



Cisco Expo
2008

Techtorial Day
SP techtorial

Multicast security
Multicast QoS



Klaudia Bakšová
Systems Engineer, Cisco Systems

Enable Your Network
Empower Your Business

Agenda

- **Multicast Security**
 - **Control Plane Security**
 - **Access Control**
- **Multicast Quality of Service**
 - **Considerations and recommendations**



Control Plane Security



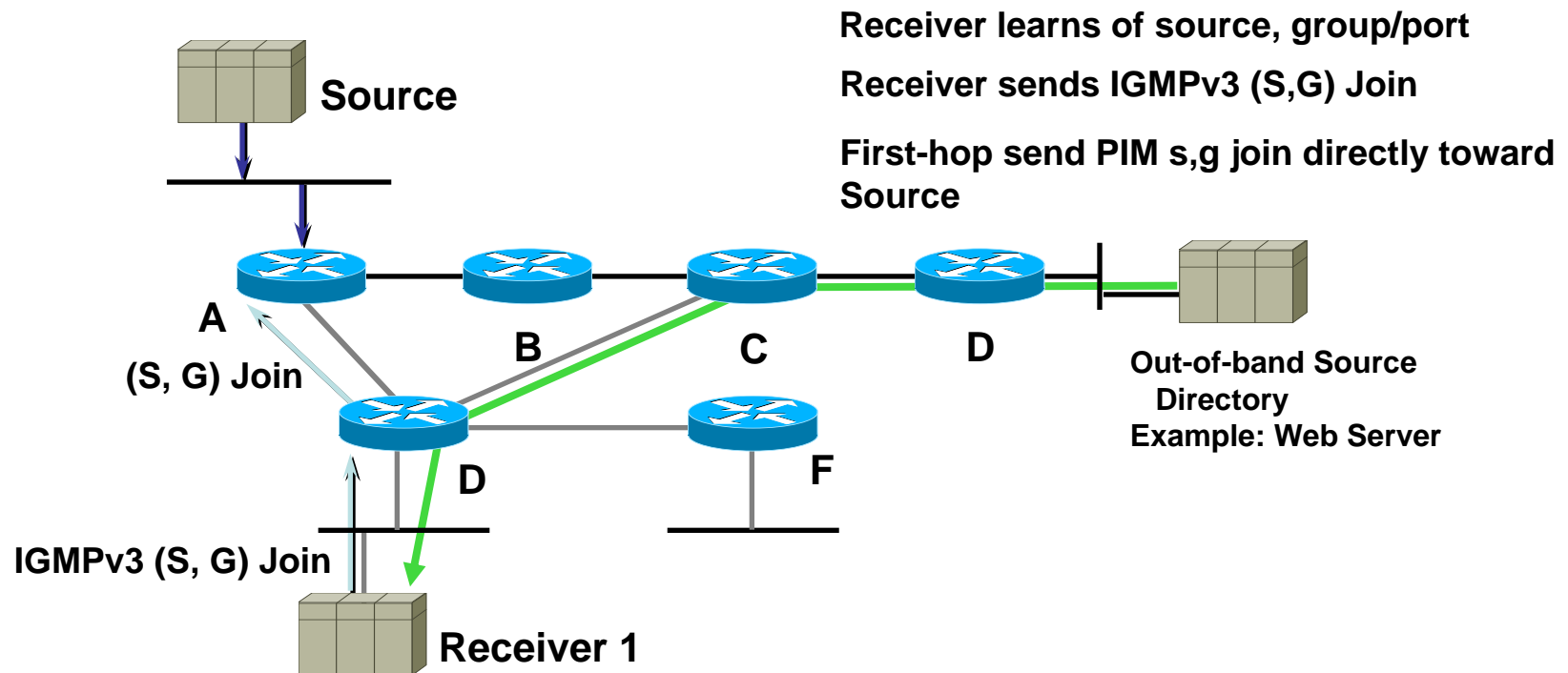
Control Plane Security

- Basis of CPS – routing protocols for mcast traffic
 - Interdomain – MSDP / SSM
 - Intradomain – PIM (DM,SM,Bidir) / IGMP
- Control plane filtering
- Primarily to protect against spoofing
 - Spoof function (RP, DR, BSR, MA, MSDP-peer)
 - DoS network, participants
- IGMP/PIM
 - Understand different packet types used by protocols
 - Understand type of attacks possible
 - Explain protocol specific filtering available
- Filtering for other protocols
- MSDP authentication

