Securing Concast

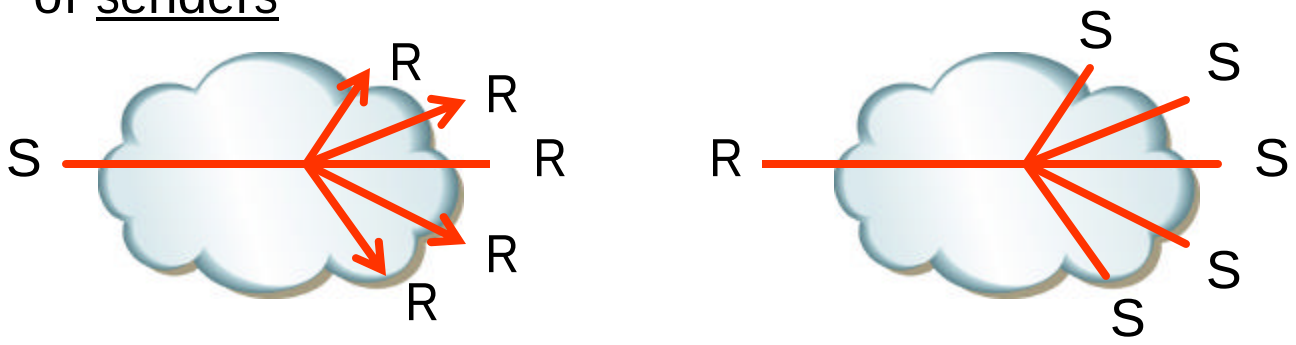
Ken Calvert (calvert@netlab.uky.edu)
Jim Griffioen, Billy Mullins,
Leon Poutievski, Amit Sehgal
ActiveCast Project
Laboratory for Advanced Networking
University of Kentucky, USA
