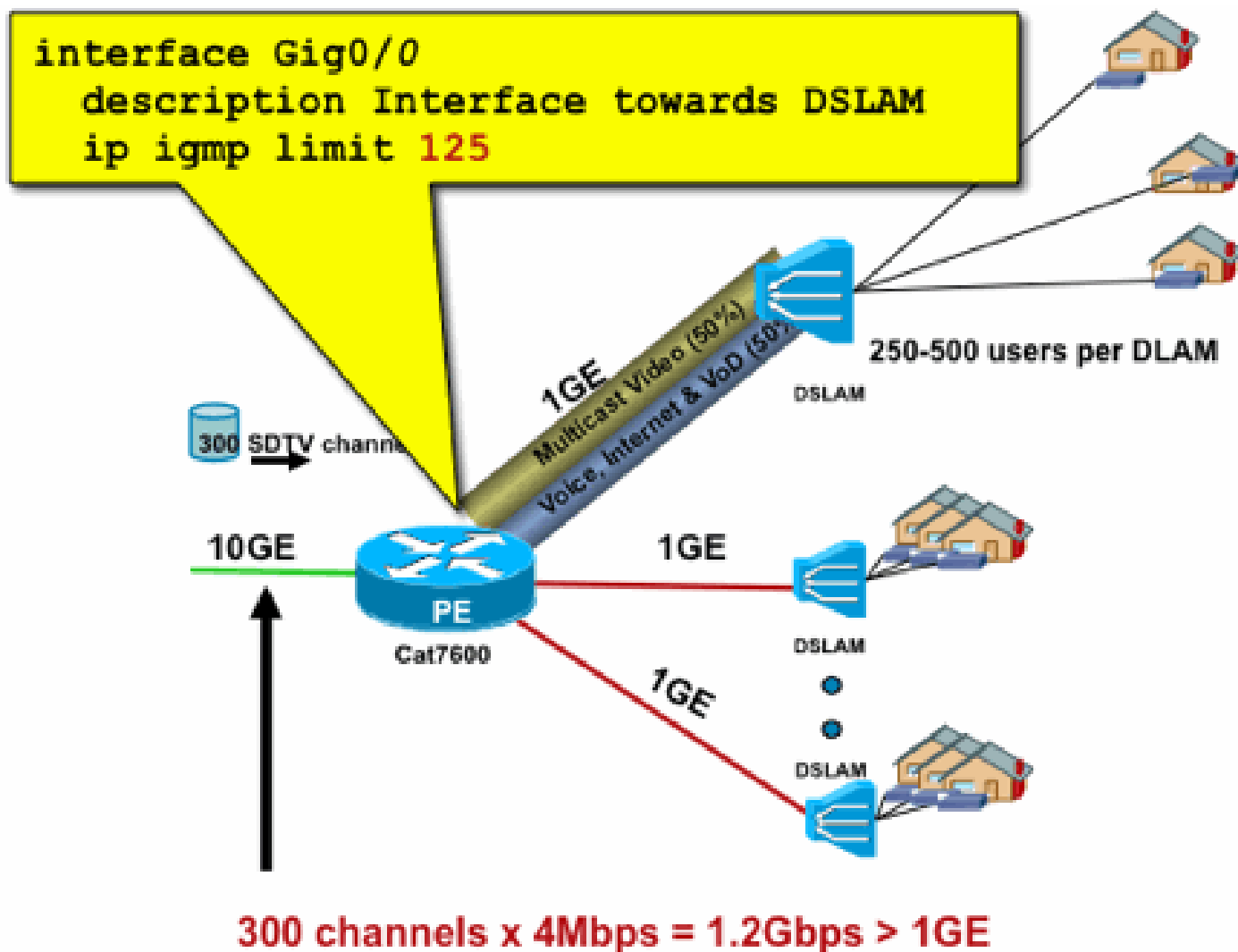
Voorbeeld 2 - Admission Control on Aggregation-DSLAM Link