Source Specific Multicast

- Assume a One-to-Any Multicast Model
 - Example: Video/Audio broadcasts, Stock Market data
- Why does ASM need a Shared Tree?
 - So that hosts and 1st hop routers can learn who the active source is for the group - Source Discovery
- What if this was already known?
 - Hosts could use IGMPv3 to signal exactly which (S,G) SPT to join
 - The Shared Tree & RP wouldn't be necessary
 - Different sources could share the same Group address and not interfere with each other
- Result: Source Specific Multicast (SSM)
- IGMPv3 for Source Filtering
- *RFC 3569 An Overview of Source-Specific Multicast (SSM)*

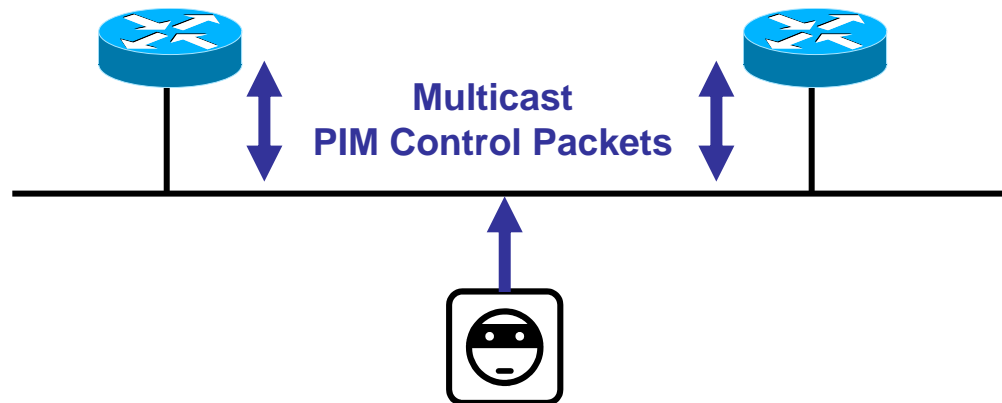
PIM Source Specific Mode



- Inhibition on DDoS attacks from unauthorized/rogue sources without the use of filters
- Explicit Subscription via IGMPv3

