Multicast Security

Piotr Wojciechowski (CCIE #25543)

About me

- Senior Network Engineer MSO at VeriFone Inc.
- Previously Network Solutions Architect at one of top polish IT integrators
- CCIE #25543 (Routing & Switching)
- Blogger – http://ccieplayground.wordpress.com
- Administrator of CCIE.PL board
  - The biggest Cisco community in Europe
  - Over 6100 users
  - 3 admin, 7 moderators
  - 48 polish CCIEs as members, 20 of them actively posting
  - About 150 new topics per month
  - About 1000 posts per month
  - English section available!

Agenda

- Main security issues
- Securing the edge of multicast network
- Trusted and secure sender/receiver
- Dense Mode Fallback problems
- Tunneled multicasts
- Admission control

Main Security Issues

Main security issues

- Why to control?
  - Access control – permit specified sources/destinations
  - Policies
  - Admission – can we transport multicast?
- Where to deploy security?
  - Local router/switch
  - policy-server

Main security issues

- What we have to protect?
  - Content and services
  - Device control-plane
  - Data plane protection – saturation of network links
- How we can protect?
  - Packet filtering
  - Registration filtering
  - State creation
  - Encryption

Main security issues

- Threat overview
  - Threats against confidentiality
    - Must multicast applications does not encrypt data – traffic can be eavesdropped
  - Threats against traffic integrity
    - Without application-level security or network-based security multicast traffic is open to being modified in transit
  - Threats against network integrity
    - Unauthorized senders, receivers, or compromised network elements can access the multicast network, send and receive traffic without authorization or overload network resources.
  - Threats against availability
    - There are a number of denial of service attack possibilities that can make resources unavailable to legitimate users

Main security issues

- Threats from the sender side
  - Layer 2 attacks – not multicast specific but still dangerous
  - Masquerading – sender can pretend to be another sender (ie. Source IP Spoofing)
  - Theft of service – without proper control it is possible to use the multicast service illegitimately from the sender side

Main security issues

- Threats from the sender side
  - Attacks with multicast traffic
    - Network saturation
    - Multicast state attack – to many states created on router
    - Attempt to become PIM DF on LAN segment
    - Fake RP announcement to disrupt PIM-SM/BiDir service – spoofing AutoRP or BSR
    - Unauthorized sender
    - Attacks against control-plane using multicast traffic (ie. OSPF multicast traffic)

Main security issues

- Threats from the receiver side
  - Similar attacks as for sender side
  - Layer2 attacks
  - Masquerading and thief of data
  - Attack vector usually an IGMP

Main security issues

- **Threats against a Rendezvous Point and BSR**
  - PIM-SM RP and PIM-BSRs are critical points in multicast network
  - Vulnerable to all forms of attacks described before
  - Additionally:
    - PIM Unicast attacks with source IP Spoofing
    - DoS attacks by sending PIM Register and PIM Register-stop messages

Securing Multicast Edge

Securing Multicast Edge

- Multicast PIM Control Packets:
  - Hello, Join/Prune, Assert etc.
  - All messages are link-local (TTL=1)
  - Destination All-PIM-Routers (224.0.0.13)
  - Attack must originate on the same subnet
- Unicast PIM Control Packets:
  - Register, Register-Stop, C-RP-Advertisement
  - Attacks can originate from anywhere

Securing Multicast Edge
Filtering PIM Messages

- Filter all PIM packets from untrusted sources
  - Router must receive PIM Hellos to establish relation
  - PIM packets can be filtered
  - It's not spoofing-proof

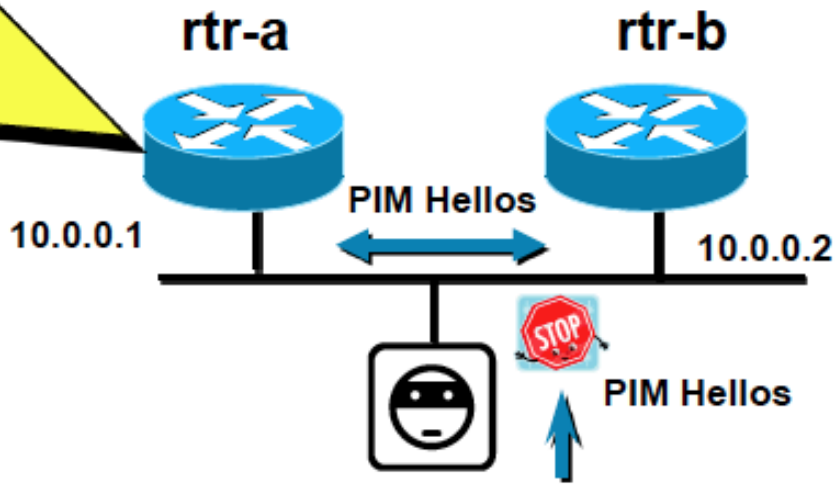
Securing Multicast Edge
Filtering PIM Messages

- Filter all PIM packets from untrusted sources

```
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
```



Securing Multicast Edge
Prevent RP Mapping

- RP Announce Filter
  - Configure it on Mapping Agent
  - Specify which IP addresses are accepted as RP Candidates for which groups.

```
ip pim rp-announce-filter rp-list RP group-list MGROUPS
!
ip access-list standard MGROUPS
 permit 224.0.0.0 15.255.255.255
ip access-list standard RP
 permit 10.0.0.2
 permit 10.0.0.3
```

