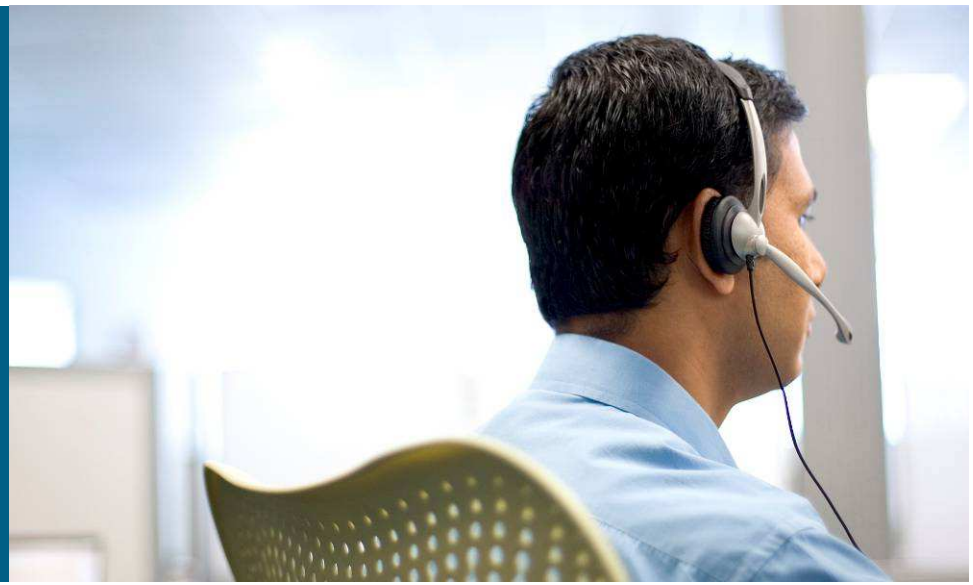


Securing a Multicast Network

Michael Behringer <mbehring@cisco.com>

ESNOG, 16 Oct 2008, Barcelona

Securing a Multicast Network – Agenda

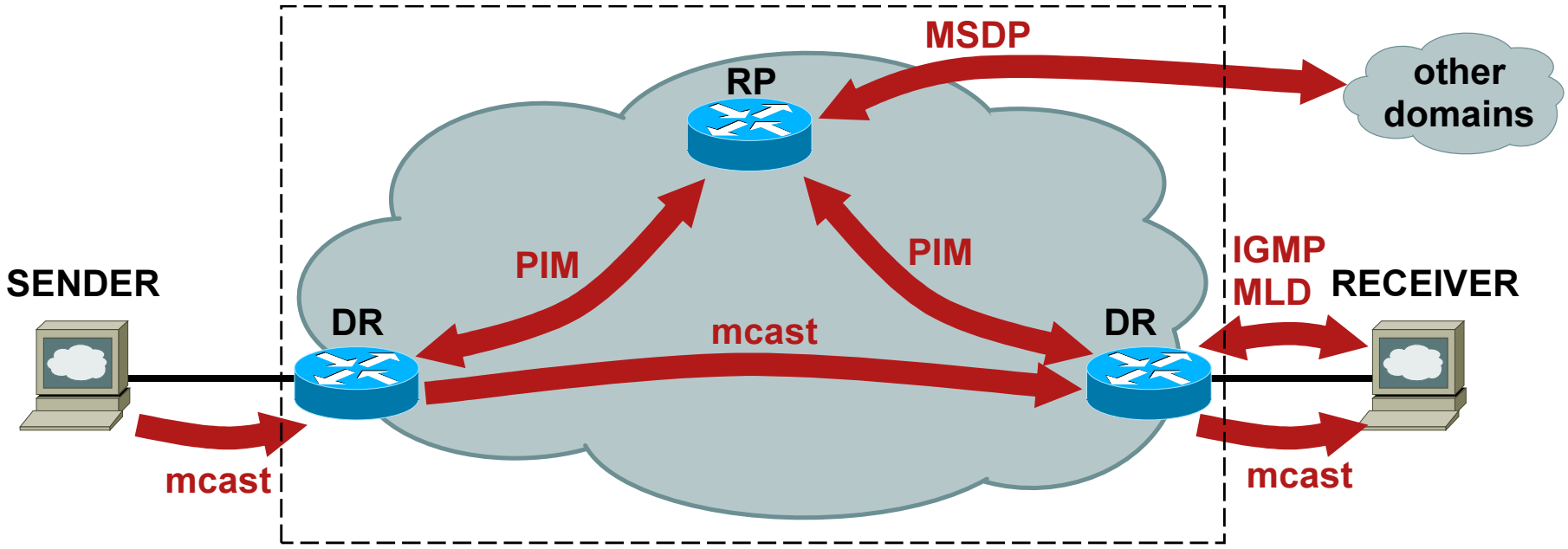
- Background / Introduction
- Securing a Multicast Network
- MVPN Security Overview
- Multicast and IPsec