http://protocols.netlab.uky.edu/~acast/

Outline

- Concast overview
- GSEC Interest (?)
- Security requirements for concast
- IPsec-based Approach
- Policy considerations

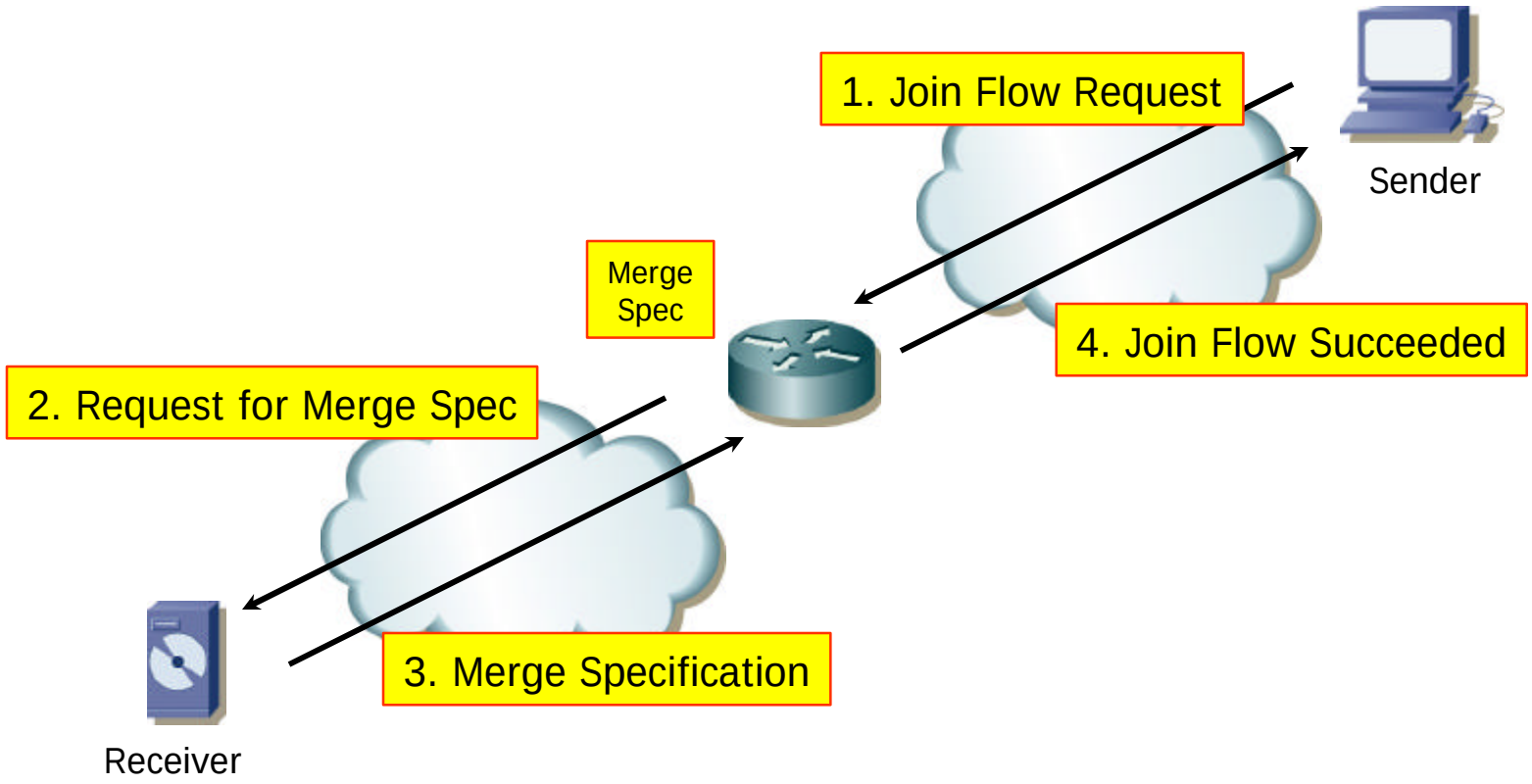
What is Concast?