For what groups MA should accept C-RP

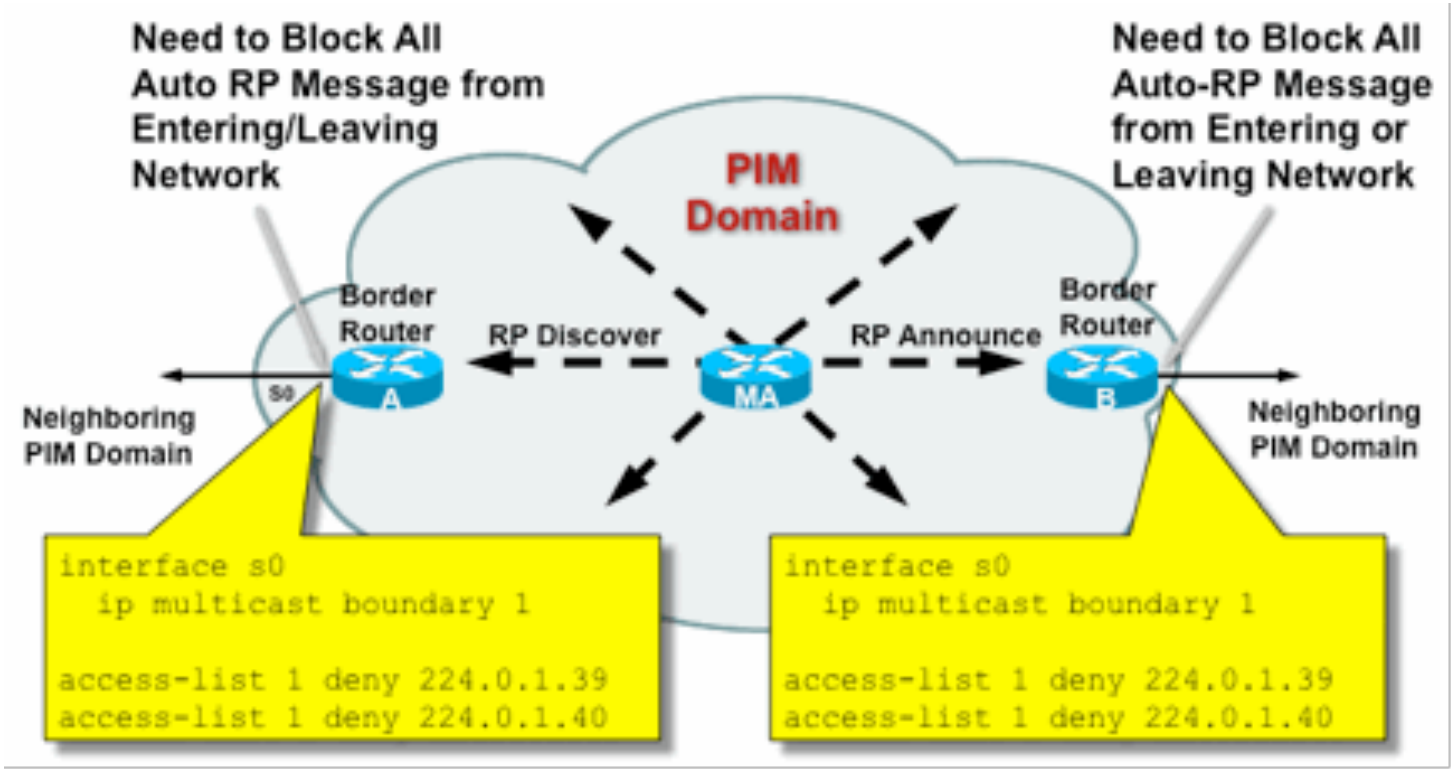
List of allowed C-RP's

Securing Multicast Edge
Multicast network boundary

- Multicast boundary
  - Administratively scoped boundary on an interface in order to filter source traffic coming into the interface
  - Prevent mroute states from being created on the interface
  - Enables reuse of the same multicast group address in different administrative domains
  - Filter data and control plane traffic including IGMP, PIM, and Auto-RP messages. PIM Register messages are sent using unicast and will not be filtered.

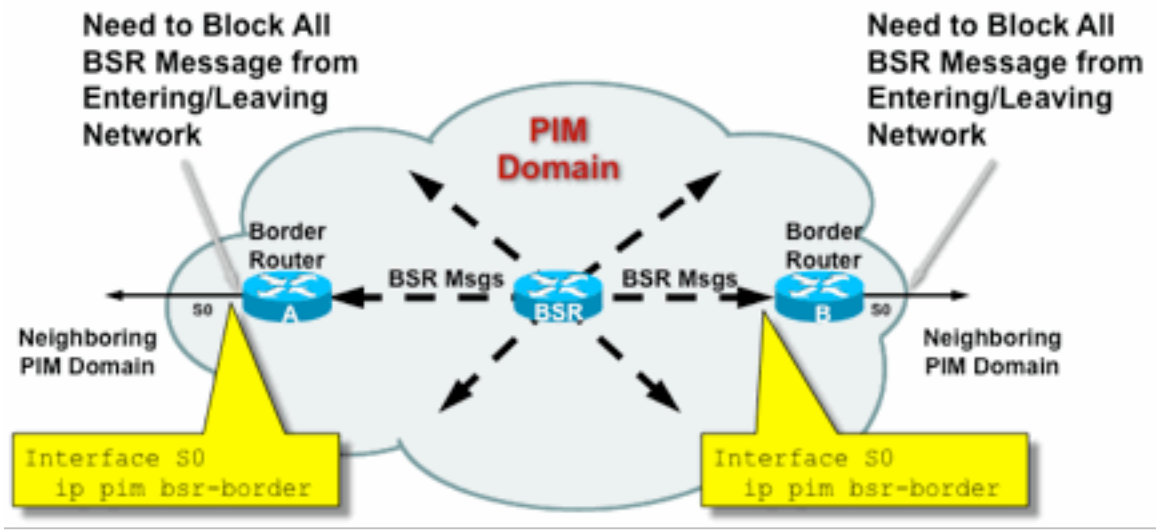
Securing Multicast Edge
Multicast network boundary