Background

General Comments

- Mcast optimisation different from unicast
  - Unicast: Optimise around topology
  - Mcast: Optimise around applications
- Mcast attack specifics:
  - Hard to attack end system (receiver driven)
    - But can create state, attack network
  - Focus on state (Unicast attacks also on bandwidth)
- Mcast packets: data plane *and* control plane
  - → Complicates security

Zones of Trust: SP Core



- Zone of trust: Defines “trusted” and “untrusted”

  (not 100% reliable definition; ignores insider attacks)

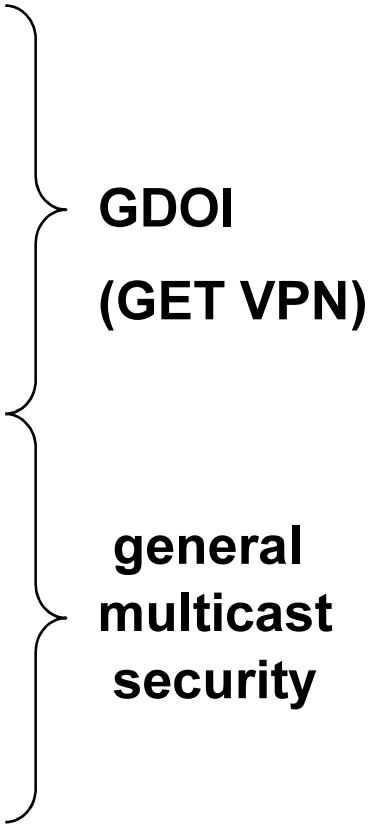
- Simplifies security:

  Secure boundaries: Mcast, IGMP/MLD, MSDP

- Basic idea: Block everything else (eg PIM, if not needed)

Threats

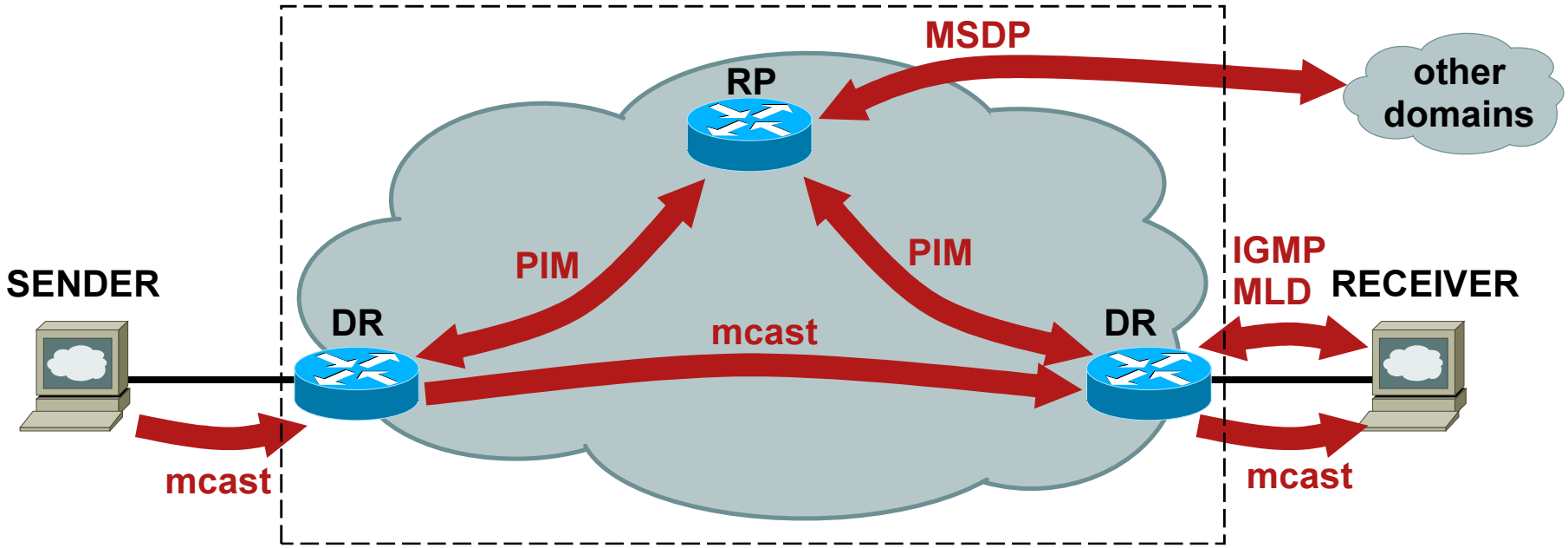
- Confidentiality: eavesdropping on mcast streams
- Traffic integrity: modification
  - E.g.: control plane traffic, eg: PIM, OSPF
- "Service integrity":
  - E.g.: unauthorised senders or receivers
- Availability
  - Various forms of DoS attacks, resource starvation