Deze opdracht kan ook worden gebruikt om een vorm van bandbreedtetoegangscontrole te bieden. Als het bijvoorbeeld nodig was om 300 SDTV-kanalen te distribueren, die elk 4 Mbps zijn, en er een 1 Gbps link is naar de Digital-Subscriber-Line-Access-Multiplexer (DSLAM), kunt u een

beleidsbeslissing nemen om de tv-bandbreedte te beperken tot 500 Mbps en de rest voor internet en ander gebruik achter te laten. In dat geval kunt u de IGMP-statussen beperken tot 500 Mbps/4 Mbps = 125 IGMP-statussen.

Deze configuratie kan in dit geval worden gebruikt:

Fig 20 gebruik van IGMP-limieten per interface; toegangscontrole op Agg-DSLAM Link



## Routebeperkingen per interface

Het toestaan van de grenzen van de per-interfaceroutestaat is een genereuzere vorm van toelatingscontrole. Het beperkt niet alleen de IGMP- en PIM-status op een uitgaande interface, maar biedt ook een manier om de status van inkomende interfaces te beperken.

Gebruik de opdracht `ip multicast limit`:

```
<#root>
```

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

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

De status kan afzonderlijk worden beperkt op invoer- en uitvoerinterfaces. De direct aangesloten bronstatus kan ook worden beperkt met het gebruik van het sleutelwoord "verbonden". De voorbeelden illustreren het gebruik van deze opdracht:

#### Voorbeeld 1 - Uitgangstoegangscontrole op AGG-DSLAM Link

In dit voorbeeld zijn er 300 SD-tv-kanalen. Stel dat elk SD-kanaal 4 Mbps nodig heeft, met een totaal van niet meer dan 500 Mbps. Tot slot, ga er ook van uit dat er behoefte is aan ondersteuning van Basic-, Extended- en Premium-bundels. Voorbeeld van bandbreedte toewijzingen:

- 60%/300 Mbps basissnelheid
- 20%/100 Mbps uitgebreid
- 20%/100 Mbps premium

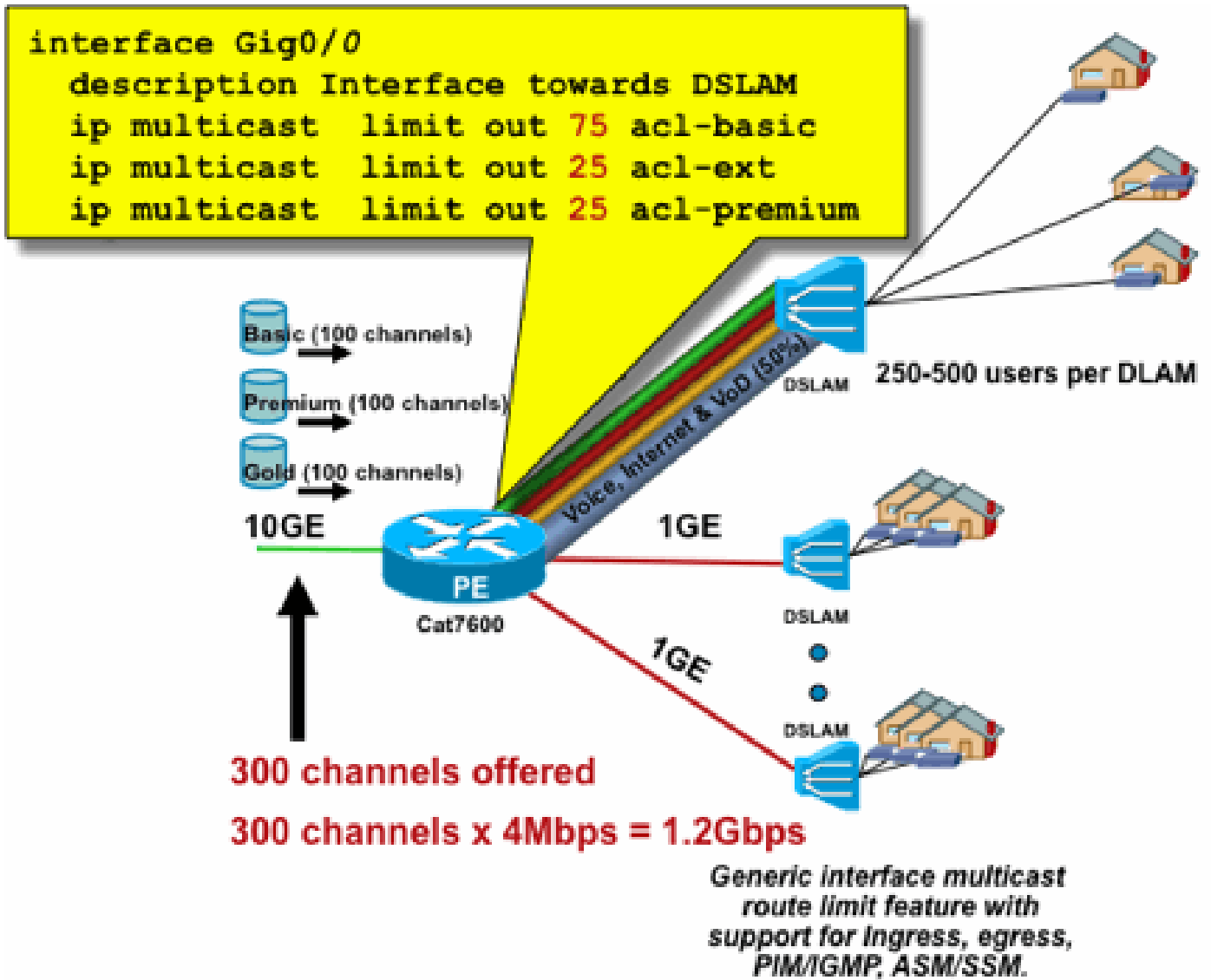
Gebruik vervolgens 4 Mbps per kanaal, beperk de DSLAM uplink tot:

- Basis 75 staten
- Uitgebreide 25 staten
- Premium 25 staten

Configureer de limiet op de uitgaande interface met de DSLAM vanaf de PEAgg:

Fig 21: Gebruik van per-interface-routebeperkingen; toegangscontrole op AGG-DSLAM Link