- Multicast boundary
  - AutoRP Filtering



Securing Multicast Edge
Multicast network boundary

- BSR Border
  - BSR message filtering applied to interface
  - Protects from both sending and receiving BSR messages
  - Does not set up multicast boundary



Securing Multicast Edge
PIM Passive

- PIM Passive Interface
  - No PIM messages are sent or received
  - Router does not join to 224.0.0.13
  - No AutoRP or BSR messages are sent
  - Unicast PIM Packets unaffected
  - Configure only on non-redundant segments!

```
interface Ethernet0/0
 ip address 10.0.12.1 255.255.255.0
 ip pim passive
```

Securing Multicast Edge
Multicast group filtering

- Multicast groups filtering
  - New and nice way to filter all multicast traffic for particular groups
  - Introduced in IOS 12.2(33)SXI, 12.2(33)SRE, 15.0(1)M; IOS XR 2.6
  - Disables multicast protocol actions and traffic forwarding for unauthorized groups or channels for all interfaces on the router
  - No IGMP/MLD cache entries, PIM, MRIB/MFIB state are ever created for these group ranges and all data packets are immediately dropped

Securing Multicast Edge
Multicast group filtering

- Multicast groups filtering
  - VRF aware
  - Access-list that defines the multicast groups or channels to be permitted or denied globally
    - Standard ACL for groups
    - Extended ACL for (S,G)
  - AutoRP have to be explicitly permitted, otherwise it would be filtered

```
ip multicast group-range 1
!
access-list 1 permit 224.0.1.39 0.0.0.0
access-list 1 permit 224.0.1.40 0.0.0.0
access-list 1 permit 239.0.0.0 0.255.255.255
```

Trusted and secure sender/receiver

Trusted and secure sender/receiver *ACL on the edge*

- Many multicast security issues originating at the sender can be mitigated with appropriate unicast security mechanisms
  - Source address spoofing protection (uRPF and ACL with IP Source Guard for the access layer)
  - Infrastructure ACL

```
interface GigabitEthernet0/0
 ip access-group permit_mcast

ip access-list extended permit_mcast
 permit 10.0.0.0 0.0.0.255 239.0.0.0 0.127.255.255
 deny ip any 224.0.0.0 15.255.255.255 log
 permit ip any any
```

Trusted and secure sender/receiver *ACL on the edge*

- Advantages of ACLs:
  - Done in hardware on most platforms
  - Filters before multicast routing occurs so no states are created if denied
  - Best for ingress filtering
  - Search documentation for best practice examples

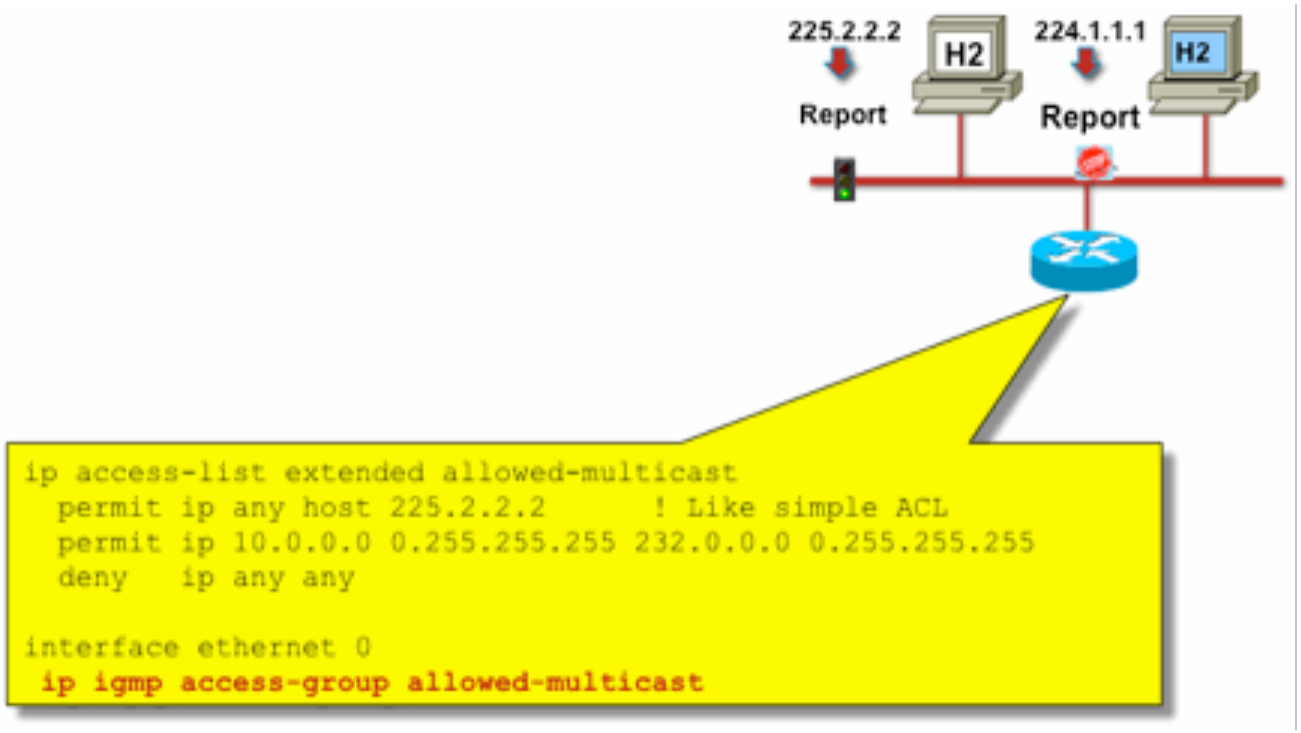
TRUSTED AND SECURE SENDER/RECEIVER *ACL ON THE EDGE*

```
ip access-list extended igmp-control
 …
 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 15.255.255.255 host-query    ! IGMPv1/v2/v3 queries
 permit igmp any 224.0.0.0 15.255.255.255 host-report   ! IGMPv1/v2 reports
 permit igmp any 224.0.0.0 15.255.255.255 7             ! IGMPv2 leave messages
 deny igmp any any                    ! Implicitly deny unicast IGMP here!
…
permit ip any any                     ! Permit other packets

interface ethernet 0
 ip access-group igmp-control in
```