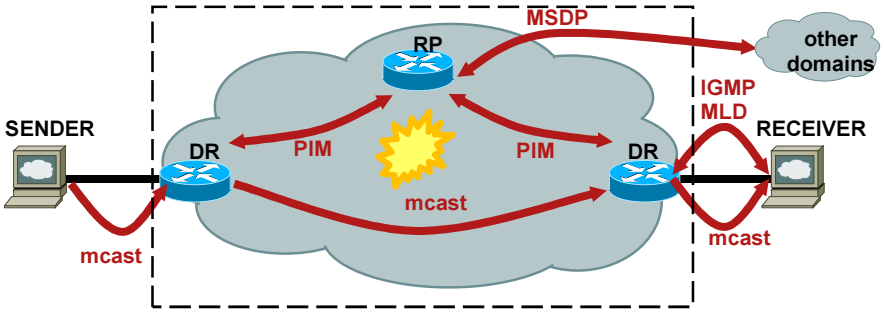
Securing a Multicast Network

Securing a Multicast Network

- Securing a Network Element
- Securing the Network
- Sender / Source issues
- Receiver issues – Controlling IGMP
- Admission Control



Securing a Network Element



- General router security

  physical security, strong passwords, secure protocols, AAA, …

- Protecting the control plane

  rACL, CoPP

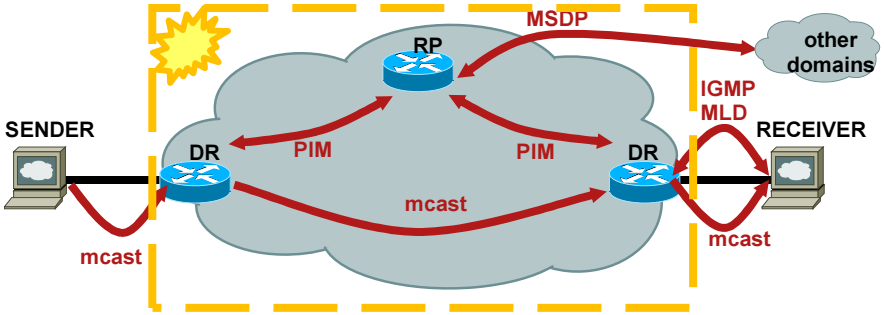
- Controlling mcast state

  ip multicast route-limit;

  no ip sap listen;

  ip multicast mrinfo-filter; (note: permit/deny counter intuitive)

Securing the Network



- ip multicast group-range <std-acl> (only ipv6 today)

  global; limits *all* mcast operations, plus data plane.

- ip multicast boundary

  interface;

  permit only groups you need; deny auto-RP;

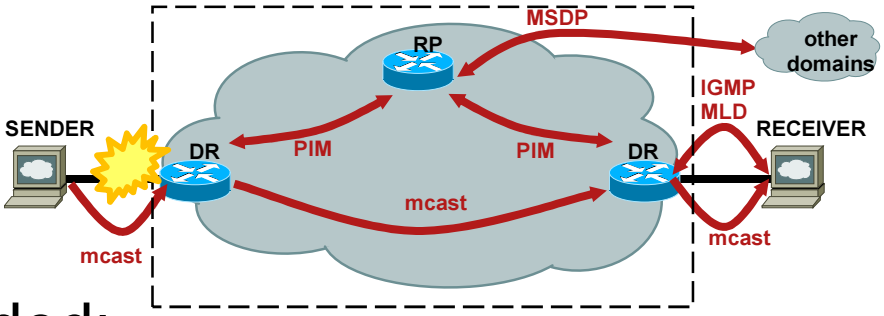
  can deny (*,G) by “deny ip host 0.0.0.0 any”

- ip msdp sa-limit

  Rate limit “source active” messages inter-domain.

(224.0.0/24) Local Network Control Block
…
224.0.0.13 All PIM Routers
…
224.0.0.22 IGMP

Sender / Source Issues



- Unicast features, recommended:

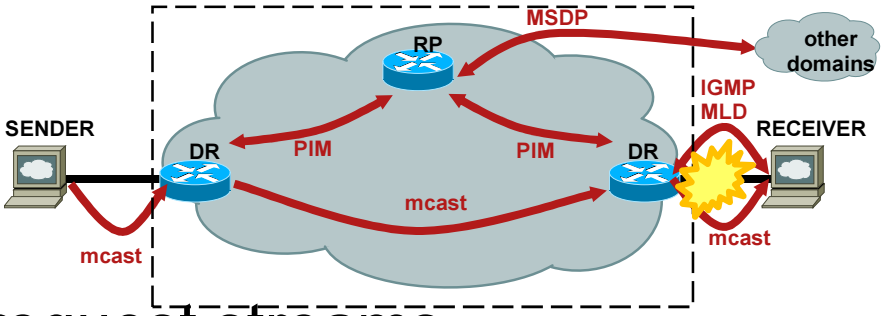
  Source address spoofing prevention: ACLs, AAA, uRPF.