Voorbeeld 2 - Ingress Admission Control op AGG-DSLAM Link

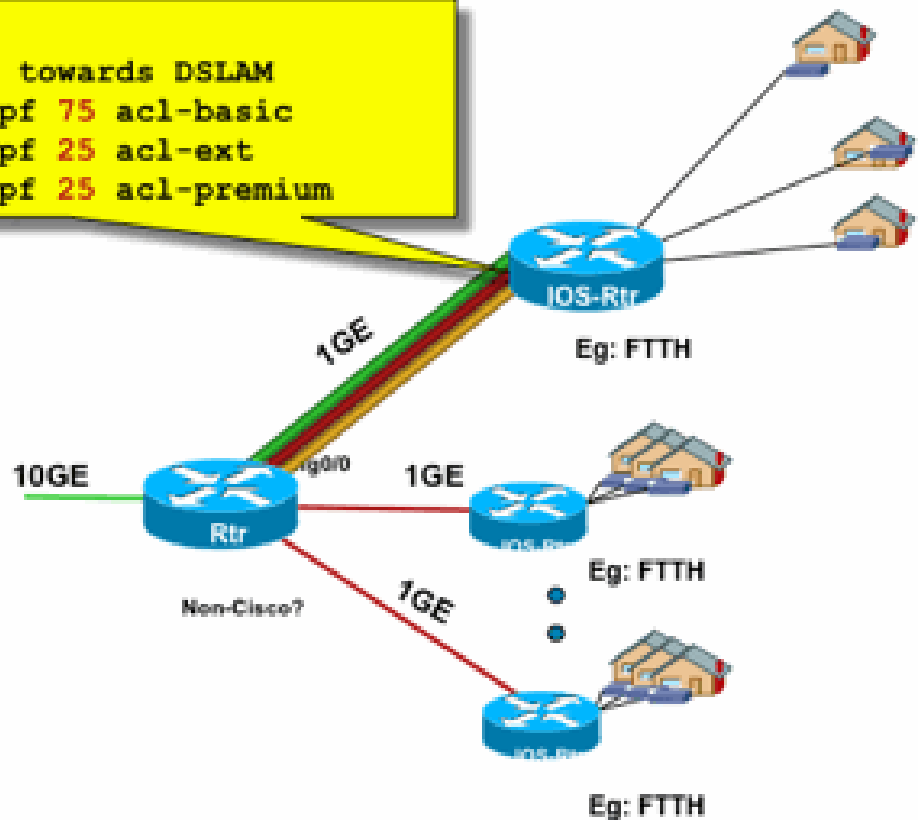
In plaats van de "uit"grens op de stroomopwaartse uitgaande interface van het apparaat, is het mogelijk om RPF grenzen op de stroomafwaartse interface van RPF van het apparaat te gebruiken. Dit heeft effectief hetzelfde resultaat als het vorige voorbeeld en kan handig zijn als het downstream-apparaat geen Cisco IOS-apparaat is.

Fig 22: Gebruik van per-interface-routebeperkingen; invoertoegangscontrole

```

interface Gig0/0
  description Interface towards DSLAM
  ip multicast limit rpf 75 acl-basic
  ip multicast limit rpf 25 acl-ext
  ip multicast limit rpf 25 acl-premium

```



### Voorbeeld 3 - Op bandbreedte gebaseerde limieten

U kunt een verdere onderverdeling van toegangsbandbreedte maken tussen meerdere contentproviders en elke contentprovider een redelijk deel van de bandbreedte in de uplink naar de DSLAM aanbieden. Gebruik in dat geval de opdracht kosten voor IP-multicast limieten:

```
<#root>
```

```
ip multicast limit cost
```

```
<ext-acl> <multiplier>
```

Met deze opdracht is het mogelijk om een "kosten" toe te schrijven (gebruik de waarde die in "multiplier" is gespecificeerd) aan alle toestanden die overeenkomen met de uitgebreide ACL in de IP multicast-limiet.

Deze opdracht is een globale opdracht en meerdere gelijktijdige kosten kunnen worden geconfigureerd.

In dit voorbeeld is het noodzakelijk om drie verschillende inhoudaanbieders met een eerlijke toegang tot elk in het netwerk te ondersteunen. Daarnaast is het in dit voorbeeld een vereiste om MPEG-stromen (Moving Picture Experts Group) van verschillende typen te ondersteunen:

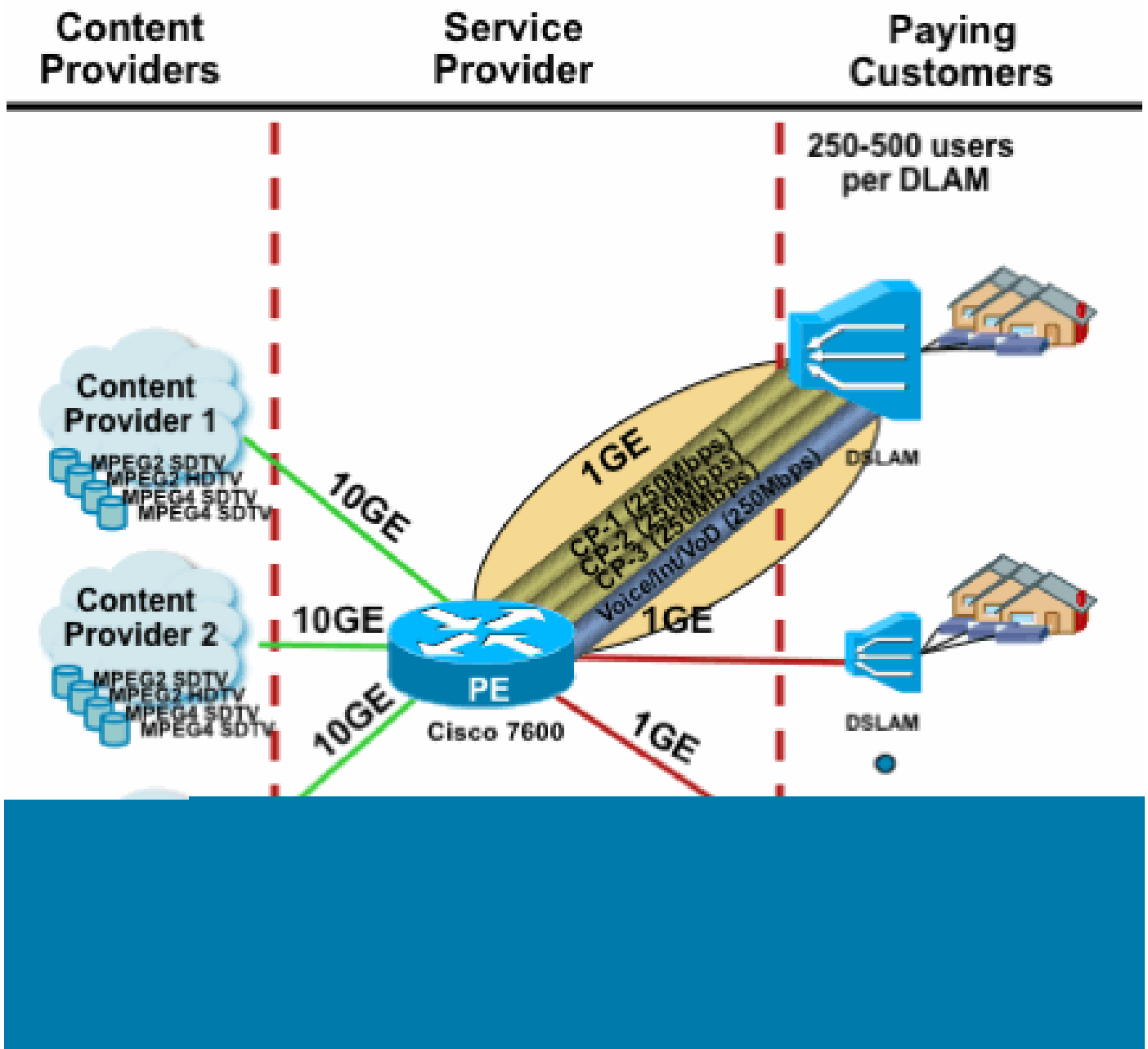
- MPEG2 SDTV: 4 Mbps
- MPEG2 HDTV: 18 Mbps
- MPEG4 SDTV: 1,6 Mbps

## MPEG4 HDTV: 6 Mbps

In dat geval kunt u bandbreedtekosten toewijzen aan elk stroomtype en de rest van de 750 Mbps delen tussen de drie contentproviders met deze configuratie:

```
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
```

Fig 23: Kostenfactor voor lidstaatlimieten per interface



## Multicast en IPSec

### Inleiding om VPN te kopen

Zoals met unicast, moet multicast verkeer ook soms worden beveiligd om vertrouwelijkheid of integriteitsbescherming te bieden. Er zijn twee belangrijke gebieden waarop dergelijke diensten vereist zouden kunnen zijn:

- Encryptie van multicast streams (bijvoorbeeld in bankapplicaties die vertrouwelijke gegevens streamen naar een grote set ontvangers die multicast gebruiken) - dit is gegevensvlak security.
- Encryptie van controlevliegtuig protocollen die multicast, OSPF of PIM gebruiken,

bijvoorbeeld - dit is de veiligheid van het controlevliegtuig.