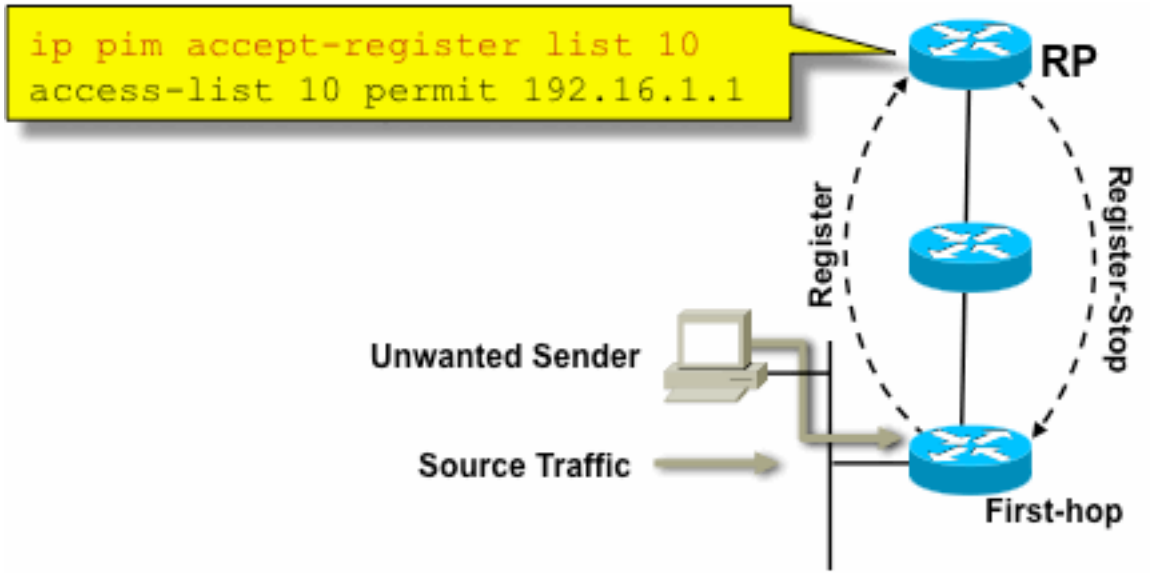
Trusted and secure sender/receiver *ACL on the edge*

- IGMP Filtering
  - Controls entries into IGMP cache
  - Extended ACL – you know how to do it!



Trusted and secure sender/receiver *Source control*

- Rendezvous Point gives a single point of control for all sources in the network for any group range in ASM and PIM-SM networks
- (S,G) is not created on RP but still is on FHR
- It's control-plane – possibility to DDoS RP.
- Works best with other edge filtering methods