  Infrastructure ACL (iACL)

- Filtering permitted src → mcast group

  part of normal interface ACL

Receiver Issues: Controlling IGMP/MLD



- Without IGMP/MLD, cannot request streams
  - → No data plane security required in principle
  - → Focus on IGMP/MLD
- Host doesn't need mcast: Block IGMP/MLD
  - IPv4: IGMP is an IPv4 protocol type (IPv4 procotol 2)
  - IPv6: MLD is carried in ICMPv6 protocol type packets
- Filter specific IGMP types (see next slide)
- Control IGMP on switch:
  - Router Guard: define host port explicitely
  - IGMP snooping (enforce a minimum version of IGMP)

IGMP Interface Packet Filtering (data plane)

```
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 with redundant routers
  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    ! IGMPv1/2/3 quer.
  permit igmp any 224.0.0.0 15.255.255.255 host-report   ! IGMPv1/2 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
```

IGMP Filtering (control plane)

- ip igmp access-group <acl> / ipv6 mld access-group

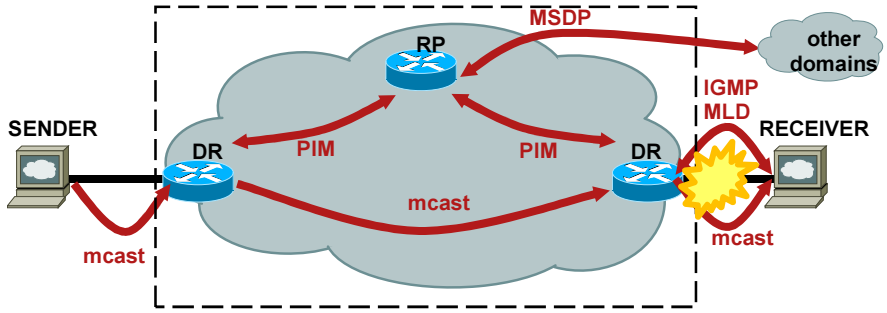
  Interface command;

  defines which groups and sources can be requested by the receiver.

  For ASM / IGMPv1/2: source is ignored

  For SSM / IGMPv3: source is filtered as well

Admission Control



- Global and per interface IGMP / MLD limits:

  ip igmp limit <n> [except <ext-acl>]

  ipv6 mld limit <n> [except <ext-acl>]

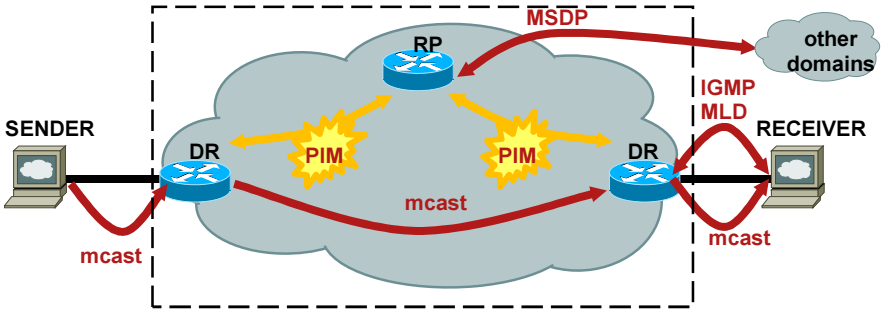
- Per interface mroute limit:

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

- Bandwidth limits:

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

PIM Security



- PIM can be blocked at the edge; only used internally.
- Rate limiting PIM register messages from DR to RP

  ip pim register-rate-limit
- On RP:

  ip/ipv6 pim accept-register list <acl> (acl lists sources)

  (note: control plane feature; DoS vector)
- Interface based PIM neighbor filtering:

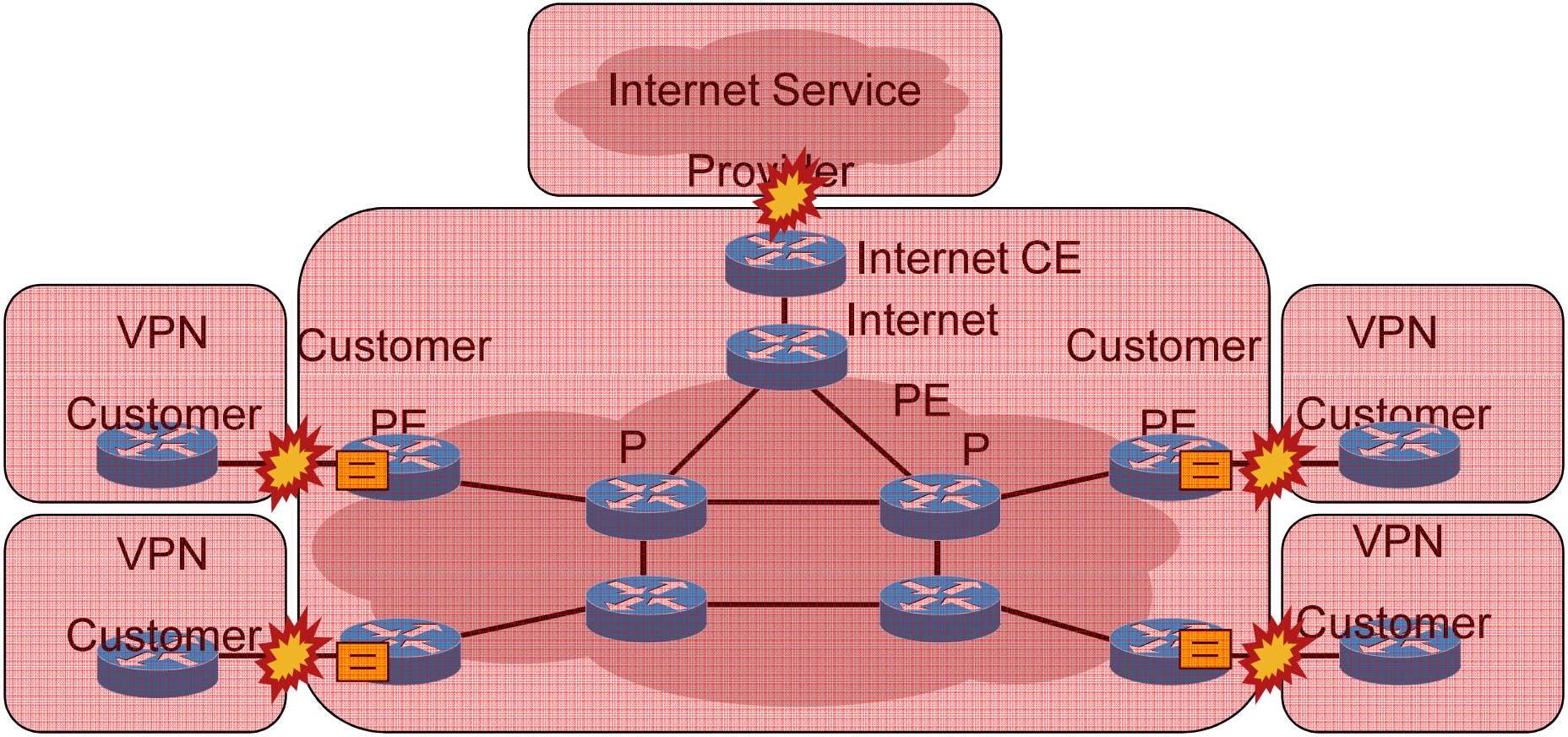
  ip pim neighbor filter <acl>
- Auto RP security