IPsec als protocol [RFCs 6040, [7619](#), [4302](#), [4303](#), [5282](#)] is specifiek beperkt tot unicastverkeer (door RFC). Daar wordt een "security association" (SA) opgericht tussen twee unicast peers. Om IPsec op multicast verkeer toe te passen, is één optie om multicast verkeer binnen een GRE-tunnel in te kapselen en dan IPsec op de GRE-tunnel toe te passen, die unicast is. Een nieuwere benadering gebruikt één enkele veiligheidsvereniging die tussen alle leden van de groep wordt gevestigd. De Group Domain of Interpretation (GDOI) [RFC [6407](#)] definieert hoe dit wordt bereikt.

Gebaseerd op GDOI, heeft Cisco een technologie ontwikkeld die Group Encryption Transport (GET) VPN wordt genoemd. Deze technologie maakt gebruik van "Tunnel Mode with Address Preservation", zoals gedefinieerd in het document "Draft-ietf-msec-ipsec-extensions". In GET VPN wordt eerst een groepsbeveiligingsassociatie opgericht tussen alle leden van de groep. Vervolgens wordt het verkeer beveiligd, met ESP (ingekapselde security payload) of AH (authenticatieheader), die tunnelmodus met adresbehoud gebruikt.

Samenvattend, GET VPN kapselt een multicast pakket in dat de adresinformatie van de oorspronkelijke header gebruikt, en beschermt vervolgens het binnenste pakket met betrekking tot het groepsbeleid, met bijvoorbeeld een ESP.

Het voordeel van GET VPN is dat multicast verkeer helemaal niet wordt beïnvloed door de security inkapselingsmechanismen. De gerouteerde IP-headeradressen blijven hetzelfde als de oorspronkelijke IP-header. Multicastverkeer kan op dezelfde manier worden beveiligd met of zonder GET VPN.

Het beleid dat wordt toegepast op de GET VPN-knooppunten wordt centraal gedefinieerd op een Group Key Server en verdeeld over alle groepsknooppunten. Daarom hebben alle groepsknooppunten hetzelfde beleid en worden dezelfde beveiligingsinstellingen toegepast op groepsverkeer. Gelijkaardig aan standaardIPsec, bepaalt het crypto beleid welk type van verkeer op welke manier moet worden beschermd. Zo kan GET VPN voor verschillende doeleinden worden gebruikt.

## Gebruik GET VPN om multicast dataplane verkeer te versleutelen

Het cryptobeleid voor het hele netwerk wordt ingesteld op de groepssleutelserver en gedistribueerd naar de GET VPN-endpoints. Het beleid bevat het IPsec-beleid (IPsec-modus - hier: tunnelmodus met headerbehoud) en te gebruiken beveiligingsalgoritmen (bijvoorbeeld AES). Het bevat ook een beleid dat beschrijft welk verkeer kan worden beveiligd, zoals bepaald door ACL.

GET VPN kan worden gebruikt voor multicast en unicastverkeer. Een beleid om unicastverkeer te beveiligen kan worden gedefinieerd door een ACL:

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


Dit zou al verkeer met een bron IP van 10/8 en een bestemming IP 10/8 versleutelen. Al het andere verkeer, bijvoorbeeld verkeer van 10/8 naar een ander adres, zou worden genegeerd door GET VPN.

De toepassing van GET VPN voor multicast verkeer is technisch hetzelfde. Bijvoorbeeld, kan deze access-control ingang (ACE) worden gebruikt om verkeer van om het even welke bron aan respectieve multicast groepen te beveiligen:

```
permit ip any 239.192.0.0 0.0.255.255
```

Dit beleid past alle bronnen ("om het even welke") en alle multicastgroepen aan die met 239.192 beginnen. Het verkeer naar andere multicast groepen wordt niet beveiligd.