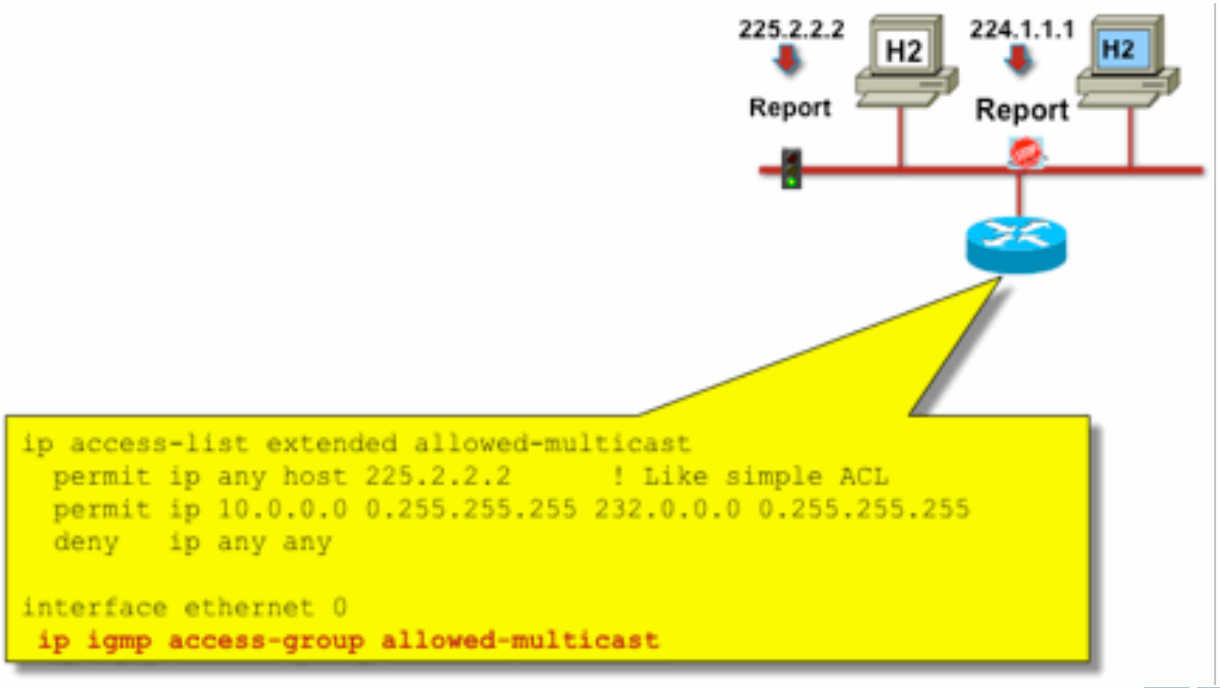


Trusted and secure sender/receiver *Securing receiver*

- Control IGMP on receiver side
  - IGMP is enabled by default if multicasts are enabled
  - IGMP carries protocols – PIMv1, Mrinfo, DVMRP, Mtrace
  - Unicast IGMP should always be filtered – those are used in special situations like unidirectional links
  - If single IGMP querier is present on non-redundant segment then IGMP queries should be dropped

Trusted and secure sender/receiver *Securing receiver*

- Restrict which multicast sources receiver can join
  - For ASM filter basing on destination address
  - For SSM using IGMPv3 filter basing on source and destination address



Dense Mode Fallback Problems

Dense Mode Fallback Problems

- Dense Mode Fallback occurs when RP information is lost
  - PIM determines whether a multicast group operates in PIM-DM or PIM sparse-dense mode based solely on the existence of RP information in the group-to-RP mapping cache
- It's event, when PIM mode falling back from sparse mode to dense mode
  - Dense mode flooding occurs

Dense Mode Fallback Problems

- Dense Mode Fallback Prevention provides a method for:
  - Preventing Dense Mode Fallback
  - Blocking multicast traffic for groups not specifically configured (there is no RP for the group)

- By default Dense Mode Fallback is enabled
  - Except when all interfaces are configured in PIM Sparse Mode (not PIM Sparse-Dense Mode)

Dense Mode Fallback Problems

```
ip multicast-routing
ip pim send-rp-announce ethernet 0 scope 16 group-list 1
ip pim rp-address 10.8.0.20 1
no ip pim dm-fallback
!
interface ethernet 0/0
 ip pim sparse-dense-mode
```

Admission Control

Admission Control

- Control-plane protection
- Resource allocation
- Bandwidth protection from congestion
- Content-based policies
- Subscriber-based policies

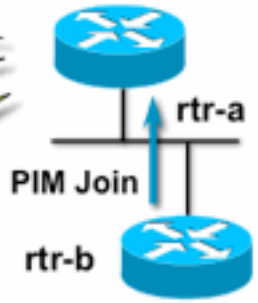
Admission Control

- Limiting number of multicast routes in mroute table
  - No new entries created after reaching limit
  - Syslog warning beyond threshold point
  - vrf-aware

```
ip multicast route-limit 1500 1460
```