  ip pim rp-announce-filter rp-list 1 group-list 2 ← on Mapping Agent
- BSR control (filter BSR messages on domain edge)

  ip pim bsr-border

M-VPN Security

MPLS VPN: Zones of Trust



- Assumption: Each zone is in itself secure
- Procedure: examine interfaces between zones!

Separation with MVPN: Between VPNs, and VPN and Internet

- Unicast traffic remains separate, as in standard 2547

  This includes unicast PIM packets: Handled per (M)VRF

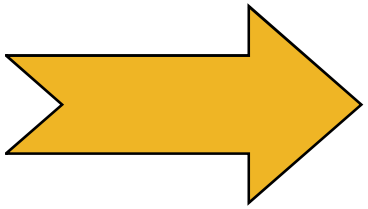
  → Even spoofed PIM will remain within VPN; control plane information handled in MVPN context only.

- Traffic → Multicast addresses

  Also stays within the VPN

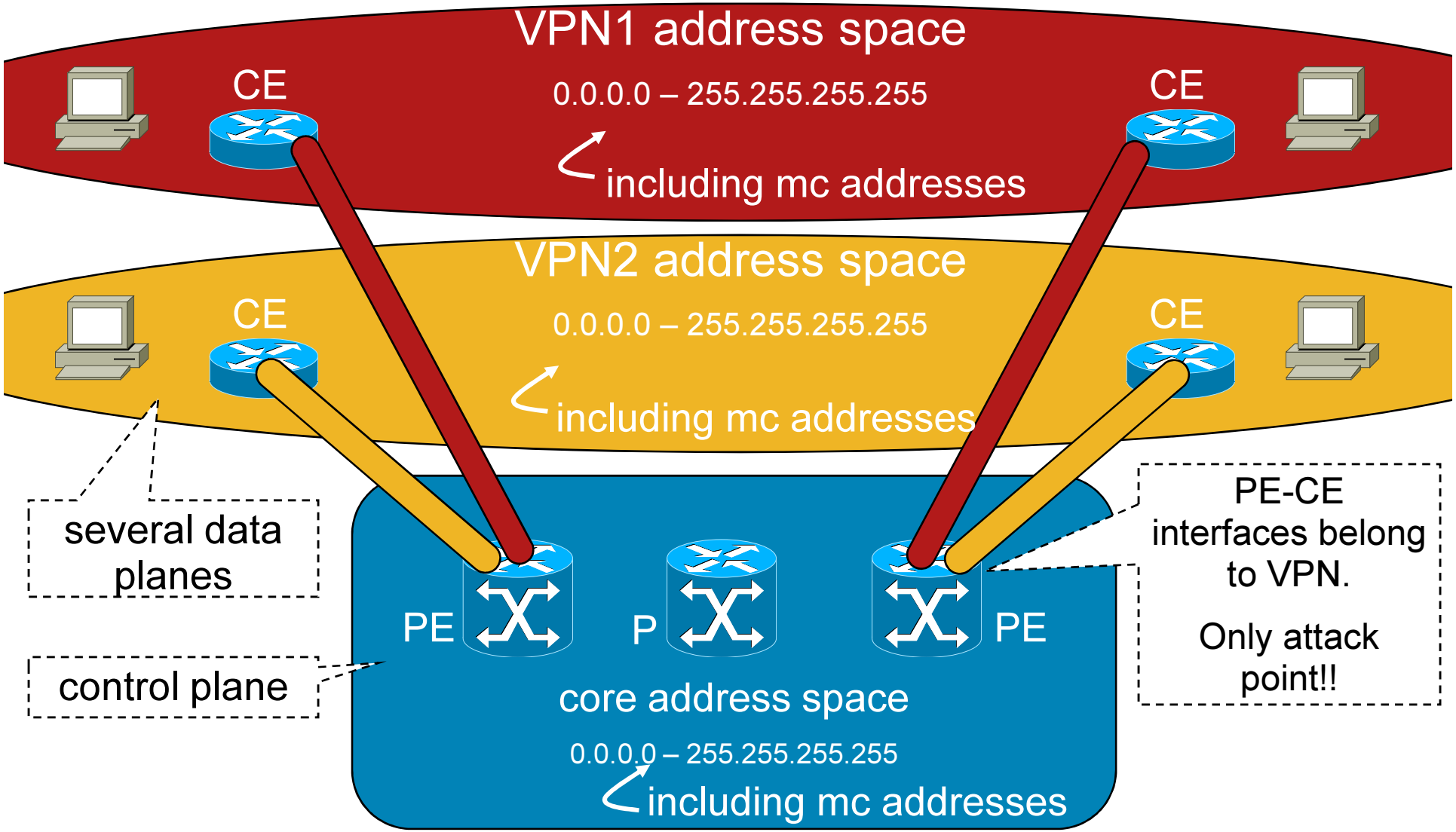
  → Each VPN may use the same mc groups