---

 **Opmerking:** er moet veel aandacht worden besteed aan de constructie van de crypto ACL. Het beheerverkeer, of het verkeer dat buiten het GET VPN-domein ontstaat maar binnenin eindigt (dat is verkeer dat slechts één crypto-eindpunt passeert), moet van het GDOI-beleid worden uitgesloten.

---

Vaak voorkomende fouten zijn:

- vergunning ip om het even welke 24.0.0.0 0.255.255.255: Dit codeert ook verkeer OSPF en ander verkeer van het controlevliegtuig, dat aan een peer router, bijvoorbeeld bestemd is.
- Het beheerverkeer is niet uitgesloten van het cryptobeleid, dat binnen het netwerk eindigt. Dit omvat ook het GDOI-verkeer zelf.

## Gebruik GET VPN om verkeer van besturingsplane te verifiëren

Het is over het algemeen een beste praktijk om verkeer van het controlevliegtuig, zoals het verpletteren van protocollen voor authentiek te verklaren, om ervoor te zorgen dat de berichten van een vertrouwde op peer komen. Dit is relatief eenvoudig voor controlevlakke protocollen die unicast, zoals BGP gebruiken. Echter, veel besturingsplane protocollen gebruiken multicast verkeer. De voorbeelden zijn OSPF, RIP, en PIM. Zie [IANA's IPv4 Multicast Address Space Registry](#) voor de volledige lijst.

Sommige van deze protocollen hebben ingebouwde verificatie, zoals Routing Information Protocol (RIP) of Enhanced Interior Group Routing Protocol (EIGRP), anderen vertrouwen op IPSec om deze verificatie te leveren (bijvoorbeeld OSPFv3, PIM). Voor het laatste geval, GET VPN biedt een schaalbare manier om deze protocollen te beveiligen. In de meeste gevallen is de vereiste de authenticatie van het protocolbericht, of met andere woorden, de controle dat een bericht door een vertrouwde op peer werd verzonden. GET VPN maakt echter ook versleuteling van dergelijke berichten mogelijk.


Om te beveiligen (gewoonlijk alleen authenticeren) van dergelijk verkeer van besturingsplane, moet het verkeer worden beschreven met een ACL en worden opgenomen in het GET VPN-

beleid. De details hangen van het protocol af dat moet worden beveiligd, waar de aandacht moet worden besteed aan of ACL verkeer omvat dat slechts een toegang KRIJGT VPN-knooppunt (dat is ingesloten), of ook een uitgangsknooppunt.

Er zijn twee fundamentele manieren om PIM-protocollen te beveiligen:

- Laat ip toe om het even welke 24.0.0.13 0.0.0.0: Dit is de multicast groep "Alle PIM Routers". Dit beveiligt echter geen unicast PIM-berichten
- Laat pim toe om het even welk: Dit beveiligt het PIM protocol, ongeacht of multicast of unicast wordt gebruikt

---

 Opmerking: de opdrachten worden als voorbeelden gegeven om een concept te helpen uitleggen. Het is bijvoorbeeld nodig om bepaalde PIM-protocollen uit te sluiten die gebruikt worden om PIM te bootstrap, zoals BSR of Auto-RP. Beide methoden hebben bepaalde voordelen en ongemakken die afhankelijk zijn van de inzet. Raadpleeg specifieke documentatie over het beveiligen van PIM met GET VPN voor meer informatie.

---

## Conclusies

Multicast wordt in netwerken steeds populairder. De opkomst van IPTV-diensten in breedbandnetwerken voor woningen en woningen en de verschuiving naar elektronische handelstoepassingen in veel van de financiële markten in de wereld zijn slechts twee voorbeelden van vereisten die multicast tot een absolute vereiste maken. Multicast wordt geleverd met een groot aantal verschillende uitdagingen op het gebied van configuratie, bediening en beheer. Een van de belangrijkste uitdagingen is veiligheid.