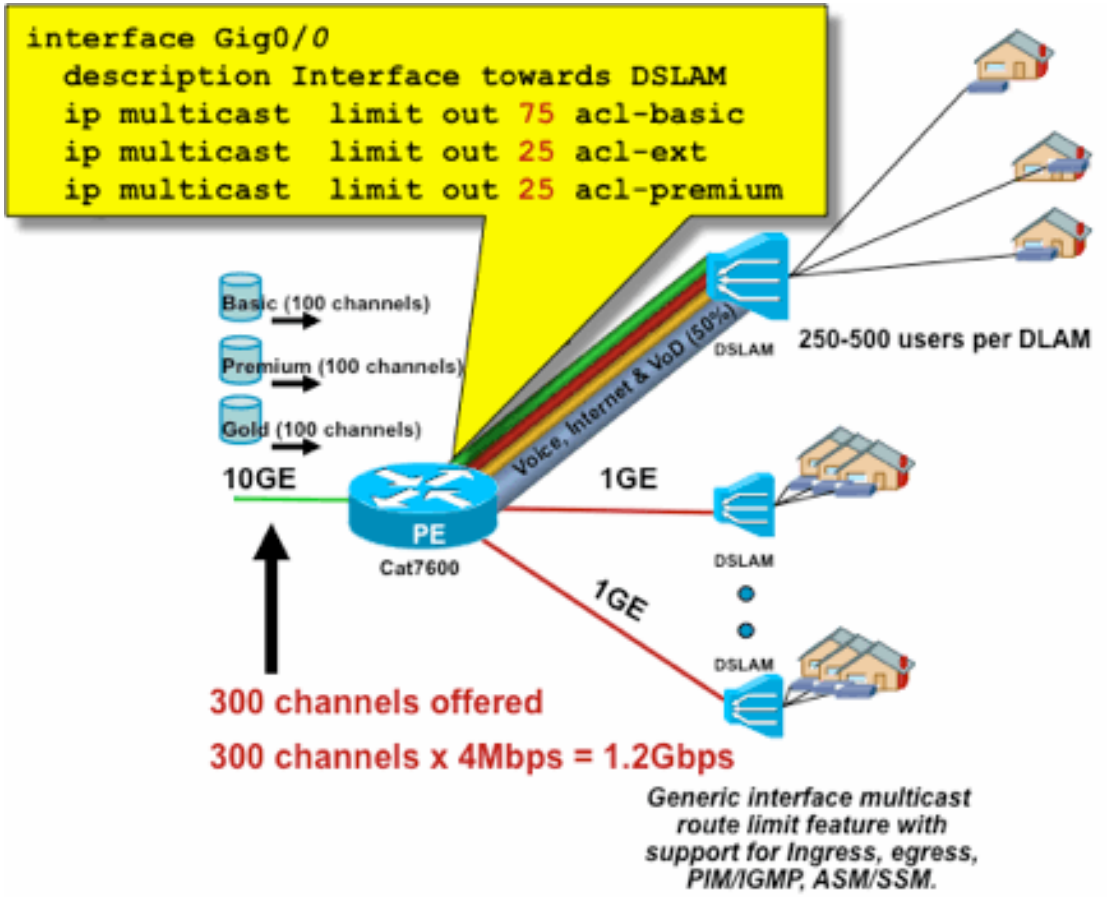
```
rtr-a> show ip mroute count
IP Multicast Statistics
1460 routes using 471528 bytes of memory
404 groups, 2.61 average sources per group
```

```
%MROUTE-4-ROUTELIMITWARNING :
    multicast route-limit warning 1461 threshold 1460
%MROUTE-4-ROUTELIMIT :
    1501 routes exceeded multicast route-limit of 1500
```



Admission Control

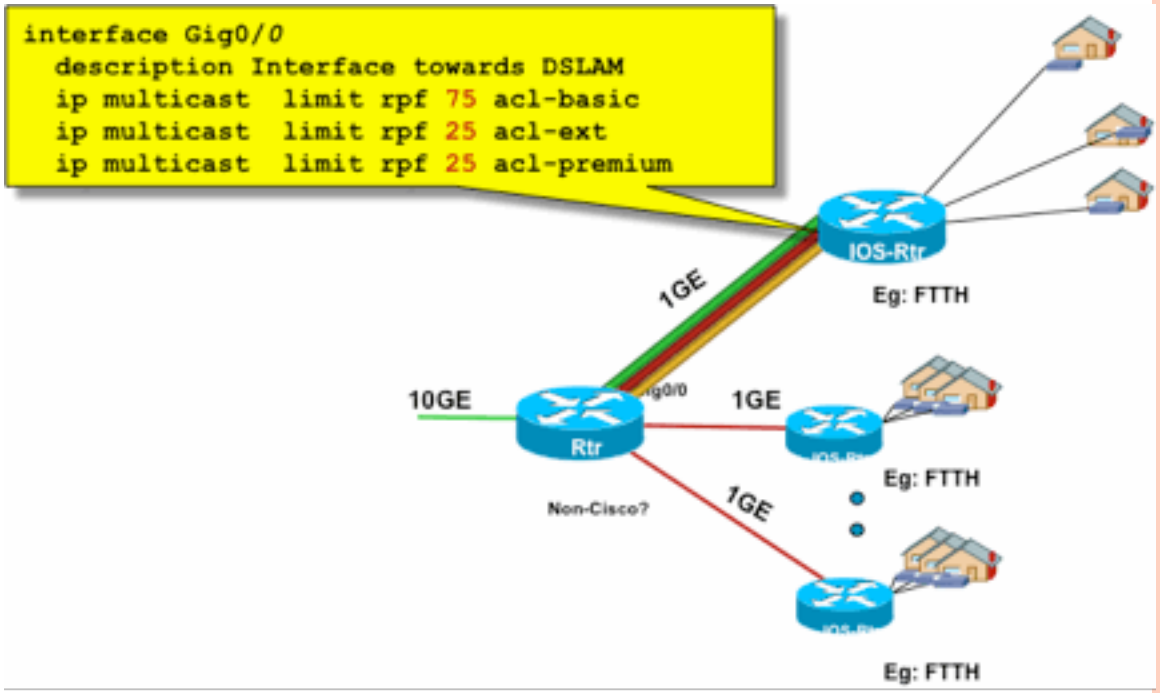
- Limiting mroute state for PIM and IGMP per interface
- Egress admission control



Admission Control

- Limiting mroute state for PIM and IGMP per interface
- Egress admission control
- Ingress admission control

```
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
```