  → Each VPN may use mc groups which are used also on the core (for Internet mc for example)



Separation for unicast and multicast traffic between (M)VPNs, and core

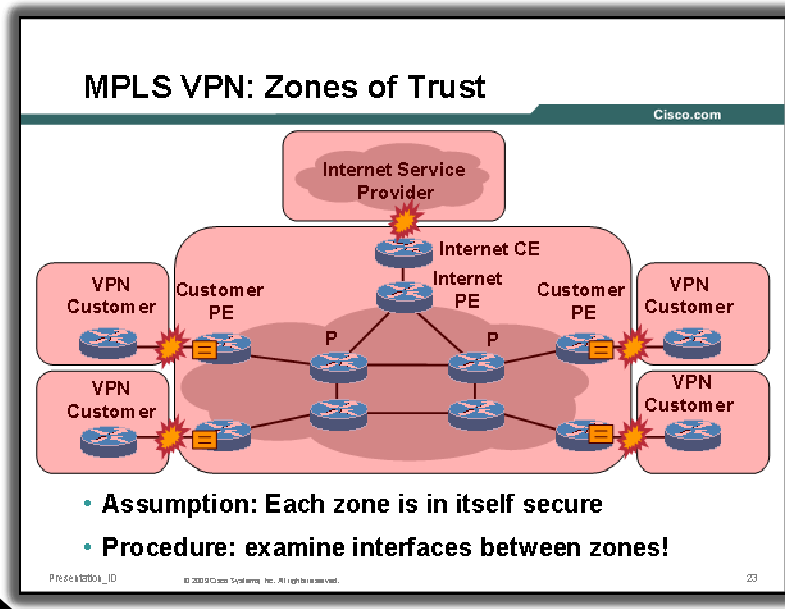
Address Planes: True Separation for unicast and multicast!



Interface PE-CE: MVPN Non-Threats

For MVPN specific traffic flows:

- PIM between CE and PE (control plane)
  - One MVPN “controlling” another MVPN through faked PIM messages
  - MVPN and core mc interference
- Multicast traffic (data plane)
  - Sending / receiving data traffic (mc) to / from another MVPN or core



Integrity breaches cannot happen due to context separation

Interface PE-CE: MVPN Possible Threats

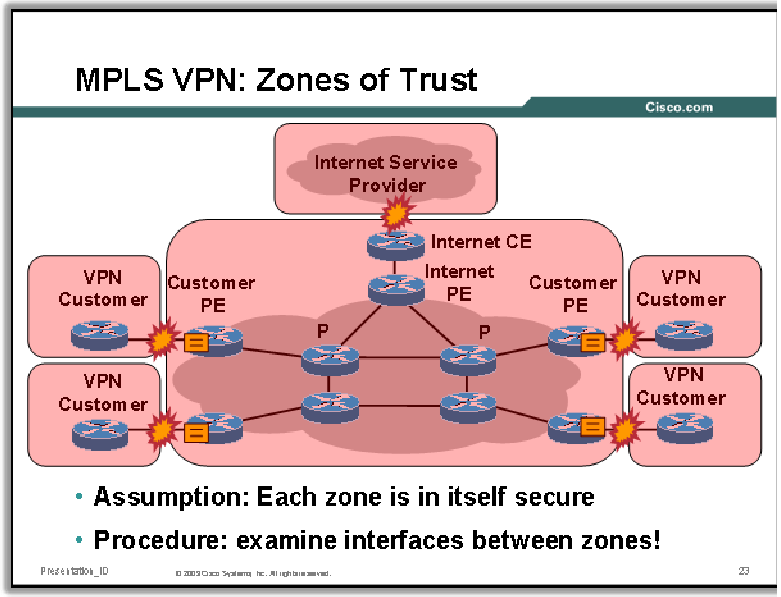
For MVPN specific traffic flows:

- PIM between CE and PE (control plane)

  Flooding with control messages
  → DoS

- Multicast traffic (data plane)

  Flooding with data messages
  → DoS



Flooding must be controlled on control plane and data plane

Attacks against PE: Faked PIM packets (Hacker's Goal: Integrity Breach)

- All PIM mc packets are link local

  → Attacks must originate on the same subnet (or CE must be compromised / faulty)

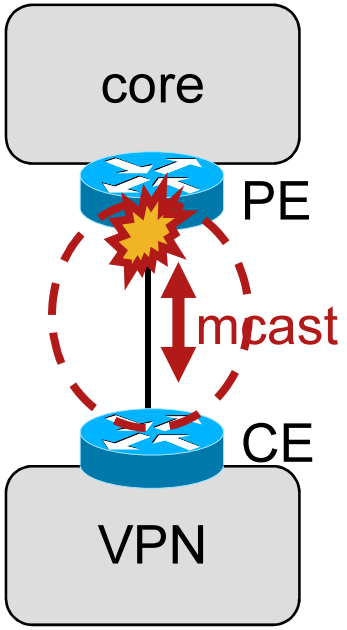
- Various attacks possible

  Forged join/prune, hello, assert, BUT:

  All attacks have only *local* effect (this VPN)

- Faked PIM unicast packets

  Also remain within the context of the VPN



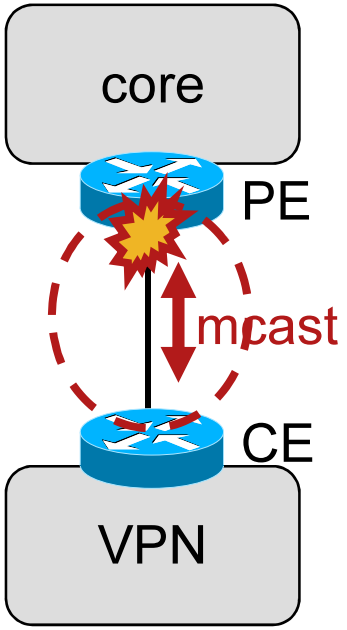
No integrity breach on other (M)VPNs or MPLS core possible (due to separation)

But … see next slide …

Attacks against PE: DoS with PIM packets

Various DoS attacks possible

- Flooding of packets
  → CPU overload on PE
- Flooding of state
  → memory exhaustion on PE



DoS Attacks *can* affect other VPNs or the core! (since the PE has shared CPU / memory)

But: This can be secured! See next section!

Attacks against PE: DoS with Multicast Data Traffic

- How would you flood with mcast traffic?

  Just send it? From many sources? High bandwidth?

  → No, mcast traffic is only sent if there are receivers

  → You would have to create both senders and receivers

  → Not easy

- Countermeassures:

  Rate-limit mcast traffic

  per router

  per interface

  In MVPN: per MDT

Securing the PE: Best Practices
Avoid RP on PE

Reason: higher exposure to DoS against PE

- RP receives join/prune messages

  Threat: Attacker sending large volume of (*,G) join/prunes with spoofed addresses.

  Can only be controlled at the edge → Hard to control

  Rate-limits???

- RP receives register / register-stop messages

  Threat: Fake register messages

  Solution: Filter ip pim accept-register, if DRs are known

  Solution: ip pim register-rate-limit on DRs (if DRs are trusted)

Securing the PE: Best Practices
Avoid src/rec directly connected to PE

Reason: higher exposure to DoS against PE

- Additional protocol needed (IGMP)
  - Additional exposure
  - Hard to secure
- IGMP per interface state limit can secure this
- IGMP ACL per group allowed can be valid service offering
- PE as last hop not recommended

Securing PIM

- Neighbor filters (only allow known PIM neighbors):
  - ip pim neighbor-filter → Recommended
- On RP: Filter on (S, G)
  - ip pim accept-register → Recommended
- Mroute table size can be limited

- Neighbor authentication:
  - PIM does not have MD5 auth built in
  - RFC: “may use IPsec AH”
  - Solution: GET VPN

Securing the Internet Access: MDT Tree Group Addressing

- MPLS core runs:

  MDTs for each MVPN (at least one)

  → Each MDT uses one mcast group

  plus possibly “native” core mcast (Internet mc)

  → Using potentially all mcast groups

- Design Recommendations:

  Avoid “native” mcast on same core as MVPN !!!