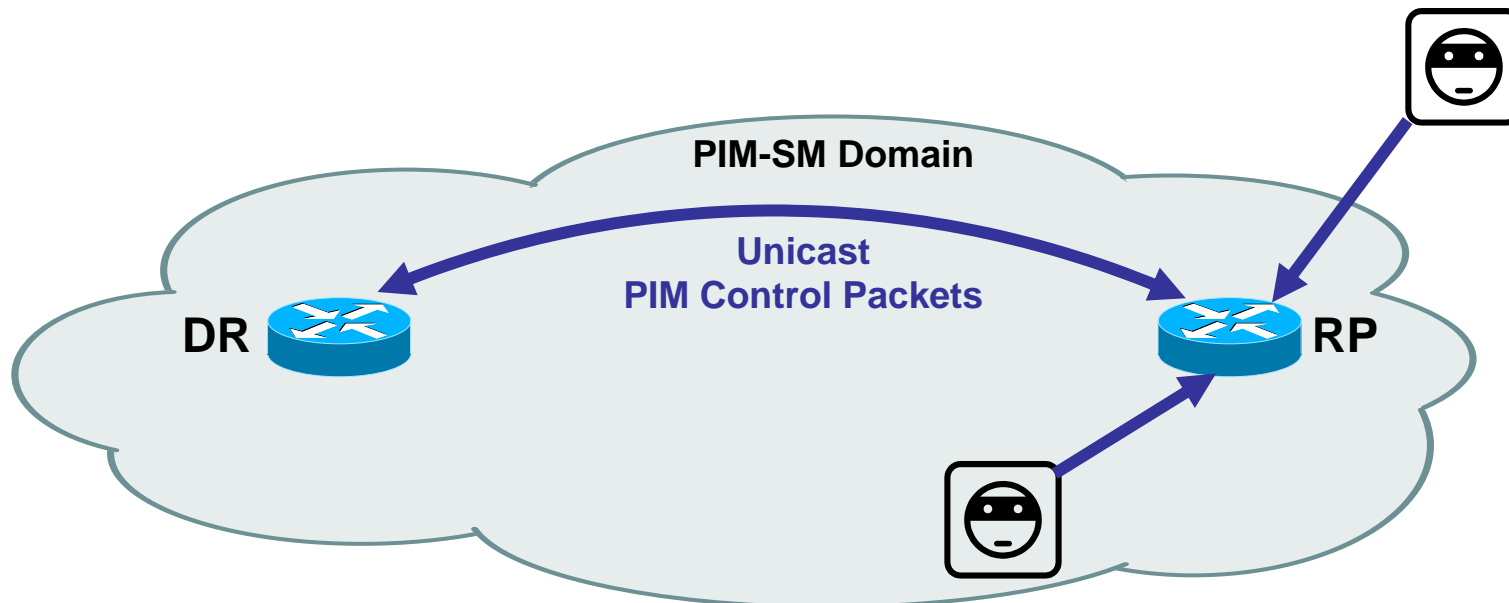
PIM Packets – Multicast

- Multicast PIM Control Packets :
 - Hello, Join/Prune, Assert, Bootstrap, DF-elect
 - All are link local multicast (TTL=1)
 - All are multicast to All-PIM-Routers (224.0.0.13)
- Attacks must originate on the same subnet
 - Forged Join/Prune, Hello, Assert packet



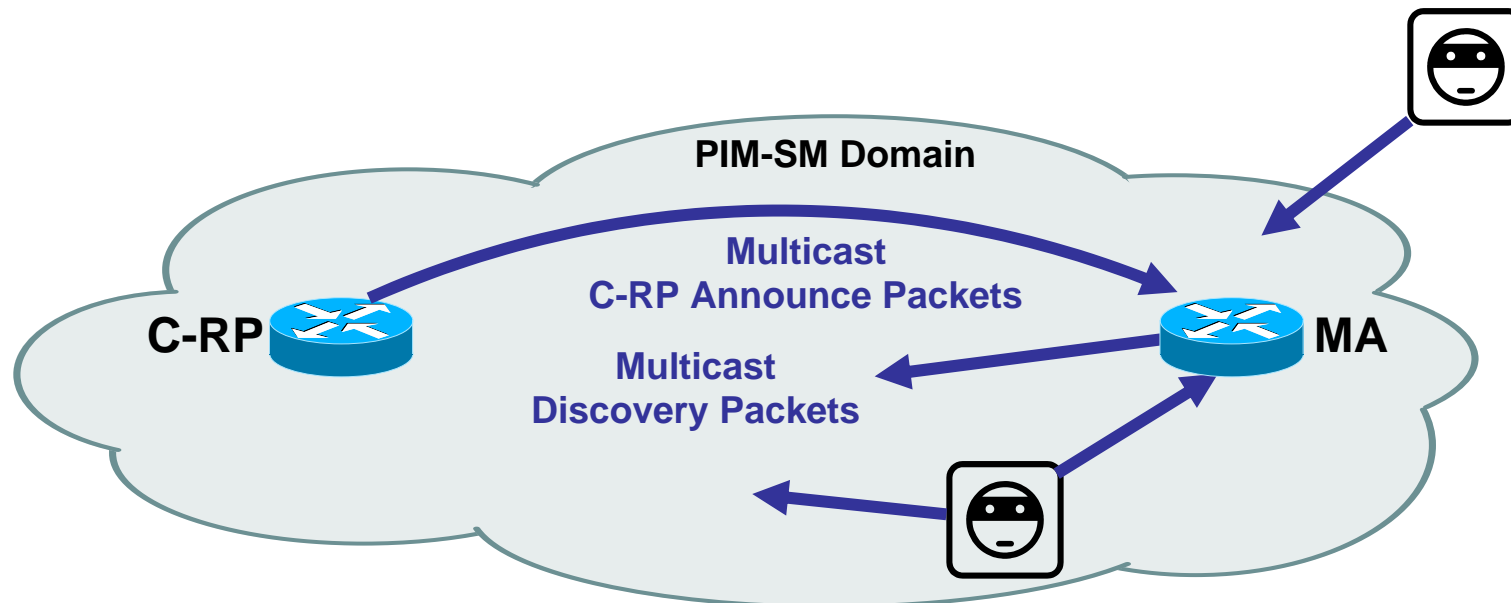
PIM Packets – Unicast

- Unicast PIM Control Packets :
 - Register: Unicast from DR to RP.
 - Register-Stop: Unicast from RP to DR.
 - C-RP-Advertisement: Unicast from C-RP to BSR.
- Attacks can originate from anywhere!



PIM Packets – Auto-RP

- IOS: AutoRP/BSR always enabled, non-configurable
- Auto-RP PIM Control Packets :
 - **C-RP-Announce**: Multicast (224.0.1.39) to all MA's.
 - **Discovery**: Multicast (224.0.1.40) to all Routers.
 - *Normally Dense mode flooded!*
- Attacks can originate from anywhere!