Admission Control

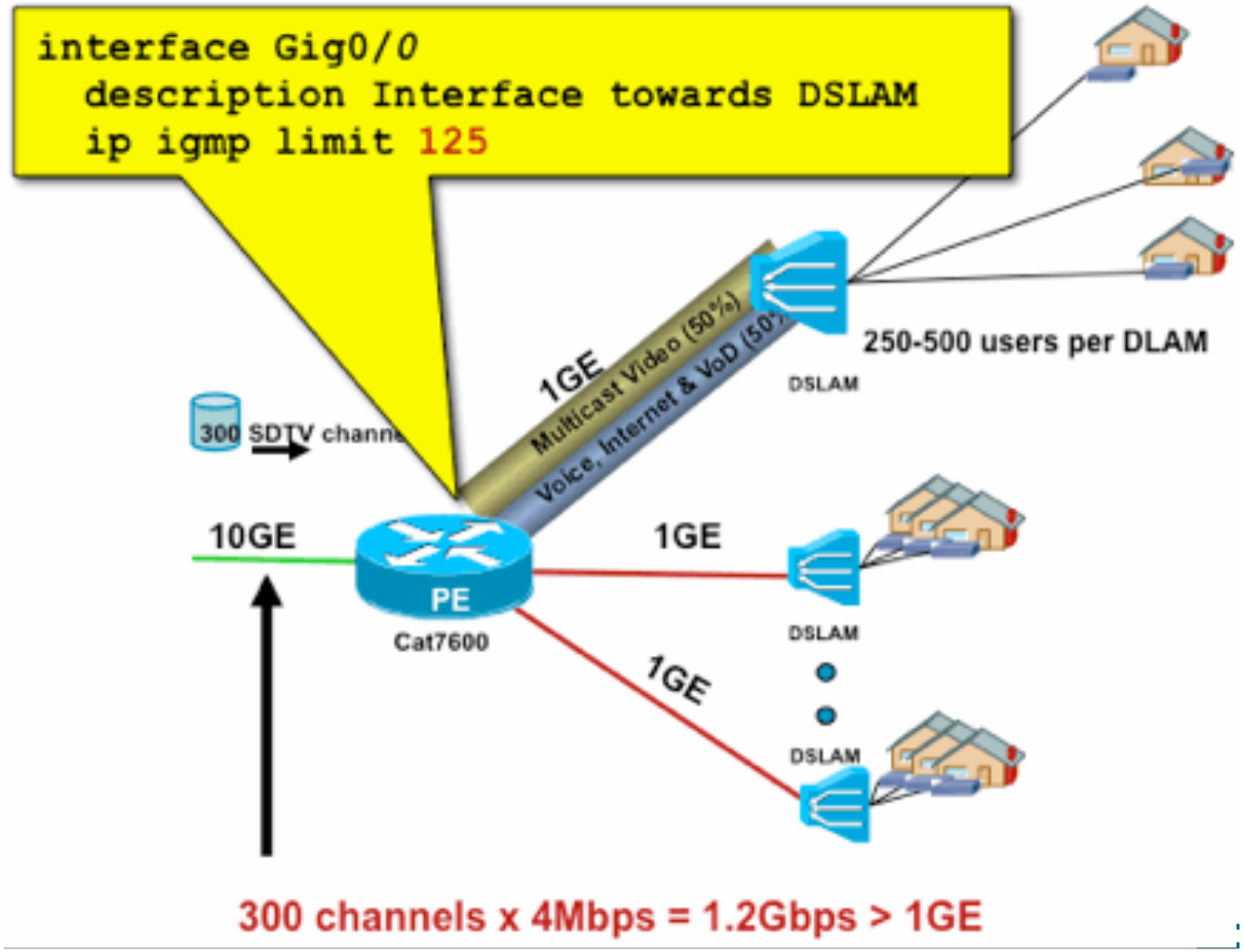
- Limit the number of IGMP groups joined both globally and per interface

```
ip igmp limit 100
```

- Exceptions can be defined by ACL

```
ip igmp limit 100 except MCAST-GRP
!
ip access-list extended MCAST-GRP
 permit ip any host 239.255.255.254
 deny ip any any
```