- Many-to-one network service (inverse multicast)
- Scalability through abstraction
  - "Inverse Multicast": Single address represents any number of senders

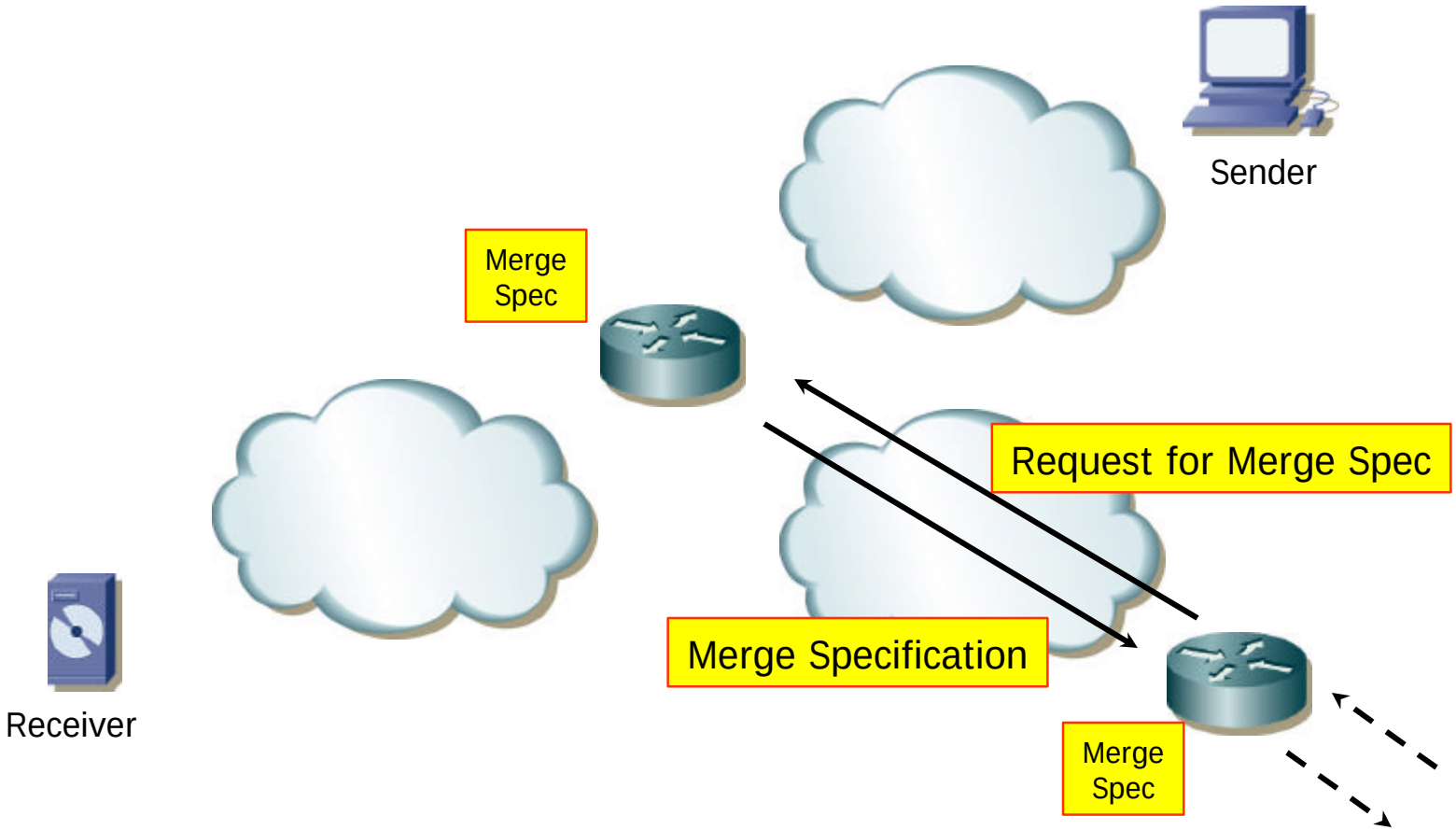


  - Network merges messages on route to receiver
    ...according to a receiver-supplied merge specification
  - Multiple sends result in single message delivery
- Benefits both receiver and network