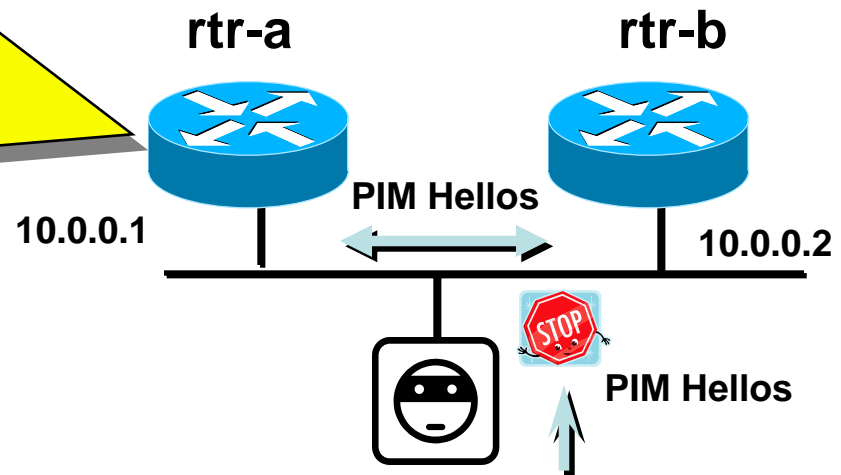


PIM Neighbor Control

```
ip multicast-routing
ip pim sparse-mode
ip multicast-routing

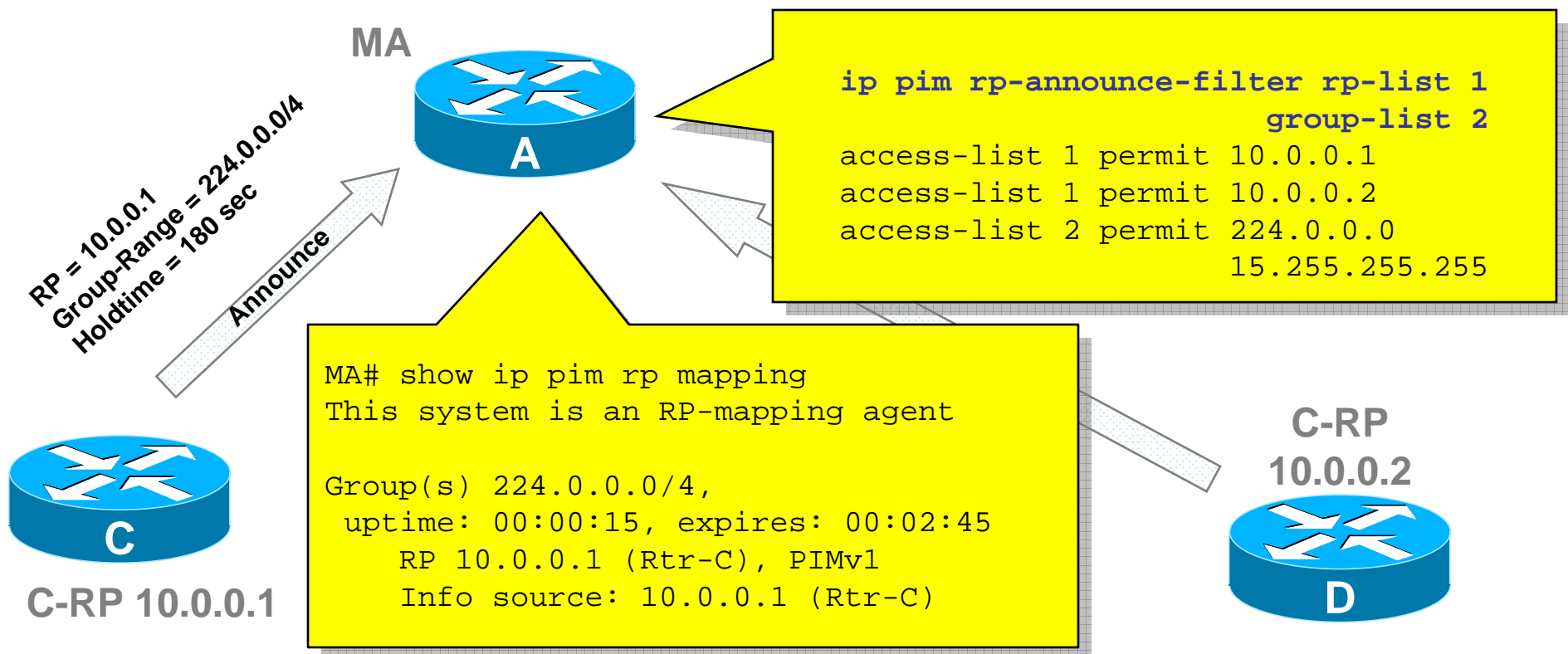
access-list 1 permit 10.0.0.2
Access-list 1 deny any

Interface e0
  ip pim sparse-mode
  ip pim neighbor-filter 1
```