Dit document onderzoekt verschillende manieren waarop multicast kan worden beveiligd:

- Kijk eerst naar de algemene multicast controle- en dataplanes, een verklaring van hoe de verschillen van unicast nieuwe beveiligingsuitdagingen met zich meebrengen.
- Vervolgens is een onderzoek uitgevoerd naar de belangrijkste protocollen die in een multicastnetwerk worden aangetroffen, met name IGMP, PIM en MSDP. In elk geval werd een beschrijving van beveiligingsbedreigingen en aanbevolen best practices voor beperking tegen deze bedreigingen verstrekt.
- Bovendien zijn er een aantal specifieke voorbeelden van hoe multicast kan worden beveiligd in bepaalde specifieke toepassingen, zoals breedbandnetwerken met randapparatuur waarbij de bandbreedte kan worden beperkt in vergelijking met de hoeveelheid bandbreedte die specifieke videostromen zouden kunnen vereisen.
- Tot slot, GET VPN architectuur werd beschreven als een middel van geïntegreerde multicast met IPsec voor levering van beveiligde VPN's.

Met multicast beveiliging in gedachten, onthoud hoe het verschilt van unicast. Multicasttransmissie is gebaseerd op de aanmaak van dynamische status, multicast omvat dynamische pakketreplatie en multicast bouwt unidirectionele bomen in antwoord op PIM CONNECT / PRUNE-berichten. De beveiliging van deze hele omgeving omvat de kennis en implementatie van

een rijk framework van Cisco IOS-opdrachten. Deze opdrachten zijn grotendeels gecentreerd rond de bescherming van protocolbewerkingen, statussen (multicast) of policers die tegen pakketten zoals CoPP zijn geplaatst. Door het juiste gebruik van deze opdrachten is het mogelijk om een robuuste beveiligde service voor IP-multicast te bieden.

Kort samengevat worden in dit artikel meerdere benaderingen gepromoot en beschreven:

1. Wijdverbreid gebruik van SSM - dit is de meest eenvoudige PIM-modus die ook het gebruik van (S,G) doorsturen mogelijk maakt.
2. Als ASM-diensten nodig zijn, zorg ervoor dat een robuuste service kan worden geleverd - het gebruik van statisch gedefinieerde RP's biedt een veiliger controlevlak dan dynamische RP-aankondigingen. Auto-RP en BSR zijn flexibeler
3. Als PIM-SM is ingeschakeld, kijk dan naar gebieden die bijzonder kwetsbaar zijn, zoals de registertunnel naar de RP, en zorg ervoor dat de DR altijd goed beschermd is. CoPP is zeer behulpzaam op deze gebieden.
4. Als er interdomainASM-services nodig zijn, overweeg dan of BiDir PIM kan worden geïmplementeerd.
5. Gebruik wereldwijde limieten voor de route-/igmp-status - begrijp de mogelijkheden van uw platform samen met de verwachte maximale hoeveelheid status die u onder normale omstandigheden en in het ergste geval nodig hebt. Configureer de limieten binnen de mogelijkheden van uw platform die uw netwerk in staat stellen om binnen de maximale limieten te werken.
6. Fundamentele filters - rACL/CoPP en infrastructuur ACLs, die PIM bij de toegangslaag blokkeert

IP Multicast is een opwindend en schaalbaar middel om een scala aan toepassingservices te leveren. Net als unicast moet het worden beveiligd op verschillende gebieden. Dit artikel bevat de basisbouwstenen die kunnen worden gebruikt om een IP-multicast netwerk te beveiligen.

## Gerelateerde informatie

- [Richtlijnen voor IP-multicast adrestoewijzing voor ondernemingen](#)
- [IPv4 IGMP-filters configureren](#)
- [Groep versleuteld transport via VPN](#)



## Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.