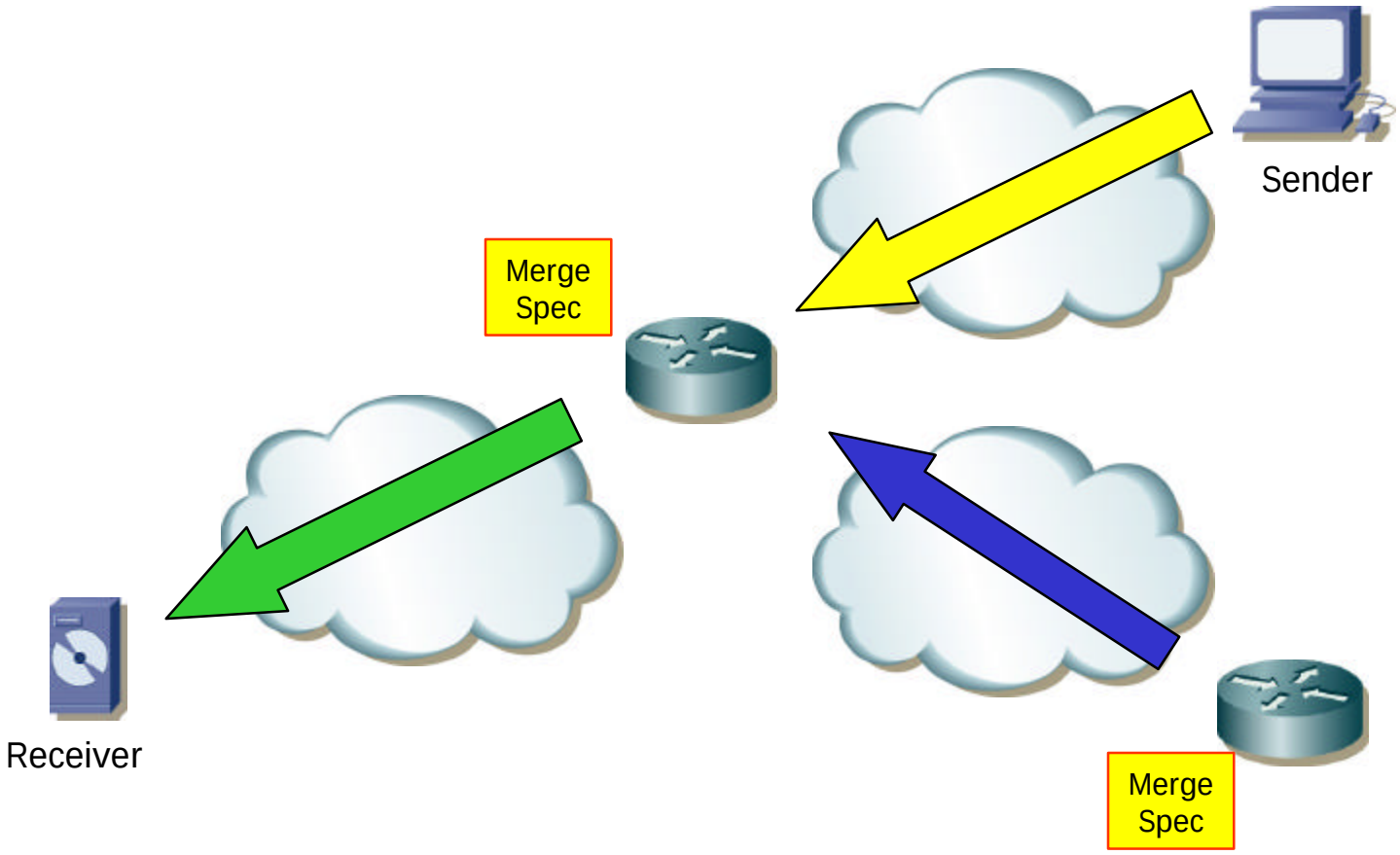
Concast Signaling



Concast Signaling



Concast Data Flow



Why GSEC Might Care (or not)

- A non-multicast group application
- A different way to secure group feedback
  - With (generic) assistance from the infrastructure
- Somewhat different policy issues
  - Third-party policy enforcement (necessary for scaling?)
- Concast is not currently deployed (is multicast?)
  - Internet draft (expired) describes the service (no signaling)
- But the ideas and approach may apply in other contexts (e.g. overlays)

Concast Security Requirements: User

- Origin: concast receiver

  (which is usually also the multicast sender)
- Requirement: Data integrity, authenticity, confidentiality
- Application-level policy:
  - Which entities can participate as a sender
- Network-level policy:
  - Which routers (IP addresses/domains) are trusted to:
    - Perform merging
    - Enforce user policies!