- Must receive Hellos to establish PIM neighbor
 - DR election, failover
 - Accept / Send PIM Join/Prune/Assert
- Use ip pim neighbor filter to inhibit neighbors
 - Filters effectively all PIM packets from non-allowed sources
 - Hellos, J/P, BSR, ... !

AutoRP Control RP Announce Filter

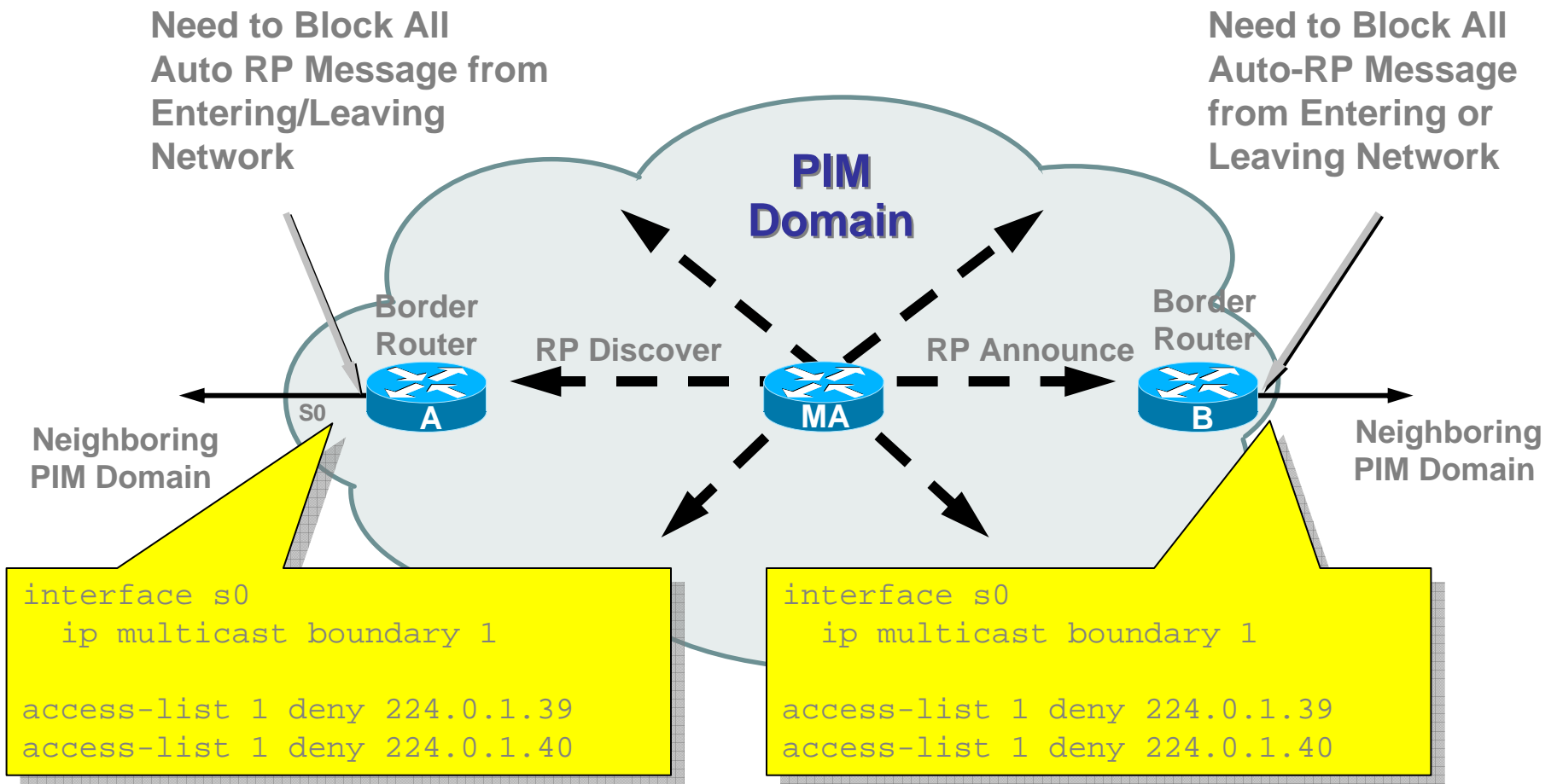


- **ip pim rp-announce-filter**

- Configure on MA which router (IP-addr) is accepted as C-RP for which group ranges / group-mode