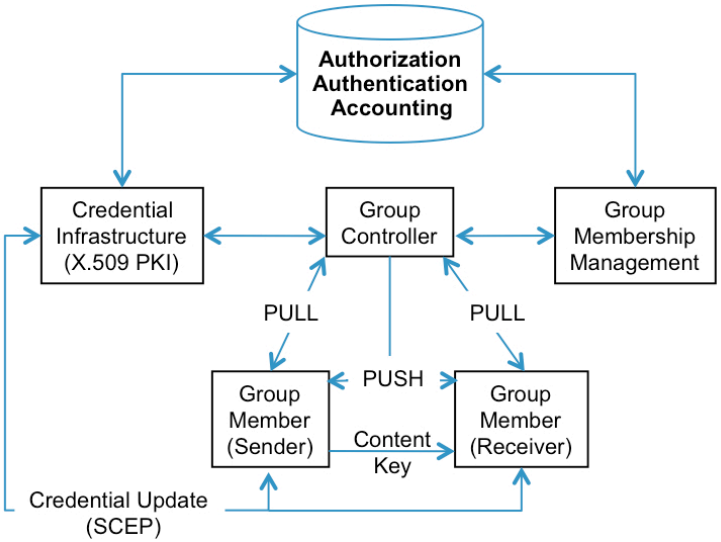
Admission Control



Tunneled Multicast

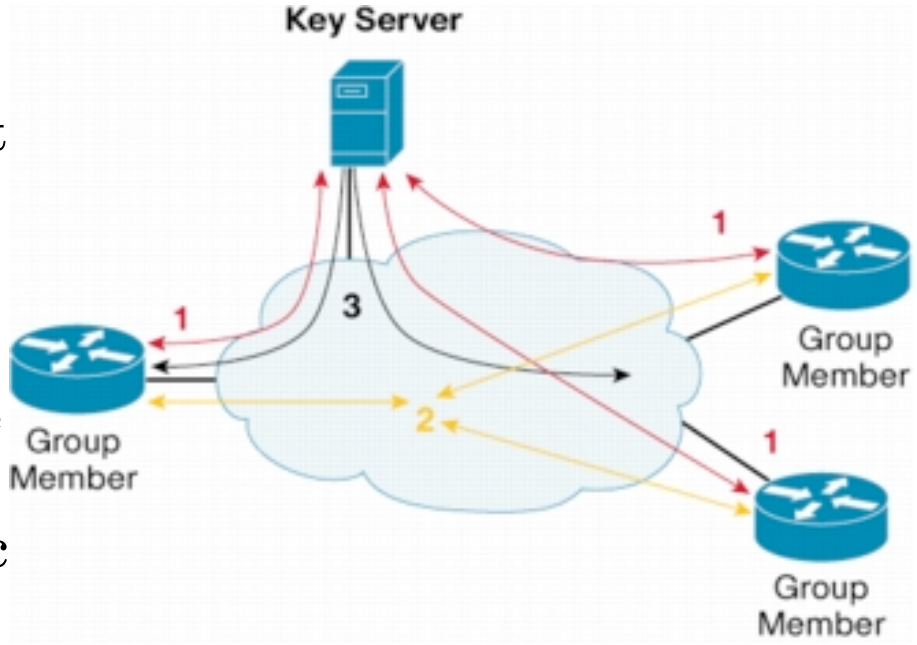
Tunnelled Multicast

- IPSec point-to-point tunnel interfaces since late 12.3T permits to encrypt multicast traffic
- Multicast for GET VPN since 12.4(6)T
  - Including control-plane security
- Manual key distribution or RFC3547 GDOI (Group Domain of Interpretation)



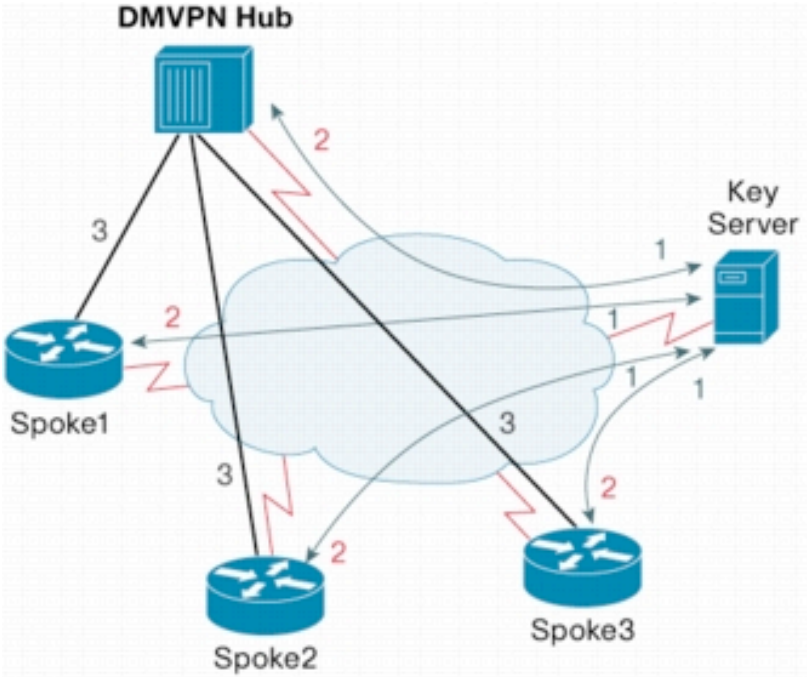
Tunnelled Multicast

- GDOI Implementation
  - Group members register with the key server – IPsec policy and keys that are necessary for encrypt and decrypt IP Multicast packets are distributed
  - Group members exchange IP Multicast packets that are encrypted using IPSec
  - As needed, the key server pushes a rekey message to the group members



Tunnelled Multicast

- GDOI with DMVPN



- DMVPN hub and all spokes are configured as group members. All group members register with the key server.
- The key server distributes group and IPsec policy information to all group members.
- A spoke-to-hub tunnel is established using NHRP. All packets traveling via the DMVPN tunnel are now encrypted using the group key.
- The spoke sends NHRP resolution request to the hub for any spoke-spoke communication
- Upon receiving NHRP resolution reply from the hub, the spoke sends traffic directly to their spokes with group key encryption.

Benefit: Using Cisco IOS Secure Multicast functionality in a DMVPN network eliminates the delay caused by IPsec negotiation.

Note: Multicast traffic will still be forwarded to hub for any spoke to spoke connectivity even with this deployment.

Tunnelled Multicast

- GDOI – few facts:
  - It's not IKE!
  - Uses UDP port 848
  - Not negotiated – server push keys and policies
  - No keepalives

Tunnelled Multicast

- Secure PIM control traffic
  - Encrypt and Authenticate PIM Packets
  - Crypt map for 224.0.0.13 (PIM Control Messages) except of PIM Register which is unicast – require additional protection
  - Hop-by-hop encryption
  - Not all combinations of hash+security+encryption works for multicast traffic!
  - Recommended mode is transport with manual keys

Questions?

Thank You