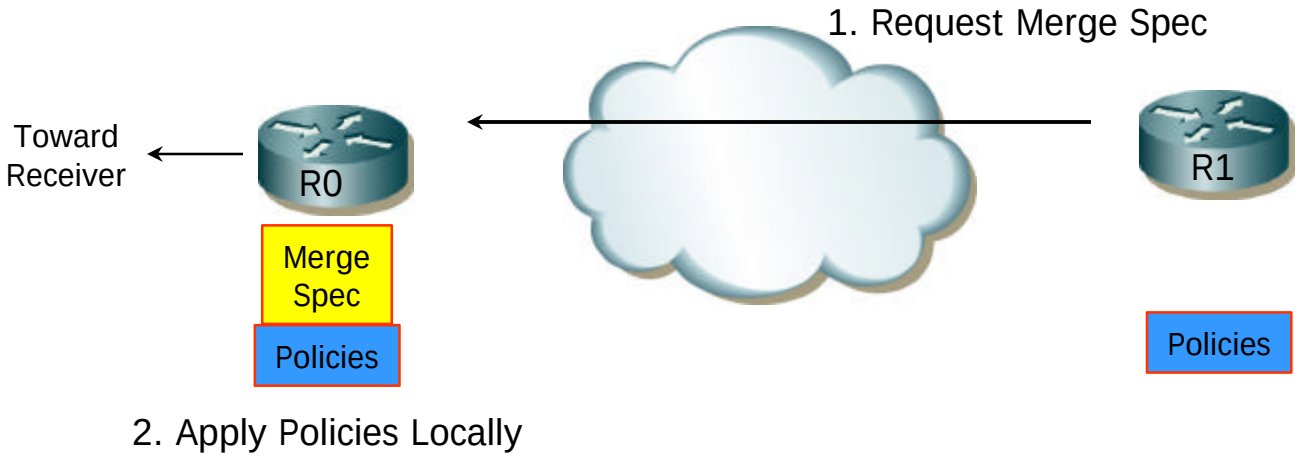
Concast Security Requirements: Provider

- Origin: concast-capable router (or proxy)
- Requirement: access control
  - Ensure that only paying customers use the service
  - Enforce customer policies about session participants
- Network-level policies:
  - Which entities (IP addresses) can participate as senders/receivers
  - Which concast-capable routers (IP addresses/domains) can be downstream/upstream of this router
    - Note: policies specify only neighbor relationships

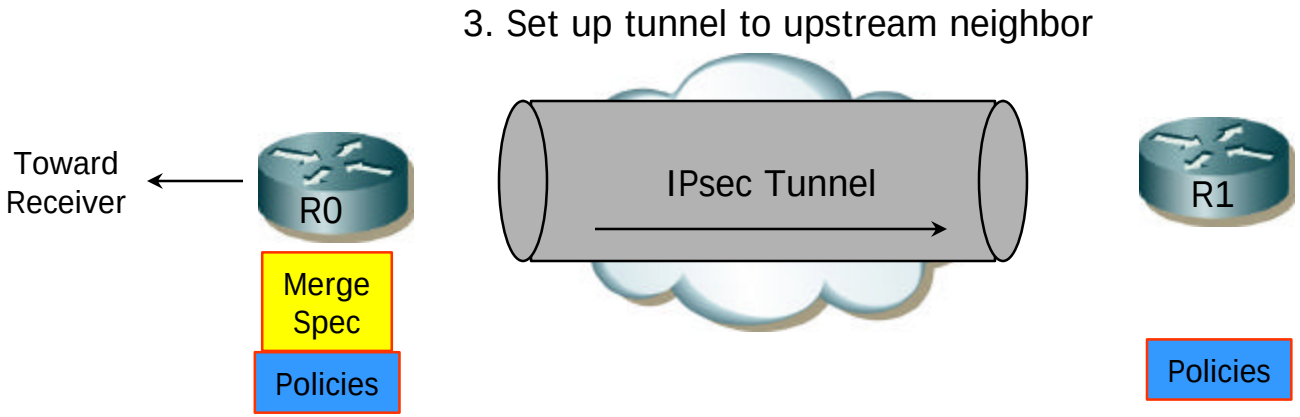
Approach

- Idea: secure the signaling; data handled via merge
- Set up IPsec tunnel between concast neighbors at signaling (join/RFM) time
  - No merge specification (including policy) sent in the clear
  - Protocol-specific (CSP) IPsec tunnel
    - Re-use for other flows between same nodes
- Data plane security: up to the application
  - Router trusted to implement user merge spec
  - Add encryption, MAC hooks to the fixed merge framework
  - Applications can instantiate them as desired
  - Transmit keys along with merge specification