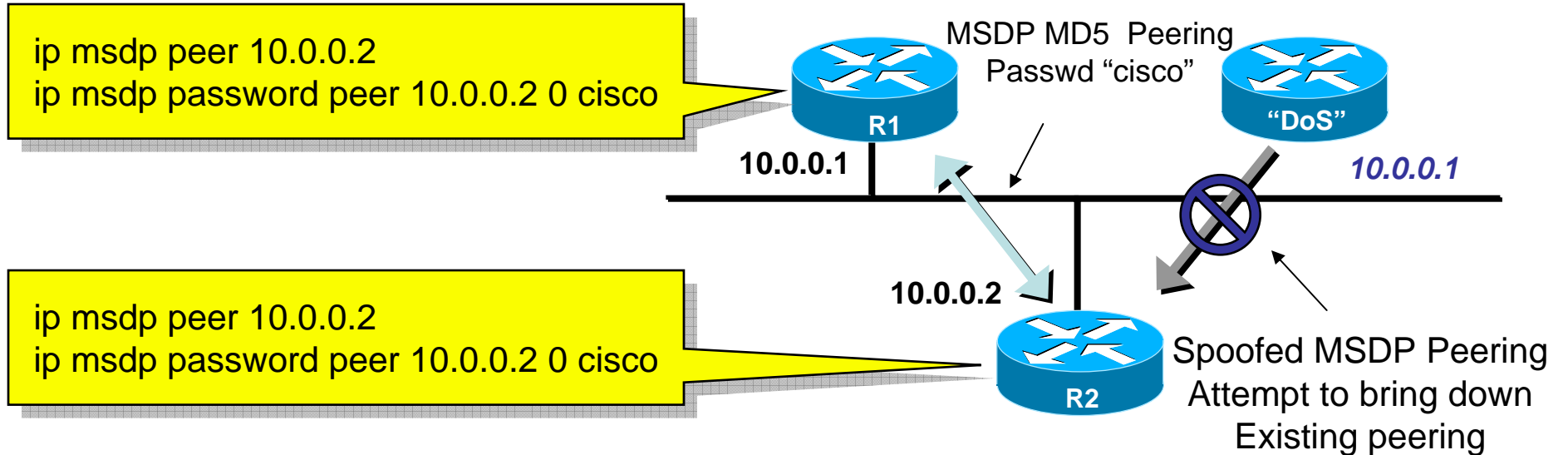
Auto-RP Control

Constrain Auto-RP Messages



- AutoRP packets:
 - 224.0.1.39 (RP-announce), 224.0.1.40 (RP-discover)

MSDP MD5 Password Authentication



- Protect MSDP peering against spoofed packets
 - Protects against spoofed sourced packets
 - Partial protect against man-in-middle
- Uses RFC2385 TCP authentication header
 - Defined for BGP
 - Actually independent of BGP

Access Control



Access Networks

Protection Against Attacks

- Attacks by hosts (multicast)
 - PIM Hellos – become DR – no traffic forwarded to LAN
 - Same applies to DF-election packets for Bidir-PIM
 - PIM joins – receive traffic (should use IGMP / filtered)
 - AutoRP RP-discovery or BSR bootstrap
 - Announce fake RP, bring down SM/Bidir service
- Attacks by hosts (unicast)
 - Send register/register-stop
 - Inject fake traffic
 - BSR announce packets – announce fake RP
- **Hosts should never do PIM !**