  MDT groups should use private mcast addresses, to avoid overlap with “native” mcast

  Groups used by MDTs must be filtered ingress from Internet / peers

Multicast VPN – Summary

- Each VPN can use multicast independently
  - Source and group may overlap with other VPN
  - Different PIM modes can be used
- VPNs remain fully separated
  - No reachability between VPNs, unicast or multicast
  - Cannot spoof other VPN, unicast or multicast
- MPLS core remains secure
  - Not attackable from VPNs, unicast or multicast
  - However: DoS of PE might affect other VPNs on that PE, this must be secured specifically
  - Core cannot be spoofed

Multicast and IPsec

Multicast and IPsec

- GET VPN / GDOI:

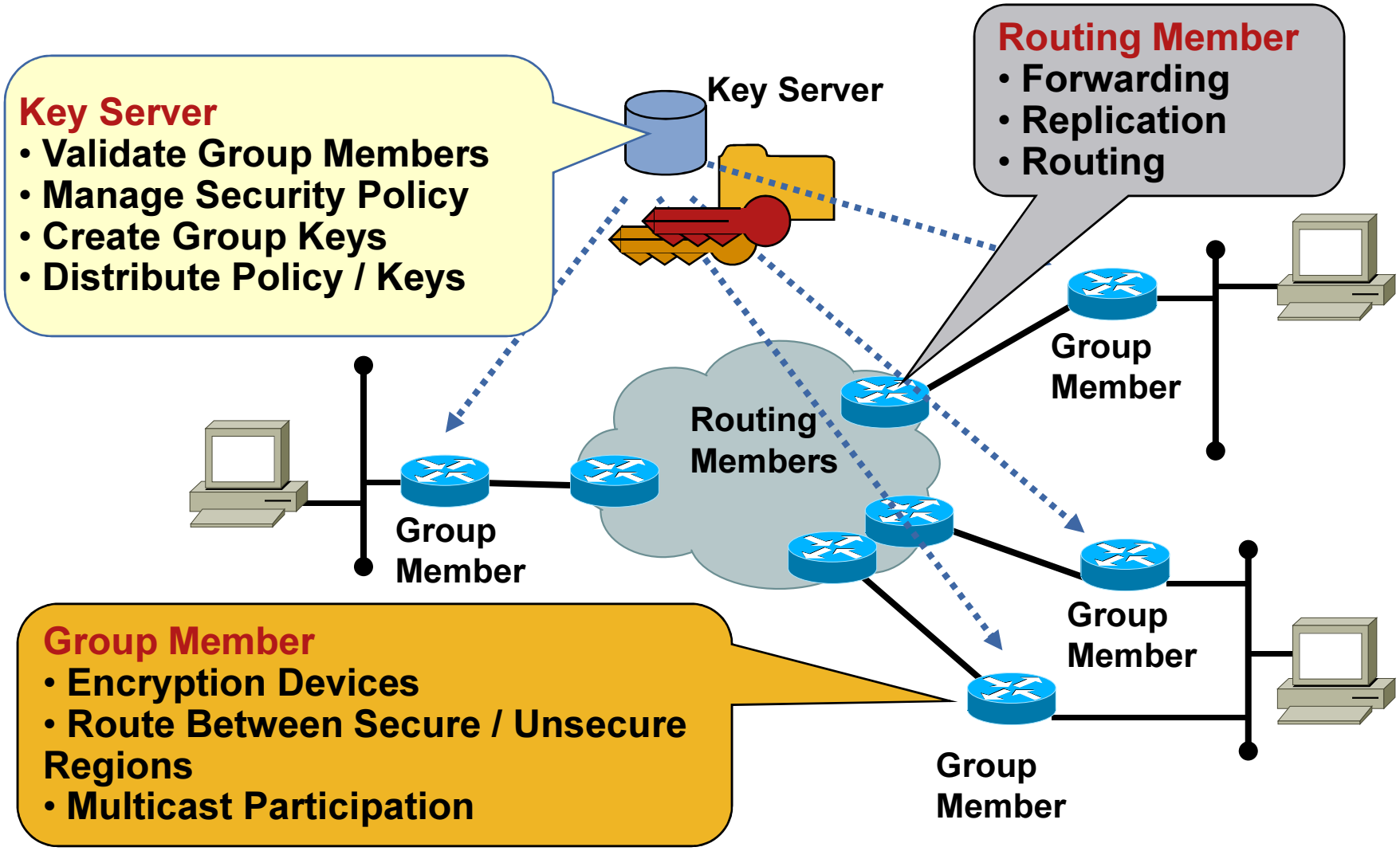
  Group SA to encrypt mcast streams

- Using GET VPN / GDOI for authentication

  OSPF, PIM, etc

See IETF msec working group

Group Security Functions



References & Further Reading

- Cisco Multicast Security

  http://www.cisco.com/en/US/products/ps6593/products_ios_protocol_group_home.html

- PIM-SM Protocol Specification

  RFC 4601, extensive security section!

- IETF Msec Working Group

  http://www.ietf.org/html.charters/msec-charter.html

- http://www.securemulticast.org/

- “Multicast Security: A Taxonomy and Some Efficient Constructions”, Ran Canetti et al., 1999

  http://www.ieee-infocom.org/1999/papers/05d_03.pdf

- Various papers on Multicast Security

  http://www.cisco.com/en/US/products/ps6593/prod_white_papers_list.html

- WP: “The Multicast Security Toolkit”

  http://www.cisco.com/web/about/security/intelligence/multicast_toolkit.html

- Multicast Security NW 2006 Presentation

  http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6552/prod_presentation0900aecd806694df.pdf