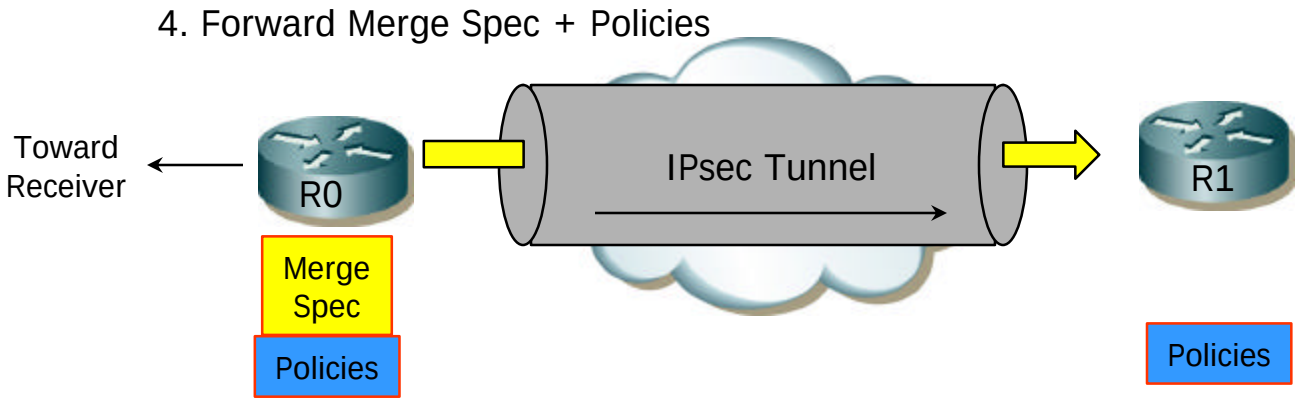
Secure Concast Flow Setup



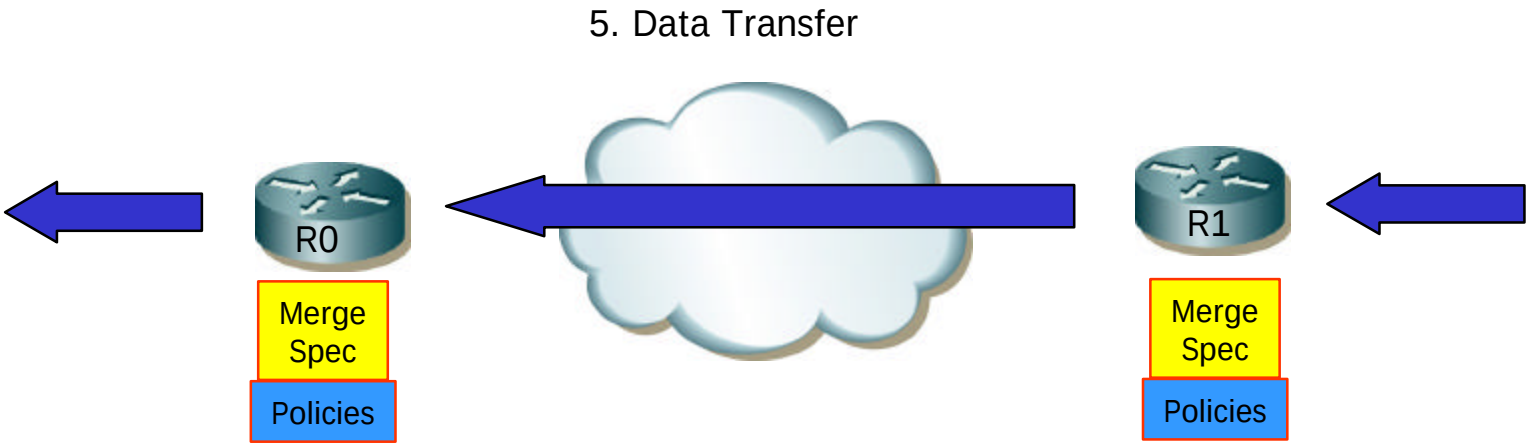
Secure Flow Setup



Secure Flow Setup



Secure Flow Setup

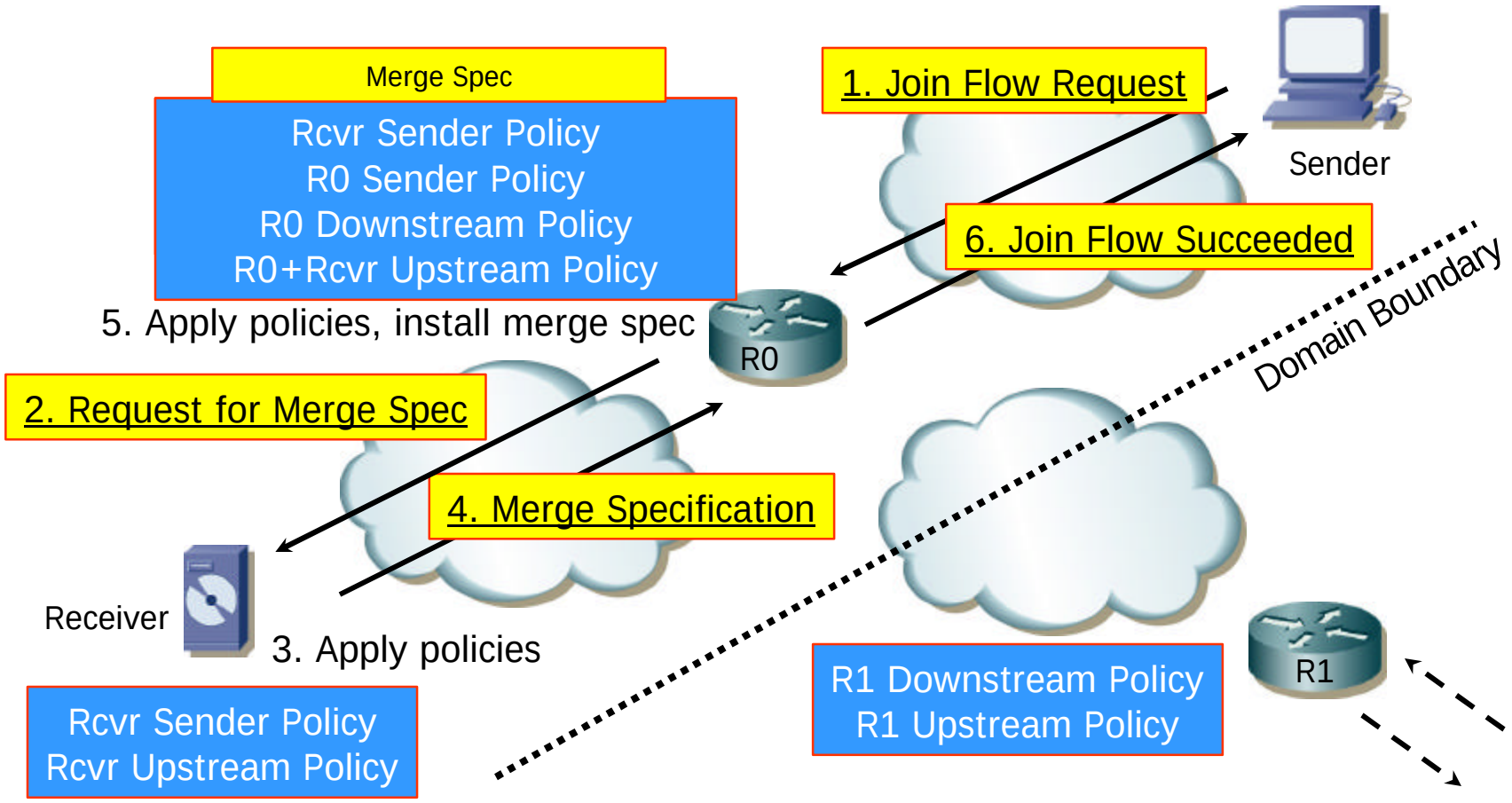


Monotonicity of Policies

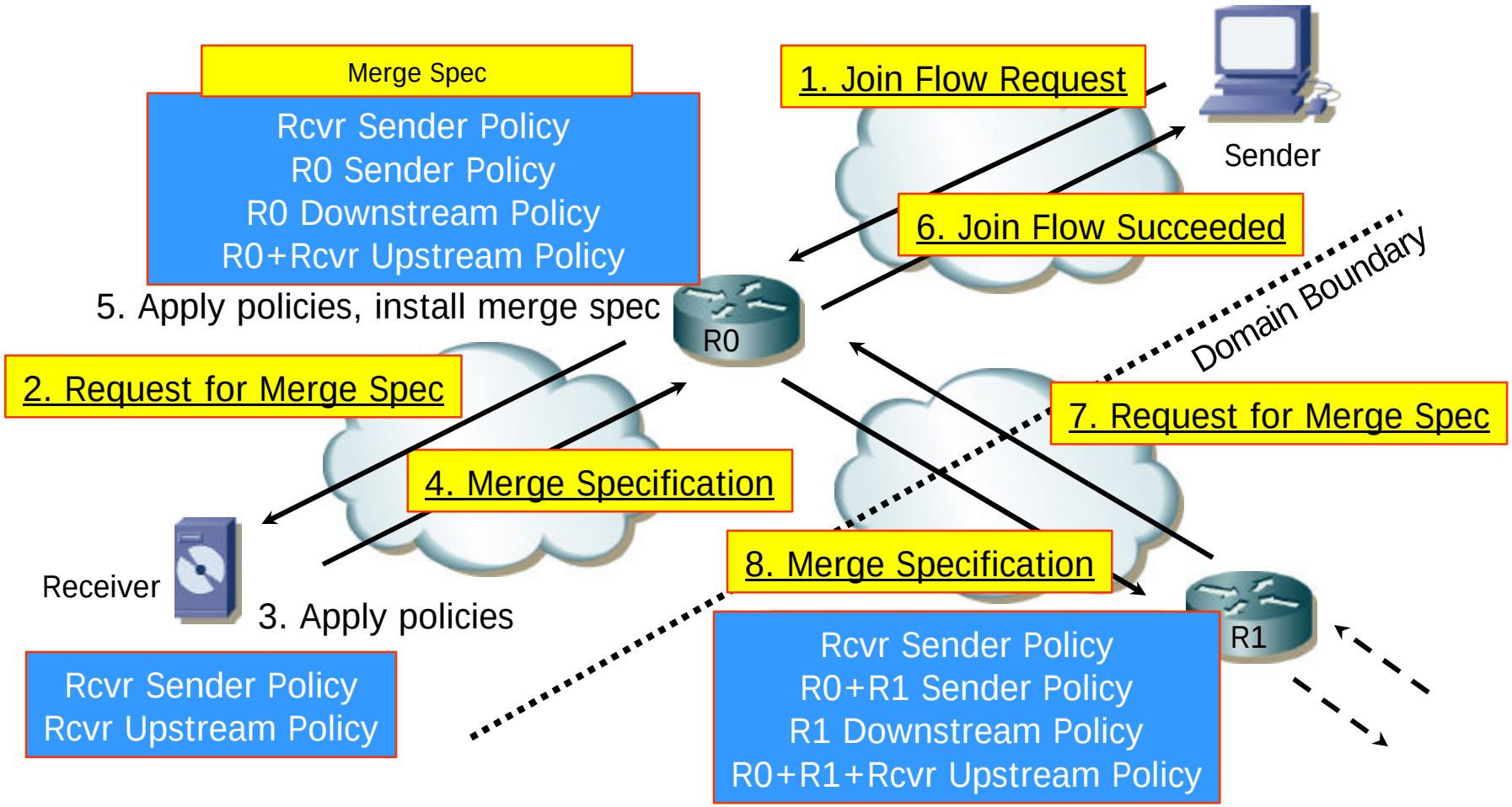
- Distributed policy enforcement
- Policies must not be weakened as they propagate upstream from receiver!
  - Need to ensure that policies at upstream nodes are not weaker than at downstream nodes
- Access control requirement:

  Every principal must satisfy local policy plus policies of all downstream nodes

Policy Monotonicity Requirements



Policy Monotonicity Requirements



Issue: Downstream Neighbor Discovery

- Upstream node does not find out identity of downstream neighbor until merge spec has propagated to that node
  - If downstream node does not satisfy policy, a lot of work may have been wasted!
- Possible solution
  - Upstream node (UN) includes its policy in the setup request message
  - Downstream node (DN) checks itself against UN's policy; if not accepted, DN forwards message without processing it
  - UN trusts DN to forward packets and enforce its policy, but not merge packets (is this sensible?)

Summary

- Concast provides a clean generic framework for doing hop-by-hop app-level processing in the network
- Security can be similarly partitioned:
  - Network is responsible for signaling security and implementing merge specifications accurately
  - Application (merge specification) is responsible for end-to-end security
- This structure helps scalability but raises issues wrt third-party policy enforcement

Questions/comments welcome!

Paper (submission to ICNP) is at:

http://protocols.netlab.uky.edu/~calvert/private/icnp03-submit.pdf