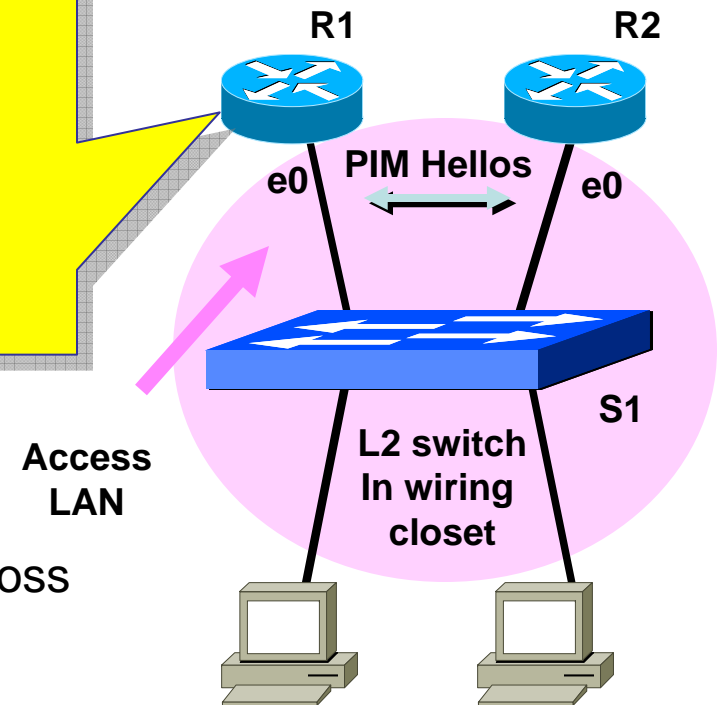
L3/L2 redundant Access Networks (1)

Protection Against Attacks

```
access-list 1 deny 224.0.1.39
access-list 1 deny 224.0.1.40

access-list 2 permit <R2>

interface e0
  ip pim sparse-mode
  ip pim neighbor-filter 2 ! Only allow R2
  ip pim bsr-border ! No BSR
  ip multicast boundary 1 ! No autorp
```



- Most common case ?
- Most complex to secure:
 - R1 and R2 need to exchange PIM-Hello across access LAN.
- Result: need to filter most control plane packets (unwanted sent from hosts), but still allow PIM Hellos
- *No simple/safe solution until PIM Hellos can be authenticated*

Secure PIM Control Traffic with IPSec Strategy/Example

- Encrypt/Authenticate PIM Packets
 - Crypto map for 224.0.0.13 (PIM Control Messages)
 - Hop-by-hop encryption/decryption of PIM msgs
 - Does not include PIM-SM registering!
(would require normal IPsec setup)
 - Use either IPSec options
 - Hash Functions: MD5, SHA1
 - Security Protocols: Authentication Header(AH), Encapsulating Security Payload (ESP)
 - Encryption Algorithms: DES, 3DES, AES
 - Recommended IPSec Mode: Transport
 - Recommended Key method: Manual
 - IPSec AH recommended in PIM IETF drafts

Secure PIM Control Traffic Example

```
access-list 106 permit ip 0.0.0.0 255.255.255.255 host  
  224.0.0.13
```

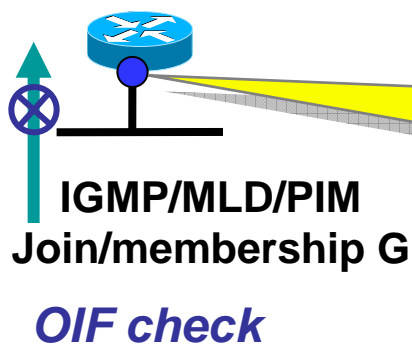
```
crypto ipsec transform-set pimts ah-sha-hmac  
  mode transport
```

```
crypto map pim-crypto 10 ipsec-manual  
  set peer 224.0.0.13  
  set session-key inbound ah 404 bcbcbcbcbcbcaaaa  
  set session-key outbound ah 404 bcbcbcbcbcbcaaaa  
  set transform-set pimts  
  match address 106
```

```
interface Ethernet0/0  
  crypto map pim-crypto
```

Interface / Protocol Level Access Control

Filtering Rules (1)



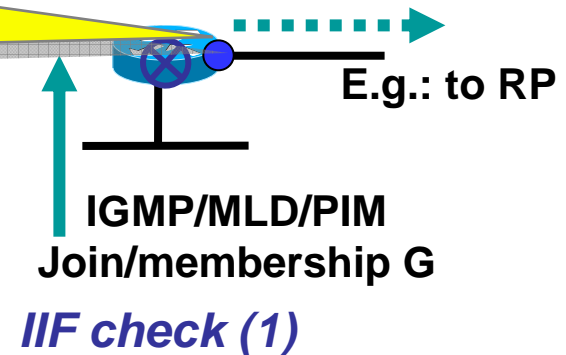
```
Interface ethernet 1
ip multicast boundary deny-groups      ! either
ip multicast boundary deny-states out  ! or
```

- OIF (“out”) check:
 - Router receives IGMP membership or PIM join on interface where boundary is configured
 - Multicast boundary (“out”) checks G or (S,G) of this ‘join’
 - If permitted, normal processing continues
 - If denied: ‘join’ is ignored.
No state created in PIM/mroute/IGMP tables for it.

Interface / Protocol Level Access Control

Filtering Rules (2)

```
Interface ethernet 0
 ip multicast boundary deny-groups      ! either
 ip multicast boundary deny-states in  ! or
```

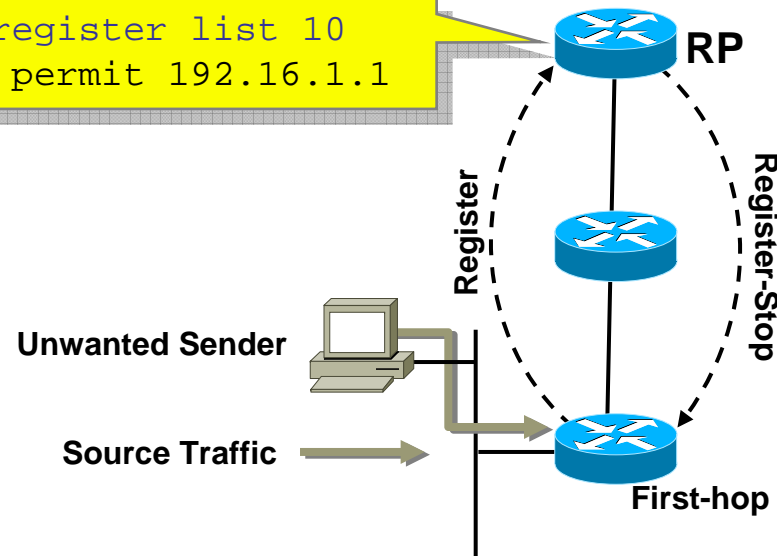


- IIF (“in”) check (1):
 - Router receives a ‘join’ on an interface.
 - Multicast boundary in the receiving interface passed the ‘join’
 - State ((*,G) and/or (S,G) is created if not already existing.
 - PIM selects RPF-interface for the state.
 - Multicast boundary on RPF interface examines (G or (S,G) of state
 - If permitted – normal processing continues.
 - If denied:
 - OIF entry for join is NOT CREATED.
NO OIF entries for this state are created.
Result: router will never send PIM join for this state (OIF empty)

PIM-SM Source Control

ip pim accept-register

```
ip pim accept-register list 10  
access-list 10 permit 192.16.1.1
```



- Unwanted source traffic hits first-hop router
- First-hop router creates (S,G) state and sends Register
- RP rejects Register, sends back a Register-Stop.

- RP-based (central) access control for (S,G) in PIM-SM
- Extended-Acl: which source can send to which group
- Imperfect:
 - (S,G) state on FHR still created
 - (S,G) traffic still to local and downstream rcvrs.

QoS



QoS Architecture

- **Video QoS Requirements**

Allowed Drop Rate $\approx 10^{-6}$

Allowed Jitter ≈ 200 Msec

- **Scheduling video traffic using DiffServ AF PHB** – guaranteed max jitter and drop rate per packet class

- **Broadcast B/W is Typically < On Demand in Dist Network**

- **Broadcast B/W Based on # Channels**

300 MPEG-2 Std Def Channels ≈ 1 Gigabit

- **On Demand B/W Based on # Subscribers**

20,000 Video Subscribers * 10% Peak ≈ 7.5 Gigabit

- **Broadcast Availability Requirements Higher Than On Demand**

- **Drop VoD First in Event of Link Congestion**

Must Drop Subset of all VoD Flows

Broadcast / VoD QoS Recommendations

- **Use DiffServ AF PHB for Video**

Carry Broadcast / VoD in Same Queue

Use Queue Thresholds to Drop VoD Before Broadcast

- **DiffServ Markings**

Broadcast = AF41; VoD = AF42

- **Queue Thresholds**

Use Separate Queue Thresholds for Broadcast, VoD 1

VoD Threshold (Bytes) == Link Speed * 20 msec * VoD1 Link Util

➔ 20 msec of buffer for average video flow

➔ For 1 GigE and 70% Video Link Util

Video Queue Size = 1 GigE * 20 msec * .7 = 1.75 Mbytes

Broadcast Threshold == Queue Size



